XXII CONGRESO IBEROAMERICANO DE DERECHO E INFORMÁTICA

BOLETÍN DE INFORMACIONES JURÍDICAS - EDICIÓN ESPECIAL

MEMORIAS DEL XXII CONGRESO IBEROAMERICANO DE DERECHO E INFORMÁTICA

CIUDAD de Panamá 2018

24 al 28 de Septiembre

Autoridades de la
Universidad de Panamá
2018

Dr. Eduardo Flores Castro
Rector Magnífico

Dr. José Emilio Moreno
Vicerrector Académico

Dr. Jaime J. Gutiérrez
Vicerrector de Investigación y Postgrado

Mgtr. Arnold Muñoz
Vicerrector Administrativo

Mgtr. Denis J. Chávez
Vicerrector de Extensión

Mgtr. Fidel Palacios
Vicerrector de Asuntos Estudiantiles

Mgtr. Nereida Herrera
Secretaria General

Mgtr. Carlos Bellido
Director General de los Centros Regionales Universitarios

Universidad de Panamá
Colaboración del Centro de Investigación Jurídica
Para las Memorias del XXII Congreso Iberoamericano de Derecho e Informática 2018

Órgano informativo de la
Facultad de Derecho y Ciencias Políticas
de la Universidad de Panamá

Dr. Hernando J. Franco Muñoz
Decano

Mgtr. Eliecer A. Pérez S.
Vicedecano

Lic. Judith Loré
Secretaría Administrativa

Mgtr. Arelys Eleana Ureña C.
Directora del Centro de Investigación Jurídica

Investigadores

Lic. Vanessa Campos Alvarado
Mgtr. Lidia Karina Mercado
Mgtr. Auri Morrison C.
Lic. Samuel Prado F.
Mgtr. Carmen Rosa Robles
Lic. Camilo Rodríguez
Mgtr. Belquis C. Sáez N.

Asistentes de Investigación

Wilfredo Gómez
Maybelline González
Hilary G. Ojo
Eyda Jazmín Saavedra
Jorge Del Cid Shailer Herrera

Secretaria
Licda. Gisela Espinosa

Biblioteca
Lic. Marcial Guerrero

MEMORIAS DEL XXII CONGRESO IBEROAMERICANO DE DERECHO E INFORMÁTICA

JUNTA DIRECTIVA DE APANDETEC

Presidente: Mgter Yoselin Vos Castro
Vice Presidente: Lic. Norman Gough
Secretaria: Mgter. Katiuska Hull
Subsecretario: Lic. José Vega Sacasa
Tesorero: Mgter Jorge Troyano
Vocal 1: Mgter Yadira Aguilar Gordón
Vocal 2: Lic. Sandy Wallace

COMITÉ ACADÉMICO APANDETEC EVALUADORES EXTERNOS

Título	Nombre	Cargo
Magister	Jorge Troyano	Coordinador del Comité Académico
Doctora	Bibiana Luz Clara	Presidente del Instituto de Derecho Informático del Colegio de Abogados de Mar del Plata
Doctor	José Heriberto García Peña	Profesor- Investigador de Derecho de la Escuela Nacional de Ciencias Sociales y Gobierno del Tecnológico de Monterrey
Profesor	Gustavo Amoni	Director General de la Escuela Nacional de la Magistratura de la República Bolivariana de Venezuela
Doctora	Vilma Sánchez	Letrada de la Sala Constitucional de Costa Rica
MCSE.	Álvaro X. Andrade Sejas	Director de Tecnología de la FIADI
Doctora	Nadia Noemí Franco Bazán	Profesora del Departamento de Procesal Penal de la Universidad de Panamá
Profesor	Guillermo Zamora	Facultad de Ingeniería en Sistemas en la Universidad Nacional de la Patagonia San Juan Bosco
Magister	Juan Kuan Guerrero	Segundo Vicepresidente del Colegio Nacional de Abogados de Panamá
Doctor	Humberto Carrasco Blanc	Profesor asociado derecho económico -comercial de la Universidad Católica del Norte, Chile

Universidad de Panamá
Año 2018 – Edición Especial

Facultad de Derecho y Ciencias Políticas de la Universidad de Panamá
Centro de Investigación Jurídica (CIJ)
Mgtr. Arelys Eleana Ureña,
Directora del CIJ.

Para correspondencia, canje y suscripción:
Centro de Investigación Jurídica (CIJ) de la Facultad de Derecho y
Ciencias Políticas de la Universidad de Panamá
Estafeta Universitaria
Panamá, República de Panamá
Teléfono: (507) 523-6139
Correo electrónico: c_investigacion_juridica@up.ac.pa
http://www.up.ac.pa/PortalUp/CentroInvestigacionJuridica.aspx?menu=456
Publicación Especial: ISSN 2075-4175

Corrección de textos:
Consejo Editorial
Asistente de Edición - Consejo Editorial
Eyda Jazmín Saavedra Herrera
Panamá, República de Panamá
Teléfonos: (507) 523-6139 – 523-6143

Diseño de Arte: APANDETEC

APANDETEC agradece infinitamente a la Universidad Tecnológica de Panamá por ser la sede oficial del XXII Congreso Iberoamericano de Derecho e Informática (CIDI)

***Primera Edición: 50** ejemplares*

CONTENIDO
MEMORIAS DEL XXII CONGRESO IBEROAMERICANO DE DERECHO E INFORMÁTICA

Págs.

MEMORIAS DEL XXII CONGRESO IBEROAMERICANO DE DERECHO E INFORMÁTICA

MISIÓN

Innovar, desarrollar, investigar, capacitar y promover, en la población panameña e internacional, el manejo seguro de las nuevas tecnologías, aportando en la creación de leyes, reglamentos y políticas que aborden la relación existente entre el Derecho y la informática, creando líderes que difundan la cultura de la innovación y conciencien a la ciudadanía en los ciberderechos que los protegen.

VISIÓN

Ser una Asociación referente en los proyectos de innovación, desarrollo y derecho en Panamá, impulsando la investigación, discusión y promoción del Derecho y Nuevas Tecnologías, aportando e impactando en el foro nacional e internacional.

VALORES:

1. *Innovación*
2. *Responsabilidad social*
3. *Voluntariado*
4. *Trabajo en equipo*
5. *Comunicación*
6. *Ciudadanía Digital*
7. *Sensibilización y Capacitación*
8. *Disrupción*
9. *Pensamiento Crítico*
10. *Cultura ética*

Estas memorias contienen los trabajos que fueron evaluadas por el Comité Académico para el XXII Congreso Iberoamericano de Derecho e Informática (CIDI).

PRESENTACIÓN

El impacto que conlleva el manejo de las nuevas tecnologías, las redes sociales, la inteligencia artificial, el cibercrimen, teletrabajo, así como otros tantos temas que entrelazan el derecho con la informática, invita a la comunidad jurídica a instruirse acerca de temas, que en otrora, parecían sumamente distantes a nuestras aulas y carreras.

Hoy, es casi impensable desprender la consecuencias, positivas y negativas, de una sociedad cada día más digitalizada y que la vorágine de cambios, que es cada vez más rápido, no permite a las tradicionales columnas del derecho movilizarse, siquiera, a una velocidad parecida. Es por ello que invitamos a nuestros lectores a nutrirse del grupo de trabajos que fueron presentados y evaluados por distinguidos juristas nacionales e internacionales.

Nos encontramos en momentos de cambios estructurales en temas jurídicos, actualmente el abogado que se aleje de las nuevas tecnologías, está destinado a simplemente desaparecer profesionalmente. Es tiempo de crear sinergias multidisciplinarias, nuevos trabajos de investigación, abrirse a otros horizontes y campos de batalla, el mundo evoluciona y nosotros debemos evolucionar con él.

El congreso se desarrolló del 24 al 28 de septiembre de 2018, entre ponencias, talleres, debates que impulsaron el pensamiento crítico, docencia y prácticas, lo que produjo como corolario y conclusión del evento la denominada ***CARTA DE PANAMÁ****, un pacto por la niñez y la adolescencia donde la Federación Iberoamericana de Asociaciones de Derecho Informático (FIADI) y la Asociación Panameña de Derecho y Nuevas Tecnologías (APANDETEC), asumimos el compromiso de unirnos en la lucha contra estos flagelos que afectan a nuestros niños y adolescentes, misma que fue presentada durante el acto solemne realizado en el salón de rectores de la Universidad Tecnológica de Panamá.*

Cabe resaltar que como Asociación hemos venido trabajando en estos temas por muchos años y producto del mismo, se presentó en el evento la obra de danza contemporánea denominada SICASTENIA, inspirada en los peligros que enfrentan los adolescentes en las redes sociales y representado por El Colectivo END de la Escuela Nacional de Danza con la asesoría técnica de nuestra Asociación.

Una vez finalizado el congreso es oportuno indicar que APANDETEC se siente honrada y agradecida con la Facultad de Derecho y Ciencias Políticas de la Universidad de Panamá, representada por su Decano el Doctor Hernando Franco Muñoz, por el apoyo irrestricto

para la consecución de la publicación de la presente revista, así como para que el XXII Congreso Iberoamericano de Derecho e Informática formara parte de las actividades en celebración de los cien años de la Escuela de Derecho y los quince años de nuestra Asociación . Una vez se presentó nuestra solicitud, la Facultad la tomó como suya pues reconoció la importancia de esta rama jurídica y realizó todas las acciones necesarias para cumplir con la meta trazada como país. Igualmente extendemos nuestro agradecimiento al Comité designado para esta tarea encabezado por el Profesor Francisco Flores, al Centro de Investigación Jurídica, al personal administrativo y estudiantes que trabajaron para que esta actividad cumpliera con el alto nivel académico con el que culminó y ahora plasmado con la publicación de las presentes memorias.

También debemos resaltar a todos los patrocinadores que, conscientes de la importancia de estos temas en la región, apostaron a la propuesta de APANDETEC y contribuyeron en la consecución del mismo, a ustedes muchas gracias. Nuestro gremio finaliza con esta actividad, la celebración de los quince años de nuestra fundación.

Estimados lectores, esperamos que disfruten del contenido de estas memorias y que sus reflexiones caigan en terreno fértil para promover con más fuerza esta interesante interrelación entre el derecho y la informática.

PRESENTACIÓN DE LAS MEMORIAS DEL XXII CONGRESO DE LA FIADI

Desde el momento en que se otorgó a Panamá para ser la sede del XXII Congreso Iberoamericano de Derecho e Informática de la FIADI, la Asociación Panameña de Derecho y Nuevas Tecnologías (APANDETEC), en su condición de miembro local, tomó como propia la responsabilidad de la convocatoria y organización de un congreso de tan alto nivel académico.

Durante una semana, en septiembre del 2018, más de medio centenar de expertos y académicos de toda Iberoamérica se dieron cita en esta ciudad a fin de debatir temas de actualidad para el derecho. La convocatoria a presentar ponencias fue escuchada por profesionales y académicos tanto del sector jurídico como del técnico, cuyos trabajos fueron evaluados y compilados en esta revista que hoy conjuntamente presentamos con la Universidad de Panamá. La publicación da para el estudio, el análisis y la motivación a las nuevas generaciones a investigar e incursionar en el interminable campo del derecho de las nuevas tecnologías.

Entre otros, los trabajos compilados gravitan entre: Protección de datos personales, datos abiertos, Peritaje forense, Gobernanza en Internet, Inteligencia artificial, Gobierno electrónico, Ciberseguridad y ciberterrorismo, Internet de las cosas, fintech, criptomonedas, Bigdata, Seguridad nacional e información crítica estatal, Gestión de cambio, sociedades y TIC.

Es evidente que las tecnologías actuales giran muy aceleradamente e impregnan a la sociedad de fenómenos insospechados hasta hace poco. Publicaciones como ésta sirven de consulta y constituyen un andamiaje a trabajos que en el futuro los puedan complementar. La tecnología es cambiante y con ella la sociedad en que se desarrolla y presenta; las consecuencias de su uso merecen nuestra atención y regulación en el evento que así lo amerite.

La llamada brecha digital en ocasiones parece ensancharse; APANDETEC con la publicación de las presentes memorias, pretende aportar a que esa brecha se contraiga un poco, acercando al lector a un número importante de trabajos de investigación novedosos y en ocasiones desafiantes.

Quedan las presentes memorias como testigos claves de un trabajo académico, organizacional, hospitalario y desinteresado en bien de la investigación y la sana convivencia iberoamericana; quedan como testigo de uno de los congresos iberoamericanos de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI), en donde cada detalle fue celosamente cuidado.

Auguramos una provechosa e interesante lectura a todos los que nos honren con consultar estos trabajos, quienes sin duda despertarán su espíritu investigador y aventurero, al punto que seguramente pronto se animará a publicar en alguno de nuestros próximos eventos.

Asociación Panameña de Derecho y Nuevas Tecnologías
APANDETEC

Panamá, octubre 2018.

PACTO POR LA NIÑEZ Y ADOLESCENCIA

Las nuevas tecnologías de la información y comunicación han producido un vertiginoso desarrollo en nuestra sociedad, siendo Internet uno de los mayores motores de estas nuevas tecnologías.

Los niños, niñas y adolescentes tienen cada día mayor acceso a los medios que Internet les brinda.
Hoy en día, Internet juega en la vida de los niños, niñas y adolescentes un papel fundamental, pues para ellos, que nacieron luego de la irrupción de Internet, esta es la que día a día les ofrece, de múltiples y diferentes formas, el esparcimiento, el conocimiento y la comunicación entre ellos.

Pero así como Internet ha acercado el conocimiento a muchos y ha ayudado a los menores en su educación y comunicación, también ha creado graves peligros para la vida privada de estos, mediante conductas negativas ejercidas por los propios menores o conductas desvalidas ejercidas por terceros con el fin de dañar la salud sicofísica de los menores.

La discriminación, la pornografía, en especial la pornografía de menores de edad, el Ciberbullying, el Grooming, el mal uso de las redes sociales, los retos que ponen en riesgo la integridad de los niños, y la divulgación de noticias falsas, son entre otras conductas los mayores riesgos para los menores.

El Ciberbullying, entendiendo por tal al hostigamiento a menores través de medios informáticos, se ha vuelto una práctica común en los jóvenes en nuestras sociedades, en donde se molesta, amenaza, injuria o humilla a otros menores utilizando el correo electrónico, los grupos de chat, o las redes sociales.

Esta conducta se agrava incluso cuando se cometen acciones deliberadas de quien simula ser un mayor, a fin de lograr un acercamiento con un menor con fines de crear una amistad, para facilitar luego el abuso sexual de este. Esta conducta tipificada en muchas legislaciones como Grooming, ha alcanzado niveles alarmantes en los últimos años.
La suplantación de identidad, también es una figura jurídica poco explorada en la norma, pero sí manifestada en la práctica del ciberespacio, donde es más frecuente suplantar identidades, a fin de cometer abusos en contra de los niños.

Según cifras oficiales emitidas por el Primer Estudio Internacional de Acoso Escolar o Bullying, llevado adelante por la ONG Internacional Bullying Sin Fronteras en 18 países del Continente, siete de cada 10 niños en América Latina son víctimas de acoso en la escuela

La pornografía infantil, invade las pantallas produciendo un enorme daño en la salud síquica de muchos menores.

El uso excesivo de juegos en las computadores por parte de niños y adolescentes, así como las permanentes comunicaciones electrónicas de los menores, está creciendo en forma alarmante y transforma a estas situaciones en adicciones graves en los menores, produciendo que ellos se alejan de la integración familiar y de las relaciones directas con otros menores, llegando incluso a situaciones en las cuales el menor se aleja del mundo real para vivir en un mundo electrónico.

*Es por todo esto que este **XXII Congreso Iberoamericano de Derecho e Informática** ha debatido muchos de estos temas y ha resuello redactar este documento al que llamaremos Carta de Panamá.*

1) *Las niñas, niños y adolescentes tienen el derecho a la dignidad como sujetos de derechos; así como a no ser sometidos a trato violento, discriminatorio, vejatorio, humillante, intimidatorio.*
2) *Los padres y madres tienen el derecho y la responsabilidad de orientar, educar y acordar con sus hijos e hijas un uso responsable de internet, transmitiéndoles que Internet si bien se funda en los principios de neutralidad y de libertad de expresión, no es un espacio abierto carente de normas y de responsabilidades consecuentes cuando se causan daños, inculcándose en los menores la idea del uso responsable de internet y de las redes sociales.*
3) *Al mismo tiempo, se debe fomentar la formación en nuevas tecnologías de los progenitores por parte de los organismos públicos, con el fin de no reformular los roles entre padres y menores como educandos y educadores respetivamente, debido a la brecha digital.*
4) *Es necesario que se advierta a los menores que en cualquier comunicación electrónica, el interlocutor puede ocultar su identidad a fin de posteriormente abusar del menor, instruyéndolos del concepto de Grooming y de las gravísimas consecuencias que puede deparar.*
5) *Debemos instruir a los menores en un buen manejo de los dispositivos con actuaciones que fomenten su propia seguridad a través de acciones preventivas, tales como dejar tapada la visión de la cámara web por defecto o cambiar las contraseñas de sus cuentas de correo y redes sociales con periodicidad.*
6) *Se debe recalcar en el menor la importancia que tiene el respecto de la vida privada de los demás, a fin de que no ejerzan actos de Ciberbullying que puede causar graves daños a terceros. Existen derechos como el de la propia imagen, que protegen a la persona, frente al uso indebido de su imagen por parte de un tercero, pero no existe duda del*

necesario enfoque preventivo en Internet, que haga del ciberespacio un ambiente seguro para los niños

7) las niñas, niños y adolescentes tienen derecho a la educación pública y gratuita, brindada por el estado, que debe incluir el uso de las nuevas tecnologías, no pudiendo por ninguna causa restringirse su acceso, que debe alcanzar también a las niñas, niños y adolescentes con alguna discapacidad

8) Las niñas, niños y adolescentes tienen Derecho a la Intimidad en sus comunicaciones electrónicas, así como a no proporcionar datos personales por Internet, preservando su identidad y su imagen.

9) Los Estados a través de sus gobiernos deben comprometerse a cooperar para facilitar el acceso de los niños y adolescentes a las tecnologías de la información, a fin de promover su desarrollo y evitar la creación de una barrera tanto entre niños ricos y pobres como entre los países ricos y los pobres. Asimismo esos estados son responsables de velar por la protección de los niños, niñas y adolescentes, así como tiene un mandato para que se regule el comercio electrónico en aras de proteger al consumidor de esta población. La política pública tendría que estar enfocada en dos ámbitos: reducción de brecha digital y educación digital para niños, niñas y adolescentes.

*10) **La Federación Iberoamericana de Asociaciones de Derecho Informático (FIADI)** y **la Asociación Panameña de Derecho y Nuevas Tecnologías (APANDETEC),** asumimos el compromiso de unirnos en la lucha contra estos flagelos que afectan a nuestros niños y adolescentes, haciendo igualmente partícipes al resto de asociaciones que conforman nuestra federación de los valores y objetivos aquí expuestos.*

Dado en la ciudad de Panamá, República de Panamá, a los 28 días del mes de Septiembre de 2018

PONENCIAS

JUICIOS PARALELOS Y REDES SOCIALES

FEDERICO BUENO DE MATA
Profesor Titular de Derecho Procesal
Universidad de Salamanca
febuma@usal.es

1. El principio de publicidad en la sociedad de la información

En los tiempos en los que nos encontramos, marcados por una profunda informatización, llegamos a veces a confundir y entremezclar nuestra esfera pública con la privada. Parece que lo que no está en Internet, y más concretamente en las redes sociales, no existe o nunca ha sucedido.

Esta sobreexposición pública y el afán por querer compartir nuestro día a día ante millones de desconocidos en tiempo real, hace que nuestro afán por conocer todo lo que ocurre a nuestro alrededor aumente. Del mismo modo, si a lo anterior sumamos que todo lo que se cuelga en la Red es objeto de cuestionamiento, crítica y opinión; vemos como la Red se convierte en una especie de nuevo ágora virtual en el que las personas ejercen su derecho a la libertad de expresión sin tener en cuenta las repercusiones de las palabras que han lanzado a golpe de *click*.

El estado de opinión se acrecienta cuando hablamos de servicios públicos como la sanidad o la justicia, pues como coloquialmente se escucha, todos llevamos un médico o un juez dentro de nosotros, lo que nos habilita a opinar sobre cualquier tipo de cuestión sin tener necesariamente un conocimiento especializado en la materia que sometemos a nuestro juicio valorativo.

Si nos centramos en el sector judicial, debemos partir de que, tal y como reconoce el art. 120.1 de la Constitución Española, "las actuaciones judiciales serán públicas, con las excepciones que prevean leyes de procedimiento". De esta forma se podría ligar este precepto con lo recogido en el artículo 20 de nuestra norma suprema, al contemplar las libertades de expresión y de información. Así en su punto primero letra a, se indica que se reconoce el derecho "a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción.", mientras que en su letra d, dice reconocer igualmente el derecho "a comunicar o recibir libremente información veraz por cualquier medio de difusión", pero a este último ya le aplica un cierto límite al decir que se deberá tener en cuenta el secreto profesional en el ejercicio de estas libertades pero recuerda que no deberá restringirse mediante ningún tipo de censura previa.

Pues bien, este primer escenario hace emerger un debate sobre si es ético, prudente y lícito trasladar al debate público determinadas actuaciones judiciales, más cuando muchas personas creen, desde nuestro punto de vista de manera errónea, que la Constitución hace que todo el mundo entienda que podemos tener acceso a cualquier caso amparándonos en nuestro a la

acción o al derecho a la jurisdicción, entendido como un derecho público subjetivo de forma ilimitada.

Si bien es cierto que dentro del Título I de la CE, dedicado a los derechos fundamentales, en la sección primera del capítulo segundo se regulan "derechos fundamentales y libertades públicas", nuestro artículo 24. 2 recoge que "todos tienen derecho (…) a un proceso público"; el precepto no se refiere con ello a un principio de publicidad absoluto, pues posteriormente reconoce su limitación en dos modalidades: un principio de publicidad absoluto en el que las actuaciones pueden ser conocidas por toda la sociedad o bien un principio de publicidad relativo, en el que las actuaciones judiciales solo serán conocidas por las partes en conflicto así como por las pruebas personales que cada una de ellas desee proponer en juicio y sean admitidas por el juzgador.

Esta limitación viene igualmente reconocida en el art. 232 de la LOPJ al decir expresamente que de manera excepcional "por razones de orden público y de protección de los derechos y libertades, los Jueces y Tribunales, mediante resolución motivada, podrán limitar el ámbito de la publicidad y acordar el carácter secreto de todas o parte de las actuaciones". Por todo ello, a pesar de que la regla general es que las actuaciones judiciales sean públicas, no quiere decir que tengamos que tener acceso siempre a ellas y, en el caso de que existan filtraciones, podamos y debamos opinar libremente a través de medios tecnológicos pues de esta manera estaríamos ejerciendo nuestros derechos al tiempo que menoscabamos los de las de las partes involucradas en un determinado proceso al tiempo que podemos a llegar a interferir en el buen hacer de distintos operadores jurídicos.

Llegados a este punto debemos plantearnos si las nuevas tecnologías pueden llegar a suponer una amenaza o un instrumento exponencial para hacer cumplir el principio de publicidad procesal. Nuestra respuesta en este sentido debe ser equilibrada y supeditada al buen uso de la tecnología y al buen entendimiento de lo que el principio de publicidad supone.

Por un lado, pensamos que las tecnologías pueden realzar este principio siempre que el mismo no se sobredimensione. Esto quiere decir que incluso pueden ser utilizadas como mecanismo para publicitar un determinado juicio con un relevante interés público a través de una difusión por *streaming*, tal y como ha ocurrido en nuestro país de manera puntual en casos tan relevantes como el caso Gurtel, en el que muchos portales de Internet ofrecieron su retransmisión en tiempo real. Con ello estamos potenciando lo que se entiende por publicidad directa o activa, al equiparar la posibilidad de que el público esté presente tanto en la sala de vistas de manera física como en sus casas a través de un monitor.

En este sentido, España podría valorar incluir en su normativa alguna referencia a este tipo de tecnología para ampliar este principio a través de la creación de un canal o un portal jurídico dedicado a estas cuestiones, como así han hecho ya países como Chile, Perú o incluso China[1]. Ahora bien, estas herramientas deberán ser usadas de manera puntual y en casos que

[1] A continuación se detallan los enlaces de los poderes judiciales de Chile y Perú: (Fecha de última consulta: 26 de diciembre de 2017)

- http://www.poderjudicialtv.cl/
- http://www.justiciatv.tv/

presenten un interés global para la ciudadanía siempre que no se interfieran con derechos de especial protección de cualquiera de las partes y en los que la sociedad en su conjunto pueda verse afectada por la resolución que se dicte, pues de lo contrario estaríamos enmarcando y defendiendo una publicidad del juicio que, a nuestro parecer, no estaría contemplada dentro de nuestro principio de publicidad procesal[2]. Así, debemos recordar que concretamente nuestro Tribunal Constitucional expuso que la finalidad del derecho fundamental a un proceso público es "*proteger a las partes frente a una justicia sustraída al conocimiento público y mantener la confianza de la comunidad en los Tribunales*", y que el mismo no es un derecho absoluto, sino que puede ser limitado o excluido por razones justificadas en una sociedad democrática.

Así nos encontramos con que las nuevas tecnologías pueden ser perjudiciales para la propia actuación judicial y para el principio de publicidad procesal, dado que su uso desmedido puede poner en duda las necesarias garantías para la celebración de un juicio justo[3]. En este sentido, el autor parte de la idea de que en los casos que presentan un alto grado de interés público, el secreto de sumario pocas veces se cumple y en ocasiones las filtraciones en los medios y a través de las nuevas tecnologías pueden hacer variar la propia investigación. Sin ir más lejos en el caso de la desaparición de Diana Quer, uno de los casos mediáticos más recientes de España, durante el 29 de diciembre de 2017 se filtró a la prensa que el principal sospechoso de los hechos había intentado repetir el secuestro y posterior desaparición de una joven, y ante el temor de que el propio autor de los hechos lo pudiera leer en la prensa digital se aceleró su detención para evitar una posible fuga.

Es necesario apuntar que las actuaciones en la fase de investigación tienen un carácter predominantemente secreto por lo que se refiere a la publicidad absoluta, al regular el art. 301 LECrim que "*Las diligencias del sumario serán secretas hasta que se abra el juicio oral, con las excepciones determinadas en la presente Ley"*, pero no así respecto a la publicidad relativa, pues, conforme al artículo 302 LECrim, las partes personadas podrán tomar conocimiento de las actuaciones e intervenir en todas las diligencias del procedimiento. Sin embargo, si estamos ante un delito público, el juez que instruye el caso puede dictar a través de un auto de oficio, o a propuesta del Ministerio Fiscal o de cualquiera de las partes personadas, el secreto total o parcial para todas las partes personadas, por tiempo no superior a un mes y debiendo alzarse necesariamente el secreto con diez días de antelación a la conclusión del sumario.

Si esta misma situación la extrapolamos a la fase de juicio oral, regulado en los artículos 649 y 680 y siguientes LECrim, con posibilidad de restringir la publicidad absoluta al comenzar el juicio o en cualquier momento del mismo mediante resolución motivada en razones de moralidad, de orden público y de protección de los derechos fundamentales o por el respeto debido a la persona o familia del ofendido.

Si esta cuestión no es bien articulada por el juzgador puede que la exposición en tiempo real de determinadas audiencias o las filtraciones provoquen que algunas pruebas personales

- Por otro lado China, al ser uno de los países menos transparentes sobre determinados procesos desarrollados en su país, ya anunció esta medida en septiembre de 2016, https://voltaico.lavozdegalicia.es/2016/09/china-retransmision-juicios-streaming/

[2] SIMON CASTELLANO (2013: 451 y ss.)

[3] SIMON CASTELLANO (2011: 67 y ss.)

como los testigos no declaren de manera totalmente espontánea al saber lo que han dicho en la sala otros testigos. Esto nos hace compartir la idea de que la fase de juicio oral deberá ser tratada con total precaución para evitar este tipo de comportamientos y por ello el juez deberá ser consciente de estas posibles modificaciones en las declaraciones de los distintos sujetos que acudan a la sala de vistas.

En último lugar nos encontraríamos el caso en el que la tecnología es usada a pesar de encontrarnos en un régimen de publicidad relativa y bajo secreto de sumario. En este caso pasaríamos a hablar de cómo diferentes herramientas digitales como cámaras de videos, fotografía o terminales móviles sirven para realizar filtraciones a distintos medios de comunicación al ser un claro altavoz y generador de opinión pública o como ya los propios particulares pueden hacer uso de esta información y colgarlas en Internet a través de cualquier web o red social, lo que nos llevaría a hablar de un nuevo canal por el que generar estados de opinión y juicios paralelos basados en un mal entendido principio de publicidad procesal.

A lo largo de las siguientes líneas abordaremos el tema del uso actual de las redes sociales como medio de creación de juicios paralelos, con el que estaríamos entendiendo de una manera errónea este principio y desvirtuando así el debido proceso, para posteriormente realizar una serie de reflexiones sobre la interacción del principio de publicidad con las nuevas tecnologías y las perspectivas futuras que deberán acometerse para amoldarlo a la actual realidad tecnológica.

2. Juicios paralelos y redes sociales

Ante un sistema judicial marcado por la lentitud y la ralentización de muchos casos con proyección mediática, los medios de comunicación y las redes sociales proporcionan una información marcada por la inmediatez en la que en algunas ocasiones se tratan cuestiones de fondo de determinados casos que a priori estarían bajo secreto del sumario, es decir, procedimientos en las que las actuaciones que se realizan en la investigación no son públicas o bien, juicios orales que se celebran bajo un régimen de publicidad relativa, por lo que las personas ajenas a las partes del conflicto tampoco deberían tener información sobre lo que ocurre en la sala de vistas.

Cuando alguna información trasciende en estos casos hablamos de las comentadas filtraciones, las cuales pueden dar lugar a juicios paralelos y generar estados de opinión en la población, lo que podría llegar, por qué no, a suponer una presión añadida al personal jurisdiscente que está conociendo el caso y que debe emitir una resolución judicial fundada en derecho. En décadas anteriores este tema ya ha sido tratado y cuestionado en multitud de ocasiones poniendo el foco de la cuestión en los medios de comunicación y cómo los mismos pueden llegar a desvirtuar de manera clara la realidad jurídica de los hechos para acabar ofreciendo una imagen distorsionada de la realidad.

Ahora bien, esta realidad se complica aún más cuando las opiniones en redes sociales afloran de una manera desmedida y descontrolada, con lo que se fabrica poco a poco una especie de escenario paralelo al que algunos expertos han catalogado como “posverdad”. Este vocablo

fue elegido en 2016 como palabra del año[4] por su uso constante para referirse a informaciones vinculadas al *Brexi*t o a la cuestionada victoria de *Donald Trump*, describe "la distorsión deliberada de una realidad, con el fin de crear y modelar opinión pública e influir en las actitudes sociales, en la que los hechos objetivos tienen menos influencia que las apelaciones a las emociones y a las creencias personales[5]". En el mismo sentido el DRAE define posverdad como "distorsión deliberada de una realidad, que manipula creencias y emociones con el fin de influir en la opinión pública y en actitudes sociales".

Debemos partir de que las redes sociales contribuyen de manera directa a la formación de esta posverdad, puesto que existen diferencias en la formación de juicios paralelos en redes sociales con respecto a los medios tradicionales, debido a las características propias de aplicaciones como *Twitter*.

Redes sociales como ésta han supuesto un espacio en el que no solo se generan juicios paralelos sino que también sirven para que muchas personas opinen de cualquier tema erigiéndose como salvador, verdugo o, incluso, juez. Así, "da la sensación de que el derecho a la libertad de expresión e información es un derecho preponderante del ordenamiento jurídico, prevaleciendo sobre el resto de derechos reconocidos constitucionalmente, y carente de límites[6]". Tan grave es el caso que nuestro propio legislador ha sido consciente de ello regulando los conocidos como "delitos de odio", al tiempo que la Fiscalía General del Estado dictó un Decreto de fecha 10 de octubre de 2011, por el cual se pone en funcionamiento la Delegación de Tutela Penal de la Igualdad y contra la Discriminación. Así, se determinó la necesidad de designar un fiscal en cada provincia encargado de coordinar la actuación de la Fiscalía en materia discriminatoria, actuando como punto de contacto con la red nacional dirigida desde marzo de 2013[7].

Con ello se pretende enjuiciar este tipo de conductas y se articula paralelamente el "Protocolo de actuación de las Fuerzas y Cuerpos de Seguridad para los delitos de odio y conductas que vulneran las normas legales sobre discriminación", aprobado mediante la Instrucción nº 16/2014[8], para que los agentes presten especial atención a determinadas pruebas periféricas así como a la intención discriminatoria real a la hora de perpetrar delitos de odio.

Con independencia de que lo publicado en redes sociales tenga la entidad o gravedad necesaria para ser delito, es cierto que la frase coloquial: "habla mal que algo queda", aquí ciertamente se cumple. Llegamos en este sentido a una especie de linchamiento mediático en el que todos los requisitos para el origen de los juicios paralelos no solo existen, si no que *Twitter* se instituye como un elemento exponencial de este tipo de juicios en los que la manipulación de la información judicial no nos deja separar lo cierto de lo incierto y en los

[4] Vid. AMÓN, R., "Posverdad: palabra del año" *Diario el País*, 17 de noviembre de 2016, disponible en https://elpais.com/internacional/2016/11/16/actualidad/1479316268_308549.html (Fecha de última consulta: 28 de diciembre de 2017)
[5] CARO FIGUEROA, G., "Post-verdad: nueva forma de la mentira", *Diario Clarín*, 22 de noviembre de 2016, disponible en: https://www.clarin.com/opinion/Post-verdad-nueva-forma-mentira_0_HyjwGEMMg.html (Fecha de última consulta: 28 de diciembre de 2017)
[6] MATUTE CHAMARRO (2017: 3 y ss.)
[7] MATUTE CHAMARRO (2017: 22)
[8] Este protocolo tiene su origen en el Protocolo de actuación que se otorga la policía autonómica de Cataluña en relación a los hechos delictivos cometidos contra el colectivo LGTB, el 10 de marzo de 2010.

que el derecho fundamental al honor y a la propia imagen de determinadas partes quedará claramente afectado.

Si nos fijamos en muchos de los *tweets* que opinan sobre casos mediáticos, vemos como en los mismos la información y la opinión se entremezclan de tal modo que se confunden, al tiempo que de manera sutil se introducen opiniones sesgadas que poco a poco calan en sus contactos favoreciendo una opinión grupal que desemboca en un veredicto de culpabilidad o inocencia acerca de la participación y comisión de unos hechos por partes de determinadas personas.

Nos encontramos ante un panorama en el que ya no solo la imagen o el honor de las partes queda afectada, sino que propiamente colisionamos de manera frontal con el principio de presunción de inocencia y lo recalificamos como una nueva "presunción de culpabilidad" en este nuevo escenario de posverdad.

Nuestra opinión acerca de que redes como *Twitter* han servido como instrumento catalizador y multiplicador de juicios paralelos se fundamenta en las propias características de estas aplicaciones basadas en la viralización e impacto de sus mensajes así como en su componente intrínseco de perdurabilidad en la Red.

En primer lugar vemos como la carga de información en 280 caracteres hace que los mensajes sean directos, casi parecidos a eslóganes en las que se debe decir mucho en poco espacio, lo que fomenta la atención. Esta característica unida a la opción de "Re twittear" el mensaje hace que el contenido vaya saltando de grupo en grupo hasta llegar a un público cada vez más elevado lo que fomenta que el mensaje se haga viral. Pues bien, esta característica propia del formato viene a su vez apoyada por un nuevo perfil de internauta denominados *influencers* que, como su propio nombre indica, cuentan con un peso especial entre distintas comunidades de usuarios a contar por cientos de miles sus seguidores y se conviertan en verdaderos líderes de opinión.

Igualmente existe la opción del *hashtag*, etiqueta consistente en una cadena de caracteres formada por una o varias palabras concatenadas y precedidas por una almohadilla, que puede ser usado como una especie de altavoz en el que unos usuarios llaman a otros para opinar conjuntamente, y por regla general de forma negativa, de cualquier asunto de actualidad[9]. Del mismo modo la posibilidad de insertar *links* o hipertextos que nos permiten enlazar lo que comentamos con páginas webs externas que refuerzan o apoyan el comentario que acabamos de compartir.

Si unimos a lo anterior que en la Red "las palabras no se las lleva el viento", podemos entender como la perdurabilidad de lo que los usuarios comparten en Internet hacen que el mensaje aún cobre mayor relevancia a tenor de que el derecho al olvido está prácticamente falto de regulación en nuestra normativa y las referencias existentes a nivel europeo son vagas y nos presentan un procedimiento arduo, lento y difícilmente comprensible para los ciudadanos con un nivel medio de informática y legos en derecho.

[9] Vid. Maledicencia 2.0 y juicios paralelos en Twitter", *Blog de FIDE: El Confidencial.com*, Disponible en: https://blogs.elconfidencial.com/espana/blog-fide/2016-05-19/maledicencia-2-0-y-juicios-paralelos-en-twitter_1202096/ (Fecha de última consulta: 30 de diciembre de 2017)

3. Retos y desafíos del principio de publicidad ante la tecnología

Como hemos visto a lo largo de este estudio, ha quedado demostrado que las nuevas tecnologías aplicadas al sector judicial pueden llegar a distorsionar la publicidad de determinados asuntos, pues conllevan una serie de problemas como las filtraciones de determinadas informaciones durante la fase de investigación cuando existe secreto sumarial o durante la fase de juicio oral cuando el mismo se celebra a puerta cerrada.

Las filtraciones en algunas ocasiones pueden dar al traste con una investigación, al poder llegar a oídos del investigado y que el mismo intente la fuga o pueden provocar que las diligencias se precipiten para evitar estos resultados, tal y como pudo haber pasado en España ante el mediático caso de Diana Quer por temor a que el autor confeso del crimen hubiera huido u ocultado pruebas. Esta primera fuga de información debería estar castigada con independencia de donde provenga, ya sea por las partes, testigos, abogados o los propios magistrados; derivando las responsabilidades oportunas basadas en el potencial perjuicio que puedan llegar a ocasionar.

Del mismo modo los juicios paralelos también se han fomentado a través de la tecnología y más en concreto, por medio de las redes sociales como *Twitter* en el que gracias a la inmediatez y permanencia en la Red de sus contenidos o actividades como compartir *links*, "retwittear" comentarios o la utilización de *hashtag*, hacen que el mensaje se unifique y viralice en un corto espacio de tiempo. Al haber millares de interlocutores con multitud de ideologías y formación jurídica dispar, el mensaje se deforma progresivamente hasta llegar a la peor versión del juego popular "el teléfono escacharrado". El problema es que aquí la materia suele ser sensible, lo que no quita para que muchos ciudadanos se crean en la libertad de poder opinar sobre todo lo que acontece a nivel judicial obviando garantías procesales básicas que afectan al desarrollo del debido proceso.

A raíz de la gravedad del asunto el legislador español hace unos años a tipificado los delitos de odio y creado incluso una fiscalía especializada para su investigación. Aun así, creemos que sería necesario explorar distintas sanciones o respuestas penales y no penales para graduar, prevenir y combatir este tipo de actuaciones que sobrepasan con creces la libertad de expresión.

Por otro lado, debemos ser capaces de vislumbrar el futuro cercano que la tecnología tendrá sobre la publicidad procesal, al encaminarnos hacia una nueva era en la que la práctica totalidad de nuestros datos recabados por las instituciones públicas estarán en la Red y puede que la Inteligencia Artificial nos ayude a Administrar Justicia de manera más eficaz.

Puede que estos cambios relativamente próximos hagan que se debilite nuestro derecho a la protección de datos personales y nos inviten a repensar nuestro derecho a la intimidad e incluso el secreto de las comunicaciones…y, por qué no, avanzar hacia no solo unos derechos de cuarta generación, sino hacia unas garantías procesales inspiradas en estos últimos. Así, puede ser igualmente el tiempo correcto para plantearnos las repercusiones que pueden tener sobre el ejercicio de la función jurisdiccional de jueces y magistrados la presión a la que pueden verse sometidos por dictar un fallo en un sentido u otro para contentar al pueblo, quién ha manifestado previamente y de manera mayoritaria un veredicto. ¿Podríamos

garantizar aquí la imparcialidad de estos jueces o cabría la posibilidad de plantearnos alguna nueva causa de abstención y recusación para contemplar esta idea?

Resultaría aquí osado hablar de una especie de "neoprocesalismo" o un avance de esta rama del derecho, pues la base del derecho procesal sigue siendo la misma: un ordenamiento que sirve de abanico garantista a las partes y que se sostiene sobre sus tres ejes básicos de jurisdicción, acción y proceso; pero lo que si tenemos claro es que los derechos ya no se ejercen de las mismas formas ni a través de las mismas vías que en 1978, cuando se promulgó nuestra Constitución. Así, creemos que determinadas garantías procesales constitucionales deberían adaptarse a la realidad que acontece, al invadir la tecnología la manera de relacionarnos entre sí y de impartir justicia en el mundo.

Por último, debemos plantearnos que los cambios que existen en el ejercicio de los derechos deben ser amparados legalmente para evitar un clima de inseguridad jurídica creciente y palpable al pensar que ante la tecnología podemos legislar caso a caso o "en caliente", sin acabar de percibir que las normas que promulguemos deberán pensar no en el presente, sino en el futuro para no quedar obsoletas o incompletas antes de ser promulgadas.

Referencias bibliográficas

GIL GONZÁLEZ, E. "Big data y datos personales: ¿es el consentimiento la mejor manera de proteger nuestros datos?" *Diario La Ley*, Nº 9050, Sección Tribuna, 27 de Septiembre de 2017

MATUTE CHAMARRO, I., "Los delitos de odio en las redes sociales", Trabajo Fin de Título Máster de Acceso a la Abogacía. USAL, (Director BUENO DE MATA, F.,), pág. 3, 2017. Disponible en gredos.usal.es

POSE ROSELLÓ, Y., MORALES ALMAGUER, I., "El principio de publicidad en el proceso penal y los medios de comunicación**",** El derecho procesal en la encrucijada entre la modernidad y la tradición **(**Memorias del III Congreso Internacional de Derecho Procesal) Versión CD, pág. 24

PEREZ- LUÑO ROBLEDO, E., *El procedimiento de Habeas Data: el derecho procesal ante las nuevas tecnologías*, Madrid, 2017.

RODRÍGUEZ VALLS, T., "Principio de publicidad procesal y derecho a la protección de datos de carácter personal: aproximación a la problemática actual en Juzgados y Tribunales españoles", *La Ley Penal*, Nº 71, Sección Práctica penal, Mayo 2010,

SIMON CASTELLANO, P., "El carácter relativo del derecho al olvido en la red y su relación con otros derechos, garantías e intereses legítimos", *Libertad de expresión e información en Internet: amenazas y protección de los derechos personales* / Valencia, 2013, págs. 451-476

SIMON CASTELLANO, P., "Los límites jurídico-constitucionales de la Administración electrónica en España y el Open Government" *Revista Aranzadi de derecho y nuevas tecnologías*, Nº. 27, 2011, págs. 67-85

Referencias de Internet

AMÓN, R., "Posverdad: palabra del año" *Diario el País*, 17 de noviembre de 2016, disponible en https://elpais.com/internacional/2016/11/16/actualidad/1479316268_308549.html (Fecha de última consulta: 28 de diciembre de 2017)

CARO FIGUEROA, G., "Post-verdad: nueva forma de la mentira", *Diario Clarín*, 22 de noviembre de 2016, disponible en: https://www.clarin.com/opinion/Post-verdad-nueva-forma-mentira_0_HyjwGEMMg.html (Fecha de última consulta: 28 de diciembre de 2017)

BLOG DE FIDE, "Maledicencia 2.0 y juicios paralelos en Twitter", *El Confidencial.com*, Disponible en: https://blogs.elconfidencial.com/espana/blog-fide/2016-05-19/maledicencia-2-0-y-juicios-paralelos-en-twitter_1202096/ (Fecha de última consulta: 30 de enero de 2017).

GONZÁLEZ RUISANCHEZ, S., "ENATIC analiza los retos y oportunidades del Big Data para los abogados", *Blog Abogacía Española*, 27 de Junio de 2016. http://www.abogacia.es/2016/06/27/enatic-analiza-los-retos-y-oportunidades-del-big-data-para-los-abogados/ (Fecha de consulta: 26 de diciembre de 2017)

JABOIS, M., "A la caza de la familia Quer", *Diario el País*. Disponible en: https://politica.elpais.com/politica/2018/01/03/actualidad/1515008214_301244.html (Fecha de última consulta: 4 de enero de 2018).

PENSAMIENTOS PARA LA REDUCCIÓN DE LA BRECHA TECNOLÓGICA-JURÍDICA Y LA ESTANDARIZACIÓN DE LAS LEGISLACIONES DEL MUNDO.

Por: ***Vilma Sánchez Del Castillo***[1]
Costa Rica

Entre el back to basics y los nuevos paradigmas de la revolución tecnológica.

1) Particularidades y bondades del Derecho Uniforme. El *back to basics*

Como fiel seguidora y creyente de las bondades y capacidades prácticas y atemporales del Derecho Uniforme del Comercio Internacional -DUCI-, sobre el cual, la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional -CNUDMI/UNCITRAL- nos ilustra desde hace más de 50 años, estimo indefectiblemente, que para atender de manera acertada la compleja disciplina jurídica y práctica que reviste al Derecho de la contratación electrónica y a su fiel asociado, la revolución tecnológica, de inicio, es fundamental dominar el Derecho uniforme del Comercio Electrónico.

El Derecho uniforme en esta rama, queda zanjado por medio de la Ley Modelo de la CNUDMI/UNCITRAL de Comercio Electrónico, que data ya del año 1995 y, que pretende, más allá del alcance del Derecho Internacional Privado, con sus normas de conflicto y fijación de la jurisdicción competente para conocer de una determinada desavenencia de carácter internacional, establecer *a priori*, cuál va a ser el fundamento legal que va a regularizar una determinada situación, estableciendo un marco normativo de carácter uniforme, cuya interpretación también, se pretenda homogénea.

Esta referencia, obliga *per se* a las partes, a ajustarse a una ordenación, que impida, o al menos, minimice, a futuro, la proliferación de conflictos. Situación que se complica, a raíz del carácter eminentemente internacional de las transacciones electrónicas.

El DUCI marca su ámbito de acción bajo la tutela de algunas máximas, que aún hoy, tras la aparición de lo que pareciera ser una Segunda Revolución o Generación Tecnológica de la Economía, una Cuarta Revolución Industrial, una *Digital Transformation* o, como voy a decirle, un comercio electrónico "*Reloaded"* -con la nube, el auge del *Blockchain*, el fenómeno de la inteligencia artificial, la 3D, la robótica y, la incesante aparición de aplicaciones y plataformas que pretenden facilitarnos o, incluso, alterarnos la vida- sienta ese *back to basics*, al trazar las líneas de acción para el desenvolvimiento del actual Derecho del comercio electrónico. Es decir, pese al despertar tecnológico, el Comercio electrónico, requerirá forzosamente, de su auxilio y entendimiento, para arribar a un buen puerto.

[1] Doctora en Derecho Privado y de la Empresa. Universidad Carlos III de Madrid, España. Experta en Derecho Uniforme y Comercio Electrónico.

Las máximas a que hago referencia, son las siguientes:

a) La equivalencia funcional.
Este ápice, se levanta como la capacidad reivindicatoria que coloca en un mismo nivel de eficacia y eficiencia jurídica, al documento electrónico y al sentado en soporte de papel. De esa forma, a fin que las manifestaciones de voluntad y, las de ciencia y conocimiento, tengan impacto y razón de existir, no solo en la práctica, sino en el ámbito legal, no se negará validez ni fuerza jurídica a las comunicaciones por el simple hecho de encontrarse en soporte electrónico.

El Derecho, principalmente, el español, con el apoyo y la inteligencia del principal creador y precursor del DUCI en el mundo, el Catedrático de Derecho Mercantil, Rafael Illescas Ortiz, introdujo en el Proyecto de Ley de Reforma al Código Mercantil español, la noción de electronificación, que viene a establecer lo que me gusta llamar, la madurez del Derecho del comercio electrónico y de esa equivalencia. De esa forma, reza la propuesta ibérica lo siguiente:

> "*Electronificación: Toda declaración o acto referido a la formación, perfección, administración, cumplimiento y extinción de los contratos mercantiles podrá efectuarse mediante comunicación electrónica entre las partes y entre estas y los terceros, salvo disposición expresa legal en contrario. 1.- Siempre que la ley exija que el contrato o cualquier información relacionada con el mismo conste por escrito, este requisito se entenderá satisfecho si el contrato o la información se contiene en un soporte electrónico. 2.- La utilización de medios electrónicos en los contratos mercantiles ni requiere el acuerdo previo entre partes*".

b) La inalteración del derecho preexistente de obligaciones y contratos.
Este axioma, ordena que no deviene necesario el dictado de toda una nueva forma de disciplina jurídica, pues, en razón de la equivalencia entre las nociones de derecho que tradicionalmente se ceñían sobre las transacciones manuales y, las electrónicas, lo indispensable sería emitir normas marco o reformas específicas, para acoplar la entrada de las nuevas tecnologías al mundo del papel. Si bien esta guía es la que más resquemores ha despertado, tomando en consideración los ya muchos cambios que la revolución digital ha levantado, no solo a nivel de nomenclatura, sino, en razón de sus posibilidades prácticas y legales, es menester tomarlo en cuenta.

Veámoslo de esta forma. Hace no mucho, era una verdad innegable que el Derecho del comercio electrónico llenaría las lagunas de los órdenes decimonónicos, ello, toda vez que, hay factores que no van a cambiar por la intrusión de la tecnología en nuestra vida. Ahora bien, lo que se debe tener en cuenta en la actualidad, es que, ya hay temas electrónicos que no necesitan del soporte del derecho tradicional para existir.

c) La neutralidad tecnológica.
Es la tercera guía que quiero resaltar. Predica que en razón de las constantes creaciones tecnológicas -de hoy, de ayer y, de mañana- no nos podemos enlazar con una sola de ellas. Es necesario, para mantener un orden normativo actualizado, aceptar desde las tecnologías pasadas, hasta las futuras, en un ámbito neutral, que se desenvuelva en una amplitud tal, que no requiera de constantes cambios.

d) La vis expansiva.
El DUCI, en la persona del Catedrático Rafael Illescas, sienta otro aforismo. La vis expansiva. Esta máxima lo que propone es hacernos caer en cuenta que la transformación digital no sólo se acomoda en la economía, en el comercio y, en las ramas civiles y mercantiles de lo jurídico, sino que, va a abarcar a todas las disciplinas, acogiendo en su seno, con las modificaciones que se requieran, a la normalización propia del Derecho público, del penal, del administrativo, del constitucional, en fin, de la materia que se nos ocurra y, además de empapar a nuestra vida cotidiana, también, lo hará en cualquier profesión imaginable.

A *grosso* modo, sus fundamentos, guiarán también el destino de todo lo que nos rodea, siendo que más allá de la acostumbrada mención al *Internet of Things*, ya debemos pensar en el *Internet of Everything*.

e) Finalmente, al menos para lo que a este artículo concierne, tenemos la buena fe, como principio que proviene del derecho preexistente y, del cual, me reservaré algunos comentarios para el desenlace de este escrito.
En pleno contubernio con los principios referidos, también, existen elementos objetivos y subjetivos nacidos del DUCI, que complementarán y darán forma al Derecho del comercio electrónico. Ellos son las nociones de: iniciador, destinatario e, intermediario, todos de un mensaje de datos y; el internet y los sistemas de información, a los que ahora se pueden ir agregando otros elementos, como lo podrían ser, el *blockchain*, la inteligencia artificial y, la robótica, por ejemplo.

Además, el DUCI, aclara nociones tan importantes hoy día, como lo son lo que debe entenderse por escrito, firma, original, lo concerniente a la admisibilidad y fuerza probatoria de los mensajes de datos y las comunicaciones electrónicas, la conservación de los mensajes de datos, la formación y validez de los contratos, el reconocimiento por las parte de los mensajes de datos, la atribución de los mensajes de datos, el acuse de recibo y, el tiempo y lugar del envío y la recepción de un mensaje de datos. Lo dicho, solo para esbozar el contenido de la Ley Modelo de Comercio Electrónico, pero dejando abierto para su consideración que esta disciplina se encarga de dilucidar muchos más ámbitos y apartados, que no creo conveniente traer a colación acá, dada la dimensión de este estudio.

En consecuencia y, en relación con la primera parte de este escrito, nótese que en el título de este pequeño artículo aludo al *back to basics*, es decir, a la concientización de la importancia de los fundamentos del DUCI en el comercio electrónico para poder comprender, de manera cabal, la disrupción en que nos posiciona el mundo moderno.

Y es que, para comprender el funcionamiento del tan destacado y omnipresente *blockchain* y compañía, deviene, indefectiblemente necesario, dominar el Derecho de la contratación electrónica en sus más elementales cimientos.

Ahora, desde mi experiencia, puedo decir que la regulación y expedición de una Ley Marco sobre Comercio Electrónico, conteniendo las menciones al DUCI y a normalizaciones de avanzada, como la comunitaria y la española, muchas veces se transforma en un camino muy intrincado, sometido a intensos cuestionamientos políticos y comerciales, de parte del Estado

y de los actores del mercado; situación que como lo he advertido antes, podría perjudicar el libre y ajustado a Derecho, desenvolvimiento de los operadores de los mercados electrónicos internacionales, provenientes, sobre todo, de países en vías de desarrollo. Esto, pese a que en los foros mundiales que abordan temas relacionados con el comercio electrónico, ya se habla de lo que la jurista española y profesora titular de la Universidad Carlos III de Madrid, Teresa Rodríguez de las Heras, denomina la Segunda Generación de las Economías y los Mercados Digitales, a la que hice referencia al inicio. Este entramado, en criterio de la abogada, vendría a sugerir un replanteamiento de la forma en que actualmente, estamos pensando regular la revolución digital y sus bondades[2].

Pienso, entonces, cómo es posible que a estas alturas, muchos de nosotros nos estemos cuestionando aspectos legales propios de la primera generación de la economía digital, cuando ya los retos nos están llevando a otras dimensiones.

2) Los nuevos paradigmas de la revolución digital. En busca de la reducción de brechas

"Las olas tecnológicas vienen más frecuentes y cambiantes, pero la empresa promedio de América latina es un surfeador demasiado propenso a trastabillar o, peor aún, dejar pasar las mejores oportunidades del lucirse en el mar de competidores globales"
INCAE, Costa Rica

Retomando la idea esbozada en el apartado precedente, la aparición de sistemas como el *blockchain* y la inteligencia artificial -por mencionar solo dos, ello, obedeciendo al principio de neutralidad tecnológica-, nos provoca aún más cuestionamientos acerca de la forma en que debe erigirse este Derecho. Tengamos en cuenta que hace nada de lo que se hablaba era de la nube o el *cloud computing* y, del *big data*.

Nosotros, los abogados, como curiosos/expertos/apasionados/estudiosos del derecho que rige a las tecnologías de la información, dando seguimiento a los propios prodigios que inventan y crean las tecnologías en sí, debemos cuestionarnos algo crucial, hacia dónde vamos y en dónde estamos. Esto, se podría zanjar creando un mapa mental, actualizado con los últimos avances electrónicos, que contenga una visualización de lo que sería el futuro, acompañado por la forma en que vayamos a regular o no, estas novedades; tratando siempre de no alterar su libre desenvolvimiento.

Sin embargo, para nadie es un secreto que los Estados y sus organizaciones internas, para normalizar o ponerse de acuerdo en algo, deben ajustarse a intrincados procesos burocráticos, que por demás está decir, frenan el avance oportuno de la creación de cuerpos jurídicos legales que regulen, en lo que se estime necesario, el auge tecnológico. A ello se suma que la legalidad, ni por asomo, puede transitar a la misma velocidad que lo hace la tecnología.

[2] Rodríguez de las Heras Ballel, Teresa. Conferencia magistral impartida en el V Congreso Internacional sobre Derecho Uniforme y Comercio Electrónico, llevado a cabo el 8 de junio de 2018 en el Colegio de Abogados de Costa Rica.

Los servicios de la sociedad de la información y sus respectivas plataformas, no solo se vuelven cada vez más sofisticados y demandantes, sino que, plantean desafíos y situaciones que nos pueden conducir a un replanteamiento de los dogmas legales y de los mapas jurídicos que hemos seguido durante tantos años y, que creíamos inescrutables.

Tan es así que en el marco de la responsabilidad de los prestadores de servicios de la sociedad de la información, que desde el año 2000 contempla la normativa comunitaria, según el texto de la Directiva 2000/31 relativa a determinados aspectos jurídicos de los Servicios de la Sociedad de la Información y, del 2002, acorde con la Ley 34/2002 de España, de Servicios de la Sociedad de la Información y de Comercio Electrónico, ya hoy, a más de 16 años de su vigencia, se está pensando reformar, a fin de incluir a los prestadores de servicios de intermediación en un rol más activo dentro de sus funciones, a fin que no solo se vean compelidos a eliminar los contenidos que alojen provenientes de iniciadores que utilicen sus servicios hasta que se percaten de su ilicitud o de su ilegalidad, o bien, en el momento en que las autoridades administrativas y jurisdiccionales se los impongan; sino que la nueva tendencia, rompedora de paradigmas, según información suministrada por la profesora Teresa Rodríguez de las Heras, busca que estos participantes electrónicos concursen de manera proactiva y, se vean inducidos a implementar mecanismos para revisar de manera constante, tanto, los contenidos que alojan en sus plataformas, como los datos que por su intermedio transiten.

Sé que este foro está dirigido a Iberoamérica, lo que hace que la disparidad de culturas, legislaciones y, puntos de vista, prevalezcan. A nivel europeo y, a lo que a España concierne, con el soporte que brinda la Unión Europea y la cantidad de Estados que colaboran en el pensamiento normativo que rige y, regirá a futuro los mercados electrónicos, llegamos a un vértice indiscutible. La calidad de sus normas, tanto las transpuestas, como las que entren directamente a regir en su ordenamiento interno como leyes europeas -caso de los Reglamentos Comunitarios- son por mucho, superiores a las que surgen en América Latina.

Es más, la aplicación de la normativa comunitaria, gozará de una riqueza interpretativa jurídica innegable, al provenir de las distintas jurisdicciones que engrosan los países miembros del entorno comunitario, a lo que se suma, la existencia de Tribunales Europeos.

De ahí que, sería conveniente que países como los nuestros, para progresar y estrechar las brechas que nos separan de otras latitudes, tomáramos nota de la experiencia comunitaria, del DUCI y, en fin, de potencias como los Estados Unidos de Norteamérica, con el cometido de acceder de manera adecuada y segura al mercado internacional electrónico. Cómo, reduciendo la brecha normativa y tecnológica que nos separa.

3) Podría el Derecho dirigirse a una encrucijada y caer en un fin apocalíptico en el ámbito de la electrónica? Puntos de colusión y posibles soluciones

Desde el momento en que las transacciones electrónicas no respetan las fronteras de las naciones; pulula la disparidad de las legislaciones y de las idiosincrasias nacionales; las tecnologías avanzan de forma imparable y, a veces, impredecible; crece el desconocimiento de los operadores legales hacia sitios práctica y jurídicamente in-escrutados; aumenten los vacíos y las lagunas legales; nos encontremos ayunos de mecanismos internacionales capaces

de satisfacer las exigencias de la Cuarta Revolución Industrial, y; residamos en un mundo donde el Derecho Internacional Privado ya no se prevé como una solución viable o suficiente; deviene necesario crear un nuevo mapa que nos conduzca a la mejor solución posible.

De ahí que, ante el "vaticinio" de un futuro un tanto apocalíptico para las economías latinoamericanas y, lo mismo, para su mundo normativo, propongo una serie de soluciones que, estimo, podrían favorecernos. Empero, dado mi profesión -abogada-, me limitaré en este artículo a esgrimir respuestas ligadas al campo jurídico.

Las recomendaciones a este respecto, serían las siguientes:

a) La uniformidad y homogeneidad de las legislaciones. Mi mundo ideal.

"Las incompatibilidades jurídicas y técnicas son las dos causas principales de dificultades en la utilización transfronteriza de los métodos de firma y autenticación electrónicas, en particular cuando su finalidad es sustituir una firma legalmente válida. Las incompatibilidades técnicas son las que afectan a la interoperabilidad de los sistemas de autenticación. Las incompatibilidades jurídicas pueden surgir cuando las leyes de los diferentes ordenamientos estipulan diferentes requisitos en cuanto a la utilización y la validez de los métodos de firma y autenticación electrónicas (…) El riesgo que distintos países adopten criterios legislativos diferentes en relación con las firmas electrónicas exige disposiciones legislativas uniformes que establezcan las normas básicas de lo que constituye en esencia un fenómeno internacional, en el que es fundamental la armonía jurídica y la interoperabilidad técnica".
***Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la utilización internacional de métodos de autenticación y firmas electrónicas. CNUDMI/UNCITRAL, 2009*.**

Uno de los objetivos a perseguir, es lograr que en el mundo se maneje un lenguaje común, de talante electrónico, donde la nomenclatura sea de uso general y de conocimiento de sus operadores. Además, donde lo tocante a las ordenanzas sobre protección y tratamiento de los datos de carácter personal, los terceros de confianza, los derechos y deberes de los cuales gocen las partes que participen en las transacciones electrónicas, el derecho de consumo, los derechos humanos como prerrogativas de cuarta o quinta generación -sin ánimo de ser excluyente en mis menciones-, se estandaricen.

Esa precisamente ha sido la misión y el objeto del DUCI, en manos de la CNUDMI/UNCITRAL, desde hace más de 50 años. Misión cuyo valor no puede ser negado ni desconocido, pues, a través de Convenciones internacionales, leyes modelo y guías jurídicas que han favorecido la incorporación de sus atestados a los órdenes internos de gran cantidad de naciones, no ha hecho más que beneficiarnos y brindar a muchos países en vías de desarrollo, de órdenes jurídicos de avanzada. Ahora bien, en el ámbito en que nos desenvolvemos ahora, extendería esa misión hasta el orden procesal y otras ramas en las cuales esta ordenación ha preferido no inmiscuirse.

Pensemos esto. Si todos habláramos y entendiéramos un lenguaje común, en un tema donde la nota preponderante es y, siempre será, su carácter internacional y el rompimiento de fronteras, no dudo que viviríamos en un sistema más organizado, menos complejo, más complaciente y, menos plagado de conflictos, dudas y resquemores. En este espacio quimérico que propongo, ya ni siquiera sería necesario el Derecho Internacional Privado.

Voy más allá, noten ustedes que en este universo de la homogeneidad, no estoy proponiendo necesariamente que los países y las naciones nos unamos en un Estado supranacional; para nada. Simplemente, creo que el mundo debería marchar en esta materia por un mismo rumbo, en el que los países más desarrollados y avanzados colaboren con los que nos encontramos en vías de desarrollo, para que esa brecha digital y legal que nos separa, desaparezca o, al menos, se reduzca.

Pero bueno, esta solución de equidad no se encuentra alejada de la realidad. Ya la Unión Europea la ha puesto en práctica y, ha funcionado. Es acá donde resaltan las Directivas comunitarias y los Reglamentos europeos. Además, el mundo de la autorregulación y de los códigos de conducta, grandes aliados en el tema de la electrónica, han sido y seguirán siendo, de gran soporte.

b) No sobre-regular o regular en exceso.

Hace al menos 20 años, algunos visionarios, como en su momento lo fue Santiago Muñoz Machado, habló de tres posibilidades regulatorias, enrumbadas al sistema de información conocido con el nombre de Internet, la red de redes.

La primera, proponía que este ámbito debía permanecer in escrutado, sometido a su libre desenvolvimiento en un ambiente de libertad plena y, de libre circulación de ideas y mensajes.
La segunda, se decantaba por normar algunos extremos que se previeran de interés, a fin de brindar un flujo adecuado y continuo entre la prestación de servicios y, la protección de los usuarios de la red.
Por último, la tercera propuesta, sugería la necesidad de crear un régimen jurídico extremo, que contuviera cualquier posibilidad de abuso en el uso de las tecnologías de la información.

Con el paso de los años y, con los cambios y quebrantos sufridos por el principio de inalteración del derecho preexistente, podemos decir que ya tenemos un panorama un poco más prístino, que ha ido evolucionando en un vaivén de prueba y error, que ha provocado la reforma, derogación, evolución y, cuestionamiento, de muchas de las reglas primigenias vertidas en para ámbito. En este punto no quiero dejar de mencionar que el único Derecho, que ha permanecido incólume en el tiempo, con apenas alguna variación o modernización, lo ha sido el Derecho Uniforme; lo que no es otra cosa que prueba fiel de su calidad y consistencia.

Pasando a otra idea, hay que tener mucho cuidado con la doble regulación, es decir, con la expedición de reglas contenidas en varios cuerpos normativos que, al final de cuentas, pretendan normar lo mismo.

Otra circunstancia a tomar en cuenta, es que, con la expedición de este tipo de ordenaciones, debemos, en lo posible, brindar un cierto estatus de libertad al desenvolvimiento tecnológico, en la plataforma que se presente.

Por mencionar algo, se sabe que el *blockchain* abastece de grandes beneficios al ecosistema digital. Bajo esa tesis, podemos mencionar la reducción de costes; la emulación de

transacciones seguras; la factibilidad de rescindir de la intercesión de terceros de confianza; la trazabilidad; la encriptación segura de las comunicaciones electrónicas; la transparencia, y; la creación de los denominados *smart contracts* en la modalidad que se quiera. Ante un panorama como el descrito, la perspectiva regulatoria podría decantarse hacia un marco de neutralidad -DUCI-, que se enfoque en las actividades desplegadas por los usuarios y, que tome en consideración los potenciales riesgos operacionales, como los que puedan suscitarse del tratamiento de datos personales.

Asimismo, en el caso de países que en la actualidad, no gocen de marcos legales suficientes en esta disciplina, recomiendo, acogerse a las prédicas del DUCI, mismas que han sido, con éxito, sometidas a prueba por más de 20 años, superando con creces las expectativas que imagino, pudieron haber vaticinado sus creadores. Además, en virtud de las novedosas determinaciones vertidas en esa sede, resulta potable tratar de ponerse a día en la transposición a sus órdenes internos, de esas regulaciones, en este caso, de la Ley Modelo de Documentos Electrónicos Transmisibles de la CNUDMI/UNCITRAL, aprobada hace apenas un año y, en la cual, se plantean y se brindan soluciones a temas que recién fueron puestos en entredicho.

c) Valorar la capacidad de los mecanismos de autorregulación.

Los códigos de conducta, devienen herramientas básicas en la sostenibilidad y desarrollo de los servicios de la sociedad de la información, en especial, en un mundo, donde las plataformas y los mercados a los que pertenezcamos –piénsese desde *Facebook* hasta *Waze*- nos convierten, a nosotros, los seres humanos, en habitantes de una comunidad virtual que, si bien debe respetar el orden público y las normas dispositivas de los Derechos internos, se rigen por sus propias reglas y, hasta contienen sus propios mecanismos de solución de controversias.

d) Combinar las bondades regulatorias del *back to basics* y las necesidades de la Segunda Generación de los Mercados Digitales. La confianza: a propósito de la buena fe, como fiel expresión del principio sobre inalteración del derecho preexistente obligaciones y contratos.

Finalmente, quisiera agregar a lo dicho, que la modernidad nos conduce a transitar por caminos que antes no habíamos considerado. De nuevo, quiero citar a la maestra Teresa Rodríguez de las Heras y, retomar el principio del DUCI que predica la buena fe.

La buena fe, proviene nada más y nada menos, que del principio de inalteración del derecho preexistente y, en los tiempos que corren, ha adquirido una transcendencia impactante que nos reta a nosotros, a todos, como usuarios de las tecnologías de la información, a dejarnos caer en manos de las bondades y beneficios del entorno digital.

Les comento. Hace casi 10 años -este vórtice no se ha resuelto-, surgían una gran cantidad de dudas e inconsistencias en la utilización de las firmas electrónicas, a raíz de la disparidad de ordenaciones jurídicas y los problemas en el reconocimiento de las rúbricas electrónicas extranjeras, a tal punto que la CNUDMI/UNCITRAL publicó un excelso y revelador texto titulado “Fomento de la confianza en el comercio electrónico: cuestiones jurídicas de la

utilización internacional de métodos de autenticación y firmas electrónicas", del cual, se extrajo una cita textual para ilustrar uno de los acápites previos.

Dentro de uno de sus apartados, se hizo referencia a la confianza y, en ese sentido se estatuyó lo que de seguido se transcribe:

> "*Aunque una firma manuscrita es una forma habitual de "autenticación" y sirve para documentos de transacción que cambian de manos entre partes conocidas, en muchas situaciones comerciales y administrativas una firma es sin embargo relativamente insegura. La persona que confía en el documento no suele disponer de los nombres de las personas autorizadas a firmar ni de especímenes de sus firmas a efectos de comparación. Esta situación es especialmente cierta en el caso de muchos documentos en los que se confía en países extranjeros en operaciones comerciales internacionales. Incluso cuando existe un espécimen de la firma autorizada con fines de comparación, tan solo un perito podrá detectar una falsificación bien hecha. Cuando se tramita un gran número de documentos, a veces ni siquiera se comparan las firmas, salvo cuando se trata de operaciones muy importantes. La confianza es uno de los elementos básicos de las relaciones comerciales internacionales*".

De nuevo, la sapiencia de la CNUDMI/UNCITRAL salta a la vista. La electrónica, a parte de sus implicaciones y evocación de la distancia entre las partes que la utilizan, muchas veces brinda más seguridad a las transacciones que se gestan por su intermedio, que sus homólogas del papel.

La práctica y el paso del tiempo, llevaron a la Unión Europea a dictar el Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y, los servicios de confianza para las transacciones electrónicas en el Mercado Interior y por la que se deroga la Directiva 1999/93/CE.

Dicho entramado, en suma técnico y complejo, crea la disciplina jurídica que va a girar sobre los prestadores de servicios de confianza, los sellos electrónicos y de tiempo y, las firmas electrónicas.

De manera paralela a iniciativas como la mencionada, la tecnología nos está conduciendo a otros rumbos y, acá menciono la idea esbozada por la profesora Rodríguez de las Heras. Pese a que es inevitable requerir la intervención de los terceros de confianza, ahora, convivimos en ecosistemas que predican que los propios participantes de la electrónica, es decir, los prestadores de servicios, se involucren y coadyuven en a generación de la confianza, sin necesidad, muchas veces, de acudir al auxilio de esos otros prestadores de servicios de confianza.

4) A manera de conclusión

Las posibilidades que la vida nos da en este siglo, son infinitas y, debido al auge electrónico, difíciles de predecir.

En mi criterio, creo que lejos de mostrar miedo y limitar nuestro actuar virtual, debemos disfrutar de los regalos que la modernidad nos regala, desplegándonos como lo hacemos siempre y, en el mundo real, con cautela.

Es aconsejable que los legisladores, gobernantes y los actores comerciales, abran sus mentes y faciliten la inserción de normas nacionales basadas en el DUCI y en las reglas internacionales testadas a través de los años, para evitar caer en una separación que en algún punto, fortalezca y haga crecer aún más, la brecha digital-jurídica que ya nos separa de otras latitudes.

FEDATARIO INFORMÁTICO Y LA SEGURIDAD EN MEDIOS ELECTRÓNICOS

Por: ***José Francisco Espinosa Céspedes***
Perú

I. Introducción

Desde sus inicios la seguridad aplicable a los centros de documentación, información y cómputo estaba centrado en el uso de elementos materiales como el hardware; es una realidad que en la actualidad en ámbitos físicos se colocan cadenas, candados y hasta rejas para lograr un determinado nivel de seguridad.

Lo antes señalado ha cambiado radicalmente por la gran demanda generada por el uso de las computadoras, los grandes servidores integrados y la aparición de la fedatación informática, entendida como aquella actividad profesional realizada, tanto por medios físicos como por contextos electrónicos, por un dador de fe pública denominado fedatario juramentado, profesional conocido en el mercado como fedatario informático, el mismo que en el marco de las potestades legales concedidas por el Estado peruano se encuentra facultado y capacitado para el otorgamiento de fe pública sea a nivel de operaciones de conversión de papel a digital (papel- digital) como en actividades netamente digitales partiendo de cualquier elementos inmaterial en formato digital para convertirlo a un documentos digital con pleno valor legal (digital – digital); ámbito que frecuentemente se ve afectado por una serie de ataques realizados por Hackers, Crackers, Preakers, etc.

Sobre el particular es importante tener en cuenta que el Hacker es "(…) el nombre genérico [de] los intrusos informáticos, pero en realidad el hacker es el único de ellos que tiene un código ético para sus intrusiones (…) conoce (…) los lenguajes de programación, las intrusiones y los protocolos (…)" (Aguilera, 2010, p. 109).

En relación con el cracker se ha determinado que es "(…) el siguiente eslabón y por tanto el primero de una familia "rebelde". Cracker es aquel fascinado por su capacidad de romper sistemas y software y que se dedica única y exclusivamente a crackear sistemas" (Corletti, 2011, p. 485). En el marco de sus actividades y acciones el Cracker se caracteriza por tener alguna finalidad, por ejemplo hacer daño u obtener una ventaja económica.

II.- Fedatación informática, riesgos y contingencias a nivel físico y lógico

Debido a la existencia de los atacantes e intrusos en medios tangibles surge el concepto de se seguridad física cuya tarea esencial y fundamental está centrada en buscar protección integral para todos los recursos vinculados con la infraestructura tangible, material o física que puedan estar sometidos a determinado tipo de amenaza; para tal efecto, debe tenerse en cuenta que a nivel de los controles físicos aplicables a la

Fedatación informática estos necesariamente deben estar autenticados con la finalidad de proteger al recurso humano, las instalaciones y a toda la infraestructura tecnológica.

Entre las amenazas a la seguridad física en un contexto de fedatación informática, tenemos aquellos índole natural como los huaycos (deslizamientos de grandes cantidades de agua, lodo, piedras y árboles), terremotos, tsunamis, inundaciones; diversos tipos de cataclismos como tormentas, ciclones, paracas, etc., pero debe tenerse en cuenta que también existen circunstancias generadas por el actuar el ser humano como los hurtos, robos, manifestaciones violentas, rebeliones populares que incendian centros de cómputo, servidores y centros laborales completos; con las consiguientes secuelas de pérdida de equipos y hasta la afectación a todo tipo de acceso a energía.

En ese orden de ideas, para la permanencia de la fedatación informática en el tiempo debe planificarse el uso de diversos tipos de respaldo y contingencia a nivel de seguridad física que permitan otorgar una real y eficiente garantía para lograr la continuidad del servicio iusinformático por medios electrónicos. (García-Cervigón & Alegre, 2011).

Lo mismo sucede a nivel de los elementos lógicos, los mismos que también deben ser materia de resguardo mediante la contratación de los mecanismos de seguridad que impidan que tanto hackers como crackers puedan incursionar con facilidad, y si por deficiencias técnicas logran vulnerar la seguridad puedan ser detectados a tiempo a fin de evitar la afectación a los datos, información y conocimiento de los fedatarios informáticos.

Al incursionar en materia de fedatación informática debemos estar conscientes sobre la generación de una serie de riesgos, los mismos que pueden ir desde la interrupción del servicio por daño físico o por afectación a nivel lógico (elementos inmateriales como el software), hasta la existencia de diversos actos de filtración de información a nivel interno o externo, así como la existencia de serios compromisos de seguridad que pueden afectar los elementos vitales generados en el tiempo a nivel de las diversas actividades del giro del negocio electrónico.

En el ámbito de los mecanismos de seguridad aplicables a los fedatación informática es necesario prever las posibles contingencias que puedan afectar a la seguridad lógica, como se expresó anteriormente, a fin de asegurar las operaciones típicas de los fedatarios informáticos.

En contextos informáticos debe tenerse en cuentan que los atacantes pretenden afectar las operaciones y transacciones, para tal efecto no requieren estar físicamente y presencialmente en el lugar de ataque o en el lugar donde se ejecutará la acción de criminalidad informática, por tales consideraciones hoy las empresas que actúan en el medio electrónico requieren utilizar adecuada seguridad lógica para proteger las diversas redes, entre ella las redes WiFi.

Según Espinoza (2018), por lo general en contextos técnicos se expresa comúnmente la necesidad de tener una actitud previsora respecto de lo que pueda suceder a nivel de las transacciones y operaciones electrónicas, teniendo en cuenta que la seguridad adquirida

para un año de trabajo puede verse vulnera sin problemas en un solo día y sobre todo, mucho antes de que el sistema haya cumplido por lo menos un mes de funcionamiento.

Así como es necesario tener elementos de seguridad a niveles físicos, es fundamental tener criterios y políticas seguridad para los elementos lógicos a nivel del software, redes, comunicaciones, bases de datos y cualquier otro que requiera protección en el ámbito de las comunicaciones al interior de las organizaciones vinculadas con la fedatación informática en general.

Para tal efecto, se deben cumplir una serie de principios o premisas básicas y fundamentales relativas a la generación de espacios de alta integridad, que impida la modificación o alteración de todos los datos, informaciones y comunicaciones almacenadas, donde un elevado nivel de confidencialidad son la prioridad absoluta; esto elementos deben estar matizados con altos estándares de disponibilidad a fin de tener acceso al negocio electrónico las 24 horas los 7 días de la semana y los 365 días del año, así como a toda la información almacenada pero cuidando que la misma no vaya a ser objeto de repudio y por lo tanto no aceptada por los receptores de la misma ni por el propio sistema, para tal efecto el uso de las firmas y certificados digitales es de vital importancia. (García-Cervigón & Alegre, 2011).

En el medio electrónico no menos importante es la aplicación de criterios de autenticación que permitan determinar la autoría de documentos, datos, y operaciones electrónicas; todo ello debidamente monitoreado con los mejores elementos lógicos existentes en el mercado digital que permitan generar un entorno de trazabilidad, de tal forma que casa paso, huella o acceso al sistema de fedatación informática quede debidamente registrado.

Con las implementando adecuados mecanismos de seguimiento y rastreo de operaciones electrónicas al interior del sitio definido para los fedatación informática se genera un entorno de confianza para que los proveedores y clientes operen con tranquilidad y seguridad a la hora de realizar transacciones a nivel de las redes abiertas que por su naturaleza son inseguras.

III. Aproximaciones a la seguridad informática en el contexto de la fedatación juramentada.

En el marco de la seguridad informática, es fundamental que los sistema estén preparados para prevenir tanto a los fedatarios informáticos como a los jefes de seguridad sobre cualquier alteración o cambio en los valores hash de los datos, información o conocimiento almacenado en bases de datos, servidores o en aquella almacenada en la nube y en tránsito. (Aguilera, 2010).

En todo momento los elementos de seguridad deben estar en condiciones de comunicar al fedatario informático y al personal de sistemas sobre cualquier tipo de alteración o modificación a todo o a parte de los bienes almacenados en servidores, discos duros, memorias externas y hasta en la nube (también conocido como el cloud computing

también conocido como computación en la nube por las diversas operaciones que se pueden hacer en contextos netamente electrónicos.

Debe tenerse en cuenta que en toda línea de producción donde actúa el Fedatario Informático para elaboración de microformas, por ser un lugar con información sensible, se deben hacer todos los esfuerzos para lograr altos niveles de confidencialidad y seguridad para los elementos informáticos y tecnológicos, siendo fundamental crear perfiles que permitan obtener una autenticación combinada, donde se utilicen diversos mecanismos de seguridad técnica que permitan alcanzar altos estándares de confidencialidad.

A fin de evitar pérdidas de información en las líneas de producción de microformas siempre es importante tener elementos tanto físicos como lógicos que permitan tener disponible toda los datos e informaciones que se requieran para la continuidad del servicio de fedatación informática, en dicho contexto es muy común que puedan ocurrir ataques de denegación de servicio, con lo cual sino se tienen copias, respaldos y vías de acceso a la información por diversos canales se podría estar afectando el principio de disponibilidad.

Para salvaguardar las plataformas de producción de microformas es necesario estar preparados para aplicar técnicas de defensa informática, por ejemplo utilizando diversos discos redundantes que funcionen como espejos o copias de seguridad (backup de respaldo) tanto de servidores como de discos duros en concordancia con el Decreto Legislativo Nº 681, modificado por la Ley 26612, norma esta última que permite las operaciones de Fedatación de Digital a Digital. (Espinoza, 2010).

Para efectos de la implementación de las microformas y la fedatación informática en el contexto de las entidades de la administración pública, es de aplicación lo dispuesto por el Decreto Legislativo N° 827, norma que dispone los aspectos fundamentales para el proceso de modernización del sistema de archivos oficiales en el ámbito estatal.

En contextos informáticos aplicables a la fedatación informática, deben contratarse servicios o sistemas que impidan el no repudio de las operaciones generadas durante el desarrollo de las actividades en medios electrónicos, previendo tener los elementos necesarios para impedir que los usuarios, proveedores y terceros con quienes nos relacionemos que vayan negar las operaciones que han realizado en el site o sitio de fedatación informática, además al prever mecanismos para el no repudio o no rechazo de nuestras operaciones por medios electrónicos deben preverse mecanismo que permitan conocer la posición o localidad de los usuarios, estando en capacidad de determinar la procedencia de la demanda, los medios de interacción electrónica, los ámbitos territoriales de acceso, las preferencias, los gustos, etc.

La unión con los mecanismos de trazabilidad o registro de las operaciones realizadas en nuestro sitio de fedatación informática y las actividades efectuadas mediante el uso de elementos lógicos estarán debidamente monitoreadas y aseguradas.

Por ejemplo, cada vez que se comunican con nosotros por correo electrónico, en base a lo antes planteado, estaremos generando un entorno seguro que nos permita determinar toda la información posible de quienes interactúan con nosotros, utilizando para tal efecto diversas facilidades lógicas disponibles en la red.

Generando un entorno de seguridad y bajo el principio de autenticación informática o electrónica estamos en posibilidad de conocer datos e informaciones de personas físicas o jurídicas a través de la interacción digital de sus representantes debidamente acreditados, todo ello gracias a la determinación específica del comportamiento digital de todos los que se hayan autenticado al site de fedatación informática. Todo ello a partir del ámbito de operaciones de producción de microformas de digital a digital.

La autenticación de los usuarios del sistema de Fedatación Informática permite determinar la identidad física de las personas que luego puede ser traducida, comprendida o identificada a través de su correspondiente identidad digital; se genera una transmutación técnica de una persona física a una identidad digital plenamente definida, conocida e identificada. De ahí la importancia de contar con mecanismos que soliciten determinado nivel de autorización y autenticación para realizar determinadas actividades en el negocio electrónico con la finalidad de tener un adecuado nivel de control de accesos. (Espinoza, 2018).

En el mundo de las operaciones relativas con la Fedatación Informática es importante generar un mínimo de privilegios que permitan determinar las actividades de los sujetos que visitan el entorno de producción de microformas o realizar determinados procesos entorno a él, como búsqueda de información, solicitud de información, etc.; acciones que deben ser complementadas con la implementación de ciertos mecanismos que permitan monitorear los objetos que circulan por el negocio tanto a nivel de procesos como de archivos.

El otorgamiento de permisos y privilegios no pueden entregarse indiscriminadamente sin mayor interés por el correspondiente sustento, sino que por el contrario debe fundamentarse el porqué de dicha necesidad, lo importante es que todos los privilegios y permisos sean entregados solo en la medida de lo necesario, no se debe dar más de lo requerido, ni menos de lo necesitado.

En la fedatación informática debe emplearse el ámbito de valor por omisión seguro, es decir que los Fedatarios Informáticos y los administradores de los componentes tanto físicos como lógicos deben implementar por práctica y estándar generalizado la denegación de mayores privilegios a quienes lo soliciten y solo facilitar el acceso a mayores facilidades cuando exista un real sustento del requerimiento o la necesidad por ser atendida, de tal forma que sea muy difícil que alguien logre acceso a zonas que no le competen, que no requiera o que no se vinculen con sus funciones.

En el ámbito de la Fedatación Informática debe trabajarse, por ejemplo, a nivel de los Firewalls negando todo acceso, salvo que se otorgue en forma independiente cada uno los permisos correspondientes por necesidad del servicio para los usuarios del sistema de Fedatación Informática; en dicho contexto debe tenerse en cuenta que una vez

generado el permiso el proxy se encargará de encaminar el acceso por la parte de la red a la que se haya autorizado el permiso y sobre todo el acceso a los recursos (Espinoza, 2000).

Para generar adecuadas medidas de seguridad a nivel de la Fedatación Informática es necesario bloquear todos los acceso y solo permitir el ingresos de quienes lo soliciten con el debido fundamento técnico, en el marco de las funciones del manual de producción de microformas, es decir aquellas acciones que se encuentren vinculadas con las necesidades reales de las operaciones relativas a la Fedatación Informática; sobre todo es preferible ir configurando la conectividad a solicitud y previo análisis de los reales sustentos, a dar acceso a todo el personal en forma indiscriminada porque luego tornará más complicado ir configurando y bloqueando a todos los usuarios.

La seguridad del negocio electrónico tendrá razón de ser y será más eficiente si se cierran todos los accesos y puertos por donde puedan presentarse ataques, para tal efecto es eficiente generar valores por omisión seguros, de tal forma que sea transparente y amigable para el usuario y no tenga que realizar tales actividades con la finalidad de dejar al sistema con un alto grado de confiabilidad y seguridad informática.

En todo contexto de la fedatación informática es fundamental ir hacia un contexto de implementación de seguridad en un ámbito de la denominada economía del mecanismo, que se vincula con implementar mecanismos de seguridad que sean lo más simple posible, es una tendencia va contra todo ámbito complejo, se podría decir que es una tendencia totalmente enemiga de la complejidad; en ese sentido se propone que todo lo simple, se caracteriza por ser adecuadamente administrable.

En ese orden de ideas el enfoque de la economía del mecanismo aplicable a la Fedatación Informática busca dejar de utilizar aquellos programas que no son necesarios para el logro del objetivo, y además se procede al cierre de todos y cada uno de los puertos que no sean de utilidad o no sean requeridos para que los elementos intangibles puedan operar sin problemas.

Para desarrollar elementos lógicos pensados en la fedatación informática, es importante destacar que se debe realizar un diseño cerrado, es decir que los componentes inherentes al propio sistema deben mantenerse bajo reserva para dar cumplimiento a las normas técnicas sobre fedatación informática; deberá aplicarse para los diversos procesos criptografía como medida de seguridad, el mecanismo criptográfico solo debe ser conocido por los titulares, de no hacerlo se generará un entorno de inseguridad y oscuridad que afectará directamente la propia seguridad que se pretendió generar (Espinoza, 2010).

En ese orden de ideas, existen opiniones especializadas que indican que todo software incluido aquel desarrollado para los fedatación informática deben ser evaluados por especialistas y expertos a fin de determinar si es posible que puedan ser vulnerados, por lo tanto, debemos ser conscientes que los sistema no puedan ser puestos al servicio de las empresas e instituciones que requiere hacer fedatación informática sin haber sido

evaluados previamente, con la finalidad de evitar posibles vulneraciones o ataques por no haberse evaluado adecuadamente los elementos inmateriales.

Un principio importante aplicable a la seguridad a la Fedatación Informática es la separación de funciones, de tal forma que los criterios técnicos que deban implementarse deben ser por lo menos dos mecanismos de seguridad del tipo multifactores, por ejemplo, el uso de firmas digitales combinadas con los rasgos biométricos o la implementación de firmas biométricas.

Para efecto del acceso a redes, especialmente para los fedatación informática debe aplicarse el principio de menor mecanismo común, de tal forma que los accesos sean cada vez menos predecibles a terceros y se pueda prevenirse de esta forma algún tipo de ataque, y de no ser evitable el ataque por lo menos se tendrá un tiempo determinado para evitar el ataque, reconocer el mismo e implementar las medidas de seguridad más adecuadas. (Espinoza, 2018)

En ese sentido en materia de seguridad vinculada a la Fedatación Informática debe tenerse en cuenta las relaciones de seguridad versus usabilidad, en el sentido de tener en cuenta que a mayor seguridad se tendrá menos usabilidad y que a mayor usabilidad se tendrá menor seguridad; debiendo para tal efecto buscar un justo medio o un adecuado nivel de equilibrio entre ambos conceptos.

Lo mismo puede aplicarse para la habilitación de puertos, es decir que estos pueden habilitarse para el acceso a los sistemas, con adecuados sistemas de trazabilidad, pero es muy importante no relajar la seguridad del entorno. Se dice por ejemplo que existe la figura de la aceptación psicológica, en el sentido que siempre existirá gente capaz de buscar evitar los diversos aspectos de la seguridad informática, buscando acceder a los sistemas, equipos y redes por donde no hay adecuados mecanismos de seguridad o por donde ésta no existe. Por eso debe tenerse en cuenta que todo diseño de sistemas para la Fedatación Informática debe tender a ser lo más usable posible, pero en un ambiente donde existan las adecuadas medidas de seguridad.

IV. Conclusiones

1. La Fedatación Informática requiere de elementos materiales e inmateriales que deben asegurarse mediante las técnicas y metodologías provenientes de la seguridad informática.

2. Siempre debe tenerse en cuenta que, en todo contexto de Fedatación Informática a nivel de recursos informáticos, el usuario final en las plataformas de producción de microformas es el eslabón más débil de la cadena de seguridad, quien por descuido puede ser utilizado como medio para generar ataques o intrusiones en cualquiera de los procesos generados al interior de las referidas plataformas para la generación de microformas, en un contexto de valor legal y fe pública, de ahí la necesidad de

capacitar en materia de seguridad a todo el personal que participa en las líneas de producción de microformas.

3. El ejemplo típico de inseguridad en las plataformas de producción de microformas se presenta cuando se entregan claves seguras a los usuarios y estos en lugar de aprenderlas, las anotan en algún soporte material, hecho que debe evitarse, enseñando para tal efecto al personal diversas técnicas de memorización de claves para impedir la generación de inseguridades al sistema de producción de microformas.

4. Por la existencia del fenómeno de la aceptación psicológica en el ámbito de los sistemas, esta debe ser superada con la formación del personal de las líneas de producción de microformas en materia de seguridad informática.

5. Si bien es cierto que no existe seguridad informática total o al cien por ciento, en vista que las herramientas informáticas evolucionan y los atacantes también, es importante entender que la seguridad informática no puede estar centrada en un solo aspecto o ítem. En ese sentido, no debe dejarse de lado ningún aspecto técnico, formal o jurídico que permita a los atacantes afectar la seguridad de las plataformas de producción de microformas.

V. Referencias bibliográficas

Aguilera, P. (2010). *Seguridad Informática.* Madrid: Editex.

Corletti, A. (2011). *Seguridad por Niveles*. Madrid: DarFE.

Espinoza, J. (2000). *Contratación Electrónica, Medidas de Seguridad y Derecho Informático*. Lima: Editora RAO S.R.L.

Espinoza, J (2010). *El Derecho Informático Frente a la Contratación Pública Electrónica.* Recuperado de http://biblio.juridicas.unam.mx/libros/6/2940/19.pdf

Espinoza, J (2018). *Aspectos Fundamentales en relación con la Prueba Electrónica*. Recuperado de www.asider.pe

García-Cervigón, A y M, Alegre (2011). *Seguridad Informática.* Madrid: Paraninfo, S.A.

VI. Regulación

- Decreto Legislativo Nº 681(1991). Dictan normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras.

- Decreto Legislativo Nº 827 (1996). Amplían los alcances del D. Leg. Nº 681 a las entidades públicas a fin de modernizar el sistema de archivos oficiales.

- Ley Nº 26612 (2006). Modifican el D. Leg. N° 681, regula el uso de tecnologías avanzadas en materia de archivo de documentos e información

ALGORITMOS: Los datos ocultos tras las redes sociales

Por: ***Alexis German Antoniucci Luz Clara***
Argentina

I. INTRODUCCION:

En la mayoría de los países existen legislaciones que protegen los datos de forma amplia pudiendo abarcar aquellos que son producto de las interacciones de los usuarios de distintas redes sociales.

En el caso de Argentina la ley 25.326, es clara al momento de individualizar y proteger los datos personales. Lo que muestra es una clara identificación de las redes sociales equiparándola a una base, registro, archivo o banco de datos. Art.2 *"[…]Archivo, registro, base o banco de datos: Indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso. […]"*

Los datos que son recolectados por las diferentes funciones que tienen cada una de las aplicaciones y, teniendo en cuenta los distintos permisos que se le brindan para que pueda ingresar a ciertos datos generados, llevan consigo una correlación con el Art. 6 de la misma le.

> *"Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma expresa y clara: a) La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o clase de destinatarios; b) La existencia del archivo, registro, banco de datos, electrónico o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable; c) El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos referidos en el artículo siguiente; d) Las consecuencias de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos, e) La posibilidad del interesado de ejercer los derechos de acceso, rectificación y supresión de los datos."*

En el caso de Brasil tanto la constitución en su Artículo 5 LXXII Y LXXVII hace referencia al habeas data. Luego la legislación sectorial ley N°9296/96 y N°9507/97

España tiene su propia agencia de protección de datos que es la encargada de velar por el cumplimiento de la ley orgánica 15/1999 de protección de datos personales de carácter personal.

El 25 de mayo de este año 2018, comenzó a regir un nuevo reglamento europeo de protección de datos personales (RGDP). Lo que se debe tener en cuenta como esencial es que los consentimientos deben ser expresos, específicos y verificables.

II. ALGORITMOS:

Los algoritmos si bien son un grupo determinado de instrucciones que resuelven un problema, en el caso de la programación, es un conjunto de acciones, instrucciones o pasos, que deben ser respetados para resolver un "problema". La diversidad de este tipo de algoritmos es amplia por lo cual se debe escoger con precisión el más adecuado para no desperdiciar tiempo ni espacio de los sistemas.

La sociedad vuelca e interacciona mucho dentro de las redes, eso hace que los algoritmos capten, retengan, clasifiquen mucha información. Esta, condiciona la red y la hace más "personalizada" a los requisitos de cada usuario, permitiendo en algunos casos encontrar con mayor facilidad lo que se busca y en otras no. Esto puede afectar de una manera tal que llegue a modificar el punto de vista que se tenga sobre una situación, ya que reduce o elimina la exposición a puntos de vista diferentes de los cuales uno puede partir en un comienzo. Condicionan en gran medida la percepción del entorno y como interactuar.

Los procesos para la elaboración de un algoritmo comprenden solo unas líneas de códigos, constan también de diversas lógicas profesionales con una gran cantidad de criterios que obedecen en parte a su elaboración. Impidiendo o alentando a que produzcan determinados resultados y con ello el fin esperado.

Esta herramienta viene a suplir la labor humana que se realizaba cuando se enfrenta a volúmenes de datos importantes, donde en lugar de ser de forma automatizada la elección de esta, las herramientas utilizadas se encuentran en el ámbito en el que se desempeña la persona, sus grupos sociales, familiares, etc.

Estos algoritmos lejos están de ser algo sencillo, en el caso de Youtube su algoritmo está constituido por al menos un millón de líneas de códigos de programación.

III. GOOGLE:

El primer resultado que nos ofrece el propio Google sobre su algoritmo lo encontramos sin siquiera entrar a ninguna página, nos lo muestra como preferencia "El Algoritmo de Google es la forma que tiene el buscador de posicionar las páginas ante una búsqueda, es decir, es lo que decide si sales primero, segundo o en la segunda página. Este algoritmo cambia unas 500 veces al año y resulta difícil seguirle la pista."[1]

Si bien es cierto que ocurren muchas modificaciones a los algoritmos de Google tienen una particularidad. No es seguro si es para tratar de amortiguar el golpe o solo por hacerlo menos estructurado, pero lo que si es cierto que detrás de esos peculiares nombres se cuenta también alteraciones al SEO o (Search Engine Optimization)[2]

[1] Proveniente de la página www.40defiebre.com

[2] El posicionamiento en buscadores, optimización en motores de búsqueda u optimización web es el proceso técnico mediante el cual se realizan cambios en la estructura e información de una página web, con el objetivo de mejorar la visibilidad de un sitio web en los resultados orgánicos de los diferentes buscadores. También es frecuente encontrar la denominación en inglés, search engine optimization, y especialmente sus iniciales SEO.

Una de las actualizaciones a su algoritmo es PANDA, la misma se centra en la calidad de la información que se filtra y llega al usuario. Apunta a que los contenidos que llegan y se posicionan primeros sean los que mayor aporte hagan al interés del usuario. Hace que los productores de contenidos tengan en cuenta distintos aspectos al momento de subir el mismo entre ellos, el no copiar, el pensar en las personas, que sea divertido de leer y fácil.

Otra de las actualizaciones más conocidas al algoritmo es Penguin que desde el 24 de abril del 2012 se centra en la calidad de los enlaces. Evita que se puedan insertar enlaces que no sean obtenidos de forma natural.

El 20 de agosto del 2013 llegaba Hummingbird una modificación que cambiaría el algoritmo en su conjunto desde su anterior modificación integra con Caffeine[3]. Lo que nos aporta este "pajarito" es un cambio en la búsqueda semántica y el knowledge graph[4]

IV. FACEBOOK:

Bien es sabido que Facebook es una "comunidad" que sobrepasa los 2.000.000.000 (dos mil millones) de usuarios. El servicio que proporciona no es el de la producción de contenidos sino su ordenamiento y distribución. Para aumentar si credibilidad dentro de la sociedad en la que ejerce su trabajo, se propuso modificar la forma de clasificar, filtrar, decidir, priorizar, recopilar, recomendar, los medios que falsean menos la verdad para llegar con ellos a la información verídica a sus usuarios.

A principios de este año (2018) se dijo que las modificaciones hechas a las *Fans Pages*[5] en los países piloto (Bolivia, Serbia, entre otros) se haría extensible a nivel global, dejando a estas empresas en un apartado distinto al que llamarían Explorer. Tras el masivo susto de los

---

Las personas que realizan tareas de optimización en motores de búsqueda se denominan posicionadores web o consultor SEO y en inglés search engine optimizers (cuyas iniciales también son SEO) o SEO specialists.

[3] Con Caffeine, Google analiza la web en pequeñas porciones y actualiza el índice de búsqueda de forma continua, a nivel mundial. Tan pronto Google encuentra una nueva página o una nueva información en las páginas Web existentes, Google puede adicionar esto directamente en el índice. Esto significa que es posible encontrar información más actualizada como nunca antes se había visto en el pasado —No importa cuándo ni dónde se publicó.

le permite a Google indexar páginas web a una escala enorme. De hecho, cada segundo procesa cientos de miles de páginas en paralelo. Si esto fuera una pila de papel crecería tres millas más alto cada segundo. ocupa cerca de 100 millones de gigabytes de almacenamiento en una base de datos y adiciona nueva información a una velocidad de cientos de miles de gigabytes por día. Se necesitarían 625.000 de las iPods con más almacenamiento para guardar tanta información y si estas fueran apiladas de extremo a extremo ocuparían más de 40 millas.

[4] El Gráfico de conocimiento (Knowledge Graph en inglés) es una base de conocimiento usada por Google para mejorar los resultados obtenidos con su motor de búsqueda mediante información de búsqueda semántica recolectada de una amplia gama de recursos. La aparición de este gráfico se añadió al motor de búsqueda de Google en 2012, inicialmente en los Estados Unidos, luego de haber sido anunciado el 16 de mayo de 2012. Provee información estructurada y detallada acerca de un tema además de una lista de enlaces a otros sitios. La meta es que el usuario sea capaz de usar esta información para resolver su consulta sin tener que navegar a otros sitios para que reúna la información por sí mismo. De acuerdo con Google, esta información se deriva de muchos recursos, que incluyen el CIA World Facetbook, Freebase y Wikipedia. La característica es similar en intención a los motores de respuesta tales como Ask Jeeves y Wolfram Alpha. A partir de 2012, su red semántica contenía más de 570 millones de objetos y más de 18 mil millones de sucesos acerca de –y relaciones entre– esos diferentes objetos que se usan para entender el significado del término índice ingresado en la búsqueda.

[5] La **fan page** es visible para todos, no está condicionada a la incorporación del usuario en tu relación de amigos. El acceso a ella puede realizarse a través de su optimización y la página estará visible para todo el que acceda a ella a través de un simple me gusta. Métricas.

usuarios que realizaban algún tipo de actividad publicitaria en esta red social, se anunció que esto no se extendería de los países pilotos. Esto alivio los nervios, pero de la mano con ello se anunció la modificación del algoritmo utilizado para el procesamiento de las informaciones.

Lo que se busca según Mark Zuckerberg[6] con esta gran alteración en los parámetros del algoritmo, que los contenidos que le lleguen a los usuarios no sean solo relevantes, sino que sean significativos.

Que factores determina esto:

- La cantidad de comentarios realizados, pero ahora ya no con la empresa sino entre sus usuarios
- Los videos que se suban directamente a Facebook sin pasar por otra plataforma con anterioridad. (tener la exclusividad). Aún más si son "directos".
- Que los contenidos sean pocos y de calidad, no muchos, pero pobres.
- Generación de likes, comentarios, shares y reacciones, pero sin pedirlos.

Desde la *compra de Instagram por Facebook*[7] esta ha ido sufriendo cambios, desde introducir publicidades hasta los algoritmos. Antes de la implementación de los algoritmos, los usuarios venían de forma cronológica los contenidos de quienes seguían, esto ocasionaba en algunas situaciones que se perdieran probablemente publicaciones de interés para muchos usuarios. "siempre en favor de los usuarios" se implementaron los algoritmos para evitar este tipo de fallos en la comunicación dentro de las redes.

V. INSTAGRAM:

Posee más de 700.000.000 (setecientos millones) de usuarios activos mensualmente. Desde el 2016 (junio) el algoritmo que utiliza la pantalla de inicio no ordena de forma cronológica en su Feed[8], esto llevo a que muchos "negocios" en esta red social mermaran por no saber o tener la capacidad de adaptarse a los requerimientos de esta.

El Feed de noticias principal se compone de 5 algoritmos:

- Edge Rack: encargado de mostrar las publicaciones ideales para el usuario utilizando distintos parámetros: cuentas que te gusta, cuentas con mensajes privados, cuentas buscadas, cuentas de personas que conoces en la vida real.

---

[6] **Mark Elliot Zuckerberg** (White Plains, Estados Unidos; 14 de mayo de 1984) es un programador y empresario estadounidense, conocido por ser el creador de Facebook. Para desarrollar la red, Zuckerberg contó con el apoyo de sus compañeros de Harvard, el coordinador de ciencias de la computación y sus compañeros de habitación Eduardo Saverin, Dustin Moskovitz, y Chris Hughes. A la fecha abril de 2018 es el personaje más joven que aparece en la lista de multimillonarios de la revista *Forbes*, con una fortuna valorada en US $ 63 300 millones de dólares, clasificándole como la quinta persona más rica del mundo. Fue nombrado como *Persona del Año* en 2010 por la publicación estadounidense *Time*.

[7] El 15 de Abril del 2012, tres firmas de capital de riesgo invirtieron US$ 50 millones en **Instagram**, valorando la compañía en US$500 millones. **Facebook** la compro por US$ 1.000 millones.

[8] El Feed de Instagram es el listado donde aparecen todas las publicaciones (fotos y vídeos) de las personas a las que sigues. El Feed de un perfil de Instagram es la página donde aparecen todas las publicaciones de un solo perfil.

- Ht Search: Se centra en dar prioridad a las imágenes en el apartado de las publicaciones destacadas que se realizan por búsqueda de hashtag.
- Stories Relevance: Este pone el foco en determinar qué historia se muestran o no a distintos usuarios y en qué orden aparecen.
- Ht Follow: establece prioridad de las publicaciones cuando un usuario indistintamente de cuál sea sigue un hashtag. Las variables que utiliza para lograr esto: Stories de Cuentas cuyo contenido te gustan. Stories de Cuentas con las que entablas mensajes privados. Stories de Cuentas que buscas. Stories de Cuentas de personas que conoces en la vida real. Duración de la visualización de cada Story. Número de visualizaciones de cada Story. Volumen de mensajes generados a raíz de la Story.
- Places: determina la prioridad de las publicaciones en función de la ubicación de las historias como de las demás publicaciones.

VI. TWITTER:

La red social twitter que ya lleva en funcionamiento hace ya más de 10 años, como es sabido se caracteriza principalmente por acotar la información que se puede compartir ahora aumentada a 280 caracteres, salvo algunos países en los cuales los 140 caracteres del viejo Twitter son suficientes para expresar, entre ellos Corea China y Japón.

En el 2016 se modificó de forma global el algoritmo que utiliza esta red. Esto trajo aparejado como principal y más notorio cambio el orden en que los diferentes Tweets aparecen en el time line de cada usuario, haciéndolo aún más personalizado ya que no se rige solo por el tiempo, sino que también lo hace evaluando el nivel de relevancia que los mismos van adquiriendo conforme esta subido. Hace que se tenga sin perder su línea de tiempo para no dejar de lado la característica esencial de mensajería instantánea, diferentes mensajes que puede que sean de cuentas que seguimos o no ya que puede ofrecernos algunos muy relevantes para nosotros que tal vez ignoramos por no seguir a determinado usuario.

La forma en que el algoritmo va eligiendo y valorizando lo que el usuario puede llegar a necesitar o le pueda parecer interesante lo hace a través del Deep Learning, que aprovecha la plataforma de Cortex[9], que se basa en el uso de sistemas de redes neuronales para llegar a imitar la forma del aprendizaje humano.

Antes de este cambio la forma de aparición y orden de los tweets era sencilla solo se lo realizaba de forma cronológica inversa sin mayores complicaciones. Pero luego del ingreso de este algoritmo es un poco más "personalizado". Todos son evaluados y puntuados, así se

[9] Cortex, un software pensado para simplificar el diseño, desarrollo y mantenimiento de sistemas de IA. Cortex permite aplicar esta tecnología para personalizar perfiles de usuario, pudiendo así crear experiencias individualizadas; generar informes de manera comprensible para las personas; coordinar diversos programas para automatizar procesos que requerirían la participación de un humano pero resultarían tediosas; aprender continuamente a partir de datos obtenidos en tiempo real; construir a partir de librerías de datos pre-seleccionadas y finalmente controlar todo el proceso llevado a cabo por el sistema de IA.

los puede calificar de los mas a los menos relevantes para cada uno de los usuarios poniéndolos así uno debajo del otro del más al menos relevante de forma instantánea. Pero cuando el usuario pasa un tiempo determinado sin ingresar a la aplicación se tiene también en cuenta un módulo especifico donde el usuario podría haber perdido, por no estar en uso la red, de algunos que le fueran de sumo interés, sin importar si se sigue o no al usuario que lo realizo. La intención que se tiene es lograr que el usuario de un solo vistazo, tenga al alcance de sus ojos lo más interesante para él.

Al final el orden de aparición de los mensajes va a estar condicionado por tres factores esenciales.

- El Tweet en si (cuando se publicó, si contiene elementos multimedia, si tiene repercusión dentro de la red).
- El autor del Tweet (tiene en cuenta la relación con el autor, el origen de la relación, grado de conexión).
- La actividad en el Twitter (la frecuencia en la que se utiliza y la actividad dentro de la misma).

VII. WHATSAPP:

Uno de los sistemas de mensajería más conocidos y usados en el mundo con más de 1.500.000.000 (mil quinientos millones) de usuarios mensuales alrededor del mundo, que generan unos sesenta mil millones de mensajes diarios. La aplicación se adquirió por Facebook en el 2014 cuando ya contaba con el gran numero de 500.000.000 (quinientos millones) de usuarios.

Lo que primero asombra es pensar este medio de comunicación como una "red social" o por lo menos con la necesidad de llevar consigo algoritmos. ¿Para qué quiero algoritmos en mi app de mensajería instantánea? El algoritmo, por ejemplo decide el nivel de seguridad de la conversación que se está ejecutando en la aplicación, no de los mejores: el RC4[10], que es un tipo de algoritmo utilizado entre otras cosas para otorgarle seguridad a una red WIFI con sistema WEP[11]

La inserción de los algoritmos dentro de la aplicación esté ligada de a que la compañía fue adquirida por Facebook.[12]

[10] Dentro de la criptografía RC4 o ARC4 es el sistema de cifrado de flujo Stream cipher más utilizado y se usa en algunos de los protocolos más populares como Transport Layer Security (TLS/SSL) (para proteger el tráfico de Internet) y Wired Equivalent Privacy (WEP) (para añadir seguridad en las redes inalámbricas). RC4 fue excluido enseguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.

[11] Wired Equivalent Privacy o "Privacidad equivalente a cableado", es el sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite

[12] El 6 de febrero del 2014 fue aprobada por las entidades regulatorias la compra de WhatsApp por parte de la empresa Facebook por una suma que asciende a los 22.000 millones de dólares.

VIII. LINKEDIN:

Esta red social un tanto particular ya que se enfoca más al ámbito profesional de los usuarios, no es la excepción a la regla de los algoritmos. Si también está controlada, filtrada y pensada por un algoritmo.

La aplicación en una primera instancia clasifica los contenidos, ya sean imágenes, videos, textos, long form o links. Se determina su clasificación en "spam", "de baja calidad" o "limpios" Teniendo en cuenta que tipo de contenido sea se lo distribuye un porcentaje de a las conexiones que uno tenga en esta red[13]. Luego existen dos posibilidades, o bien que sea degradado por su bajo contenido y calidad o por en su caso contrario que se lo difunda de forma más intensiva como una suerte de premio a la calidad del trabajo realizado.

Existen tres niveles en los cuales se le puede dar difusión. El primer nivel seria solo a los contactos que uno tiene, luego ya en los casos de trabajos más importantes se los hace llegar a los contactos de estos contactos. Y ya solo con una gran popularidad los mismos son mostrados no solo a los contactos de los contactos con los que se tiene conexión, sino a los contactos de los contactos de los contactos que tiene el usuario haciendo que el alcance de esto sea incalculable. El nivel de popularidad de la publicación se calcula por un sistema de puntos no muy complejos. Las recomendaciones (Likes) darán 1 punto, los comentarios por su parte 2 puntos y el compartir la publicación hace ganar 3 puntos.
Todas estas posibilidades son evaluadas por los algoritmos que clasifican, descartan y difunden la información que pasa por esta red.

IX. AMAZON:

El SEO aquí nace de la necesidad de vender más, optimizan sus servicios o productos. Teniendo en cuenta que un 40% de los consumidores estadounidenses comienzan sus búsquedas de información sobre un producto por esta plataforma. A9[14] es el nombre elegido para el complejo algoritmo que aún está en proceso de maduración de esta plataforma, se espera que sea con el tiempo cada vez más compleja ya que este tipo de algoritmos tienen la particularidad de ir aprendiendo con el transcurso del tiempo.

La respuesta del algoritmo es de 212 milisegundos, procesa unos 45.000.000 de Queries[15] diarios, analiza el big data en interacción con el historial de búsqueda, las compras realizadas y el género del usuario, pudiendo hacer un perfil bien definido del mismo para poder hacer muy precisos y certeros los resultados que ofrezca la plataforma. De esta forma hace más tentador tanto para el oferente como para el receptor de estas ofertas elegir estos medios para

[13] Los equipos de Marketing de la empresa Linkedin dijo que esa muestra a la cual se le muestran las publicaciones es un 20% de la cantidad de conexiones que uno tiene dentro de la red (contactos).
[14] U n algoritmo A9 es una clave del modelo comercial de Amazon, ya que ayuda a maximizar los ingresos generales al asegurar que los productos más vendidos con los márgenes más razonables por los vendedores más centrados en el cliente se coloquen frente a compradores que están listos para comprar.
[15] Query string o, en español, cadena de consulta es un término informático que se utiliza para hacer referencia a una interacción con una base de datos. Es la parte de una URL que contiene los datos que deben pasar a aplicaciones web como los programas CGI.

su comercialización ya que provee un particular análisis del mercado al que se le hace la oferta.

Para determinar la posición en la que van a aparecer estos productos o servicios se tienen en cuenta factores como el precio del producto, la disponibilidad del mismo, la selección e historial de ventas, el grado de textos. También es posible que se incremente el nivel de exposición a mayor interacción del vendedor con sus clientes aportando mayor cantidad de datos sobre los productos o servicios que se comercializan.

X. YOUTUBE:

En el caso de esta red social famosa por sus contenidos visuales, ya sabemos que no es encargada de valorar los videos en buenos o malos. El algoritmo aplicado aquí, se centra, como en otras redes, de comprender como los distintos usuarios interactúan con los contenidos que se suben. Esta inteligencia se funda en más de 80.000.000.000 de comentarios que se producen por día sobre los distintos contenidos que la plataforma ofrece. Las interacciones que esta inteligencia artificial evalúa son: qué tipo de video ven y cual no, cuanto tiempo permanecen en el video elegido, cuanto es el tiempo por el que se extiende la sesión del usuario y fundamentalmente sus opiniones con cada video (me gusta, no me gusta, no me interesa).

De esta forma es como Youtube logra sorprendernos con las recomendaciones que nos hace día a día no solo sobre los canales a los cuales se suscribe y se quiere mantener actualizado, sino de todos aquellos otros de los cuales no se tiene conocimiento pero que pueden resultar de sumo interés para el usuario. Esto es de sumo interés para la empresa ya que al poder ser precisos con el tipo de contenidos que le son ofrecidos, se aumenta de forma exponencial las visitas, la permanencia y la interacción que se tiene.

XI. SNAPCHAT:

Esta es otras de las aplicaciones de mensajería instantánea que sucumbió ante los supuestos beneficios que los algoritmos podían aportan al mejoramiento y personalización de la aplicación a cada usuario. La aplicación apunta a un público de edades no muy elevadas haciendo que sus promedios sean menores a los 25 años. También ocurrió que sufrió el cambio de estar organizado de manera cronológica a esta nueva forma de organización algorítmica. Pero Snapchat[16] no es famoso por ese tipo de algoritmos sino por otro un poco más complejo, pero también más útil y llamativo, que es el denominado Viola Jones[17], que emplea procesos para detectar las caras al momento de realizar la foto o video, escaneando

[16] Snapchat es una aplicación de mensajería para el teléfono inteligente con soporte multimedia de imagen, video y filtros de realidad aumentada. Su mayor seña de identidad es la mensajería efímera, donde las imágenes y mensajes pueden ser accesibles solo durante un tiempo determinado elegido por los usuarios. Fue creada por Evan Spiegel, Bobby Murphy y Reggie Brown, cuando eran estudiantes de la Universidad de Stanford (Estados Unidos), en 2010. Actualmente está desarrollada por Snap Inc., originalmente Snapchat Inc.

[17] El marco de detección de objetos Viola-Jones es el primer marco de detección de objetos para proporcionar tasas competitivas de detección de objetos en tiempo real propuestas en 2001 por Paul Viola y Michael Jones. Aunque puede ser entrenado para detectar una variedad de clases de objetos, fue motivado principalmente por el problema de la detección de rostros.

las diferentes partes de los rostros y caras. Una vez que se detecta el rostro y se lo diferencia del resto de la imagen, en tiempo real Looksery[18] detecta las partes que lo componen determinando un patrón general facial. Luego de este análisis la compañía puede establecer una serie de puntos que marcan el ancho y alto de las cejas, ubicación del rostro, posición de nariz, ojos labios, etc. Con todos estos parámetros se realiza una máscara tridimensional del usuario.

Lo que mayor provecho tuvo para la compañía es que estas mascaras son modificadas y recalculadas en tiempo real haciendo la experiencia en la aplicación muy llamativa. Los famosos lentes son uno de los mayores ingresos que tienen, ya que se convirtió en una de las opciones más populares, esto les deja una suma cercana a los U$S.750,000 dólares por este servicio.

XII. FUERA DE LAS REDES:

También están siendo insertadas dentro de muchas otras áreas algunos tipos de Algoritmos que lo que comienzan a hacer es tomar decisiones que se tornan en muchos de los casos complicadas para los propios humanos.

JUSTICIA

Un ejemplo claro de este es el de COMPAS que es un algoritmo evaluador de riesgos que puede predecir de cierta forma las probabilidades de que un sospechoso haya o no cometido determinado hecho. Más de diez jueces de los Estados Unidos la utilizan para apoyar las bases de sus sentencias.

Uno de los casos más sonados sobre el empleo de esta herramienta es el de Eric Loomis[19] quien fue penado con 7 años de cárcel por eludir un control policial y manejar un vehículo sin consentimiento del titular. Su sentencia se basó solo en una entrevista y las probabilidades criminales del imputado, el cual tenía una calificación de *"alto riesgo de cometer un delito"*.

SALUD

Debido a la gran cantidad de consumo de drogas tanto legales como no legales. Los seguros médicos comenzaron a ver la necesidad de predecir si sus beneficiarios eran o no propensos al consumo de forma adictiva. Así es como la proveedora de seguros médicos Blue Cross[20]

---

[18] Looksery es una compañía estadounidense de software y fotografía fundada en 2013 por Victor Shaburov y Yurii Monastyrshin. La compañía tiene su sede en San Francisco y es propiedad de Snap Inc. La compañía desarrolló la aplicación Looksery que realiza modificaciones faciales de fotos en tiempo real en plataformas móviles. La compañía tiene oficinas en Rusia, Estados Unidos y Ucrania.

[19] Los abogados de Loomis rechazaron la condena usando distintos argumentos, el hecho de que COMPAS había sido desarrollado por una empresa privada y la información sobre cómo funcionaba el algoritmo nunca había sido revelada. También reclamaron que los derechos de Loomis habían sido violados, porque la evaluación de riesgo tomó en cuenta información sobre el género y la información racial. De hecho, un análisis de más de 10.000 acusados en el estado de Florida publicado en 2016 por el grupo de investigación ProPublica mostró que las personas negras eran a menudo calificadas con altas probabilidades de reincidir, mientras que los blancos eran considerados menos proclives a cometer nuevos crímenes.

[20] https://www.bcbs.com/

y la firma Fuzzy Logix[21] crearon un algoritmo que evaluando 742 variables distintas podían realizar un diagnóstico del riesgo de una persona sobre el abuso de estas substancias. Los grupos en favor del avance y la inteligencia artificial señalan que es un aporte muy valioso ya que produce un menor riesgo para las aseguradoras, pudiendo de esta forma no realizar gastos innecesarios y bajando los aportes de los usuarios. Reduciendo también el error humano y los grandes costos que estos generan en la toma de decisiones.

AMOR

Como en toda red social las aplicaciones de citas también aprovechan "en favor de sus usuarios" los beneficios de poder filtrar las distintas opciones que le pueden llegar al candidato. Uno de los casos es de eHarmony[22] el cual dio a conocer que en algunas situaciones ajustaba los distintos parámetros del perfil de un usuario para hacerlo más atractivo o interesante, esto basado en los likes del mismo. Dejando de lado alguna de las 400 preguntas que se deben responder para poder completar la cuenta.

En otros casos más simples como Tinder[23] también se ven los alcances de los algoritmos ya que se obtiene una calificación que no es vista por los usuarios, pero si por la aplicación que se basa en la cantidad de veces que la fotografía fue deslizada hacia la derecha o hacia la izquierda (like or dislike). Teniendo en cuenta esto el algoritmo evalúa que tan deseable es un usuario poniéndole a su disposición distintos tipos de eventuales candidatos, con lo que busca facilitar un acierto en el tipo de emparejamiento y en la rapidez con la que se puede conseguir uno.

TRABAJO

Las nuevas formas de poder realizar una convocatoria para ocupar un puesto de trabajo hacen que también al análisis de los distintos curriculums. Aquí es donde surge el empleo de los Sistemas de Seguimiento a Candidatos, que lo que hace es filtrar las distintas solicitudes de entre cientos o miles a tan solo unas pocas, facilitando luego la posibilidad de elección por parte de un humano. Esto les permite a las compañías ahorrar no solo dinero en la forma de elección sino también tiempo ya que la detección de los posibles candidatos más aptos se realiza de manera automática e instantánea. En Estados Unidos un 70% de las empresas se estima que filtran de esta manera las solicitudes antes de pasar a manos de un empleado de recursos humanos.

Lo que ocurre es que no se puede asegurar que este tipo de funciones sea totalmente objetivas, ya que al ir aprendiendo el mismo algoritmo sobre sus decisiones y elecciones adquiere

[21] http://www.fuzzylogix.com/

[22] eHarmony es el primer servicio dentro de la industria de citas en línea que utiliza un enfoque científico para hacer coincidir los solos altamente compatibles. La combinación de eHarmony se basa en el uso de su modelo 29 DIMENSIONS® para unir parejas en función de las características de compatibilidad que se encuentran en miles de relaciones exitosas. Se compromete a ayudar a los solteros a encontrar el amor todos los días y confiamos en nuestra capacidad para hacerlo. El sistema de compatibilidad Harmony Matching Systems® combina con mujeres y hombres solteros según 29 Dimensions® de compatibilidad para relaciones duraderas y satisfactorias.

[23] Tinder es una aplicación geosocial que permite a los usuarios comunicarse con otras personas con base en sus preferencias para charlar y concretar citas o encuentros. Su fecha de lanzamiento fue 12 de septiembre del 2012.

prejuicios y sesgos propios de un humano, pudiendo ocurrir que se filtre un buen postulante al nuevo puesto de trabajo.

ECONÓMICO

Se están implementando distintos algoritmos que traten de predecir las capacidades de pago de un crédito, en esto están sumamente interesadas las distintas entidades financieras, ya que tornaría menos o sin riesgo una inversión. Los algoritmos que evalúan y toman estas decisiones acumulan datos de distintas fuentes lo que conlleva un gran riesgo de poder recoger información sin el consentimiento del titular o posible beneficiario del crédito. Los parámetros que puede recoger son muy amplios pudiendo llegar hasta patrones de compra, búsquedas en Internet o actividades en las redes sociales. De la misma forma al ser productos de empresas privadas no se tiene certeza sobre el funcionamiento de los distintos procesos de los algoritmos que lleve inserto y con ello deja expuesto, un posible problema tanto en la transparencia como en la imparcialidad de las decisiones.

CONCLUSIÓN:

Si bien el empleo de los algoritmos en las distintas labores diarias es una forma de facilitar los tediosos trabajos de selección y acota las largas horas que se pueden pasar buscando la información adecuada, también es cierto que estamos atados al ofrecimiento que nos proporciona. De cierta forma la comparación de las búsquedas de dos personas distintas sobre un mismo tema se ve condicionada por sus interacciones a nivel global en toda la red. Esto nos lleva a estar inmersos en una burbuja marcada y sellada por nuestros propios actos, con esto quiero decir, que cada elección hecha, cada clic realizado, nos condiciona hacia el futuro y ya no es solo en el acotado ejemplo de una búsqueda de información, se extiende abarcando cada vez más. Una mala elección, una página prohibida, un amigo desconocido en las redes, un me gusta sin sentido, etc. pueden conllevar a decisiones que marquen la vida del usuario en cualquier aspecto.

Ahora más que nunca internet es una puerta a nuevos mundos, a nuevas oportunidades… ¿Lo es? O es tan solo, la ilusión que fue borrando poco a poco la recolección de estos datos de sumo interés, que sin saber vamos aportando inconscientemente, sin reparo alguno en las consecuencias que puede tener.

Internet se convierte en un sinfín de oportunidades, que a ese usuario en particular le son convenientes por su perfil. Dando oportunidades limitadas y privando de oportunidades de conocer más allá.

Nos podemos preguntar si todo lo que vemos, hacemos, decimos, compramos, usamos, etc. es una libre elección o solo es el resultado de una compleja red de algoritmos que van canalizando y filtrando todas las opciones para que nosotros usuarios solo tengamos que preocuparnos por hacer y no poder decidir. Si las elecciones satisfactorias son en realidad muestra de nuestras capacidades de decisión o solo el esfuerzo de ingenieros que acertaron con la lectura y procesamiento de los datos que son recolectados y proporcionados al algoritmo.

Aun peor, son nuestros desaciertos realmente errores de los cuales aprender, o son más bien, perjuicios ocasionados por la mala administración de uno de estos "facilitadores" o "condicionadores" de elecciones.

Lo cierto es que los Algoritmos están, ya se utilizan, y no se puede escapar de ellos, afectan al mercado, a la forma de publicitar las marcas, de dar a conocer noticias, entre muchas otras y de a poco, a los usuarios comunes.

BIBLIOGRAFIA:

https://socialmedier.com/algoritmo-de-instagram/
https://blog.hootsuite.com/es/algoritmo-de-instagram/
http://wanatop.com/algoritmo-instagram/
http://increnta.com/es/blog/algoritmo-de-instagram-2018/
http://fernandocebolla.com/algoritmo-de-instagram-2018/
https://idus.us.es/xmlui/bitstream/handle/11441/71951/21.%20Comunicaci%c3%b3n%20discursos%20algoritmos%20poder.pdf?sequence=1&isAllowed=y
https://marketingdecontenidos.com/algoritmo-de-twitter/
http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm
https://www.40defiebre.com/cambios-algoritmo-google/
https://informaticadesdelaescuela.wordpress.com/2013/12/23/los-peligros-del-whatsapp-ii-mitos-y-realidades/#more-690
http://www.bbc.com/mundo/noticias-42916502
https://www.eharmony.com/verify/
http://www.eltiempo.com/tecnosfera/novedades-tecnologia/numero-de-usuarios-de-whatsapp-en-febrero-de-2018-178184
https://josefacchin.com/ley-proteccion-de-datos/
https://www.marcosseculi.com/social-media/instagram/diccionario/#Feed_de_Instagram
https://gestion.pe/tecnologia/snapchat-tecnologia-detras-mascaras-108898
https://luisgyg.com/publicaciones-de-snapchat-no-algoritmo/
https://ascenso.org/instituto-marketing-digital/respuestas/funciona-algoritmo-linkedin/
https://www.websa100.com/blog/como-funciona-algoritmo-linkedin/
https://es.linkedin.com/pulse/c%C3%B3mo-funciona-el-nuevo-algoritmo-de-linkedin-javier-alexandre-hierro
https://es.linkedin.com/pulse/c%C3%B3mo-funciona-el-algoritmo-de-linkedin-paula-p%C3%A9rez-toledo
https://www.socialnautas.es/blog/funciona-algoritmo-linkedin/
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/45530.pdf

Formas de crear, expresar, almacenar y manipular datos personales en la Sociedad red: retos para la protección

Por: ***Nayibe Chacón Gómez***[*]
Venezuela

Sumario: Presentación. 1.- Conceptualización del *big data*. 2. Relación entre las redes sociales y el *big data.* 3.- Protección de datos del *big data* proveniente de redes sociales. Conclusión.

Presentación:

La aparición y despliegue de las llamadas *tecnologías disruptivas*, término usado en la literatura de tecnología y negocios para describir innovaciones y desarrollos que mejoran un producto en sentidos que el mercado no los espera, típicamente por un bajo precio o diseños para un grupo diferente de consumidores; así encontramos el llamado *Internet de las cosas*, (*Internet of Things* - IoT) que fue inventado como una frase para una conferencia en la compañía *Procter & Gamble* por Kevin Ashton en 1999, y se refiere al mundo en el que cada objeto tiene una identidad virtual propia y capacidad potencial para integrarse e interactuar de manera independiente en la Red con cualquier otro individuo, ya sea una máquina (M2M) o un humano.

Se pueden citar como ejemplos del IoT:

1.- **Zapatillas inteligentes**: el primero de los primeros ejemplos de Internet de las cosas está dentro de la categoría de los *Wearables*.[1] Las zapatillas *SpeedForm Gemini* 2 cuentan con hardware capaz de registrar datos como el tiempo y la distancia recorrida, parámetros que después se combinan en una aplicación móvil para extraer valor de ellos. Las zapatillas también tienen la posibilidad de enviar datos GPS para determinar las rutas seguidas por el usuario.

2.- Sensores para el jardín: una de las compañías que ofrecen este producto es *Parrot*. Más conocida por la fabricación de *drones*, la empresa francesa también tiene un catálogo nutrido de sensores. Uno de ellos, el *Flower Power*, está destinado a jardines. El dispositivo registra datos sobre la luz solar, la temperatura, el nivel de fertilizante en el suelo y el de humedad. Con esta información, el sensor analiza el estado del jardín y lo

[*] *Abogada, Especialista en Derecho Mercantil y Doctora en Ciencias, Mención Derecho egresada de la Universidad Central de Venezuela. Profesora Titular adscrita a la Sección de Derecho Mercantil del Instituto de Derecho Privado de la Universidad Central de Venezuela. Directora General de la Sociedad Venezolana de Derecho Mercantil-SOVEDEM nayibe.chacon@ucv.ve nayibe.chacon@gmail.com*

[1] En un artículo publicado en el portal Computerhoy.com a finales del año 2014, conocí de qué se trataban los Wearables, les comparto la sencilla información: "son equipos compactos, especialmente pensados para que los puedas llevar puestos como si fueran ropa y, en general, son mucho más pequeños que los teléfonos móviles. En un futuro, podrían incluso implantarse en el cuerpo. En cualquier caso, se basan en una tecnología compleja y se trata de un nueva corriente tecnológica que está implantando y en la actualidad." [Disponible en línea] http://computerhoy.com/tags/wearable (Última consulta: 11/11/2016).

que necesitan las plantas. El dispositivo envía alertas a través de *bluetooth* al *smartphone* del usuario cuando este tiene que regar o practicar otros cuidados.

3.- Garajes inteligentes: más bien puertas de garajes. Pero sí, hay una empresa que ofrece un controlador para puertas de garaje. Con este dispositivo, llamado *Garageio*, se puede controlar el acceso mediante una aplicación. Desde el móvil puedes abrir y cerrar, así como recibir alertas cuando la puerta se abra. También posible permitir el acceso a terceras personas desde cualquier parte.

4.- *Wearables* para perros: las mascotas también estarán conectadas. Al menos es la tendencia que se está observando en los últimos meses. Un ejemplo de Internet de las cosas en este ámbito es *Fitbark*, un dispositivo que se coloca en el collar de tu perro para monitorizar su actividad. Como si fuera una especie de pulsera inteligente –de hecho el nombre hace referencia a la conocida marca *Fitbit*–, el dispositivo mide la actividad del perro, la calidad de su sueño y ofrece detalles sobre su comportamiento. **5.- Botones inteligentes:** Amazon ha llegado a un acuerdo con una serie de marcas de productos domésticos para crear botones inteligentes que funcionan de la siguiente manera. Cuando estás en casa y vas a poner la lavadora descubres que apenas queda detergente. Hasta ahora lo que hacías era apuntarlo en una lista, apuntarlo mentalmente o pensar "vaya, hay que comprar detergente" y olvidarlo al cabo de un instante. La asociación de Amazon con un fabricante de detergente te permite tener un botón inteligente acoplado a la lavadora, para que cuando observes la falta del producto puedas encargarlo solo con pulsar el botón. Amazon recibe la orden de compra –un determinado bote de detergente de una determinada marca– y la procesa para enviarlo directamente a tu casa."[2]

También entre las tecnologías disruptivas encontramos las *Smartcities*, o Ciudades Inteligentes, que se presentan como un modelo pensado por Jeremy Rifkin, economista, escritor y asesor de distintos gobiernos europeos y de la misma Comisión Europea, quien trabaja para dar forma al concepto y visión de la "Tercera Revolución Industrial", la fusión de las tecnologías de Internet con las energías renovables. "En el futuro, las viviendas, oficinas y fábricas, producirán su propia energía verde y compartirán unas con otras una "Internet energética", del mismo modo en que ahora creamos y compartimos información en línea. Para Rifkin, la Tercera Revolución Industrial es la oportunidad de cambio de modelo antes que se agoten los recursos naturales."[3]

Ahora bien, ¿qué tienen en común el IoT y las *Smartcities* a los efectos de la protección de datos personales? Que estos, sumados a otros emprendimientos tecnológicos y los que aparecen cada día, son generadores y consumidores de información personal, ya que este es su alimento, convirtiendo los datos personales de sus usuarios en el activo más preciado.

[2] BEJARANO, Pablo: **5 útiles ejemplos de Internet de las cosas que pronto podrás probar**. [Disponible en línea] http://blogthinkbig.com/5-utiles-ejemplos-de-internet-de-las-cosas-que-pronto-podras-probar/ (Última consulta: 12/10/2016)

[3] CERCLE TECNOLOGIC DE CATALUNYA: **Hoja de Ruta para la *Smart City***. [Disponible en línea] http://paisdigital.org/PD/wp-content/uploads/2014/06/HojaderutahacialasSmartCities.pdf (Última consulta: 12/10/2016)

1.- Conceptualización del *big data*:

Toda esta información forma o compone lo que se ha llamado *big data*, término que comúnmente es utilizado para identificar una formula o conjunto de estas que surge dada la imposibilidad de analizar inconmensurables cantidades de información a través de las formas tradicionales de tratamiento de datos.

Pero son Viktor Mayer-Schönberger y Kenneth Cukier, quienes en el libro: *Big data: La revolución de los datos masivos*, expusieron lo trascendental de esta fórmula tecnológica: "No existe ninguna definición rigurosa de los datos masivos. En un principio, la idea era que el volumen de información había aumentado tanto que la que se examinaba ya no cabía en la memoria que los ordenadores emplean para procesarla, por lo que los ingenieros necesitaban modernizar las herramientas para poder analizarla. Ese es el origen de las nuevas tecnologías de procesamiento, como *Map-Reduce*, de *Google*, y su equivalente de código abierto, *Hadoop*, que surgió de Yahoo. Con ellos se pueden manejar cantidades de datos mucho mayores que antes, y esos datos –esto es lo importante- no precisan ser dispuestos en filas ordenadas ni en las clásicas tabulaciones de datos… los *big data*, los datos masivos, se refieren a las cosas que se pueden hacer a gran escala, pero no a una escala inferior, para extraer nuevas percepciones o crear nueva formas de valor, de tal forma que transforman los mercados, las organizaciones, las relaciones entre los ciudadanos y los gobiernos, etc."[4]

Big data puede referirse al tratamiento y análisis de enormes repositorios de datos, tan desproporcionadamente grandes que es imposible tratarlos con las herramientas de bases de datos y analíticas convencionales;[5] así entendido, los presupuestos necesarios para hablar de *big data*, es la existencia las bases de datos, que contengan los siguientes elementos o atributos, llamados la triple "V": volumen, variedad y velocidad, los cuales deben estar siempre presentes.

- ✓ **Volumen de los datos**: la cantidad de datos a tratar es tan grande que es imposible la utilización de los medios tradicionales hasta ahora conocidos, tales como las hojas de cálculos del *MS Excel* o el lenguaje declarativo de acceso a la bases de datos *SQL*.

- ✓ **Variedad de los datos:** los datos recogidos provienen tanto de fuentes estructuradas como no estructuradas: transacciones bancarias, imágenes de satélite, redes sociales, contenidos de páginas web, dispositivos móviles de geolocalización y miles de aplicaciones, las conexiones del internet de las cosas, los servicios web 2.0, e incluso el cuerpo humano (por ejemplo, cuando se utilizan sistemas de identificación biométricos). Este aspecto será tratado más adelante, en la relación existente entre las Redes Sociales

[4] MAYER-SCHÖNBERGER Viktor y Kenneth Cukier: **Big data: La revolución de los datos masivos.** Edición en castellano: Turner Publicaciones S.L., 2013. Extracto [Disponible en línea] http://www.elboomeran.com/upload/ficheros/obras/extracto_bigdata_turner.pdf (Última consulta: 25/12/2015)

[5] Para ahondar acerca de las tecnologías que convergen en el *big data*, invitamos a la lectura del trabajo de los autores CAMARGO VEGA, Juan José, Jonathan Felipe Camargo Ortega y Luis Joyanes Aguilar: **Conociendo Big Data**. Revista Facultad de Ingeniería. Fac. Ingeniería Universidad Pedagógica y Tecnológica de Colombia. Enero-Abril 2015, Vol. 24. No. 38. pp. 63-77 [Disponible en línea] http://www.scielo.org.co/pdf/rfing/v24n38/v24n38a06.pdf (Última consulta: 01/11/2016)

y el *big data*. La doctrina sobre la materia del big data reconoce que el elemento de la variedad de los datos, es el de mayor relevancia, ya que extraer información de datos tan diversos supone un gran reto; así, "las tecnologías que se han desarrollado para el *big data* permiten, entre otras soluciones, combinar datos a pesar de que no se encuentren almacenados en ficheros con la misma estructura. Así por ejemplo, una cadena de tiendas puede analizar de forma conjunta los datos de ventas con los datos de temperaturas para realizar un modelo predictivo en tiempo real para cada uno de sus locales comerciales."[6]

- ✓ **Velocidad en la transferencia de los datos**: El *big data* permite transferir datos de forma barata y eficiente, y así se pueden analizar tanto los datos dinámicos que se van creando, como los datos estáticos o históricos que ya han sido almacenados de forma previa, ya que la velocidad a la que se crean y procesan los datos está en continuo aumento, y con frecuencia para las organizaciones es importante poder analizarlos de forma muy rápida, incluso en tiempo real, algo que en ocasiones es imposible con los sistemas tradicionales. "Por ejemplo, el análisis de datos en tiempo real puede ayudar a seguir la trayectoria de huracanes y su intensidad. Esto podría llegar a permitir realizar predicciones sobre dónde pueden producir daños con horas o incluso días de antelación."[7]

  La citada autora Elena Gil incorpora tres aspectos más que permiten perfilar el *big data*, los cuales también comienzan por la letra "V": veracidad, visualización y valor de los datos.

- ✓ **Veracidad de los datos**: se refiere a la calidad del mismo. "Conseguir datos de alta calidad se ha convertido en todo un reto, principalmente importante cuando se trata de datos no estructurados. Sin embargo, tal y como IBM asegura, algunos datos son inciertos por naturaleza, como los sentimientos, el futuro, los sensores GPS que rebotan entre los rascacielos de una ciudad, o los datos creados en entornos humanos como las redes sociales; y ninguna limpieza de datos puede corregirlos. Así, manejar la incertidumbre es una cuestión esencial al tratar con tecnologías *big data*."[8]

- ✓ **Visualización**: *Data Visualization*, en inglés, es el ámbito del *big data* que consiste en representar de manera comprensible y medible los datos obtenidos para encontrar patrones y claves ocultas en el tema a investigar. Es entendida como el conjunto de herramientas que posibilitarán comprender los datos gráficamente y en perspectiva contextual.[9]

---

[6] GIL, Elena: **Big data, privacidad y protección de datos.** Agencia Española de Protección de Datos. Agencia Estatal Boletín Oficial del Estado. Madrid, 2016. pp. 22-23. [Disponible en línea] https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/premios_2015/Big_Data_Privacidad_y_proteccion_de_datos.pdf (Última consulta: 20/09/2016)

[7] GIL, Elena: **Big data, privacidad y protección**…, ob. cit., p. 22.

[8] GIL, Elena: **Big data, privacidad y protección**…, ob. cit., p. 23.

[9] "Una de los servicios punteros en *Data Visualization* es el que ofrece *CartoDB*, una *startup* española que no ha parado de crecer desde su fundación. Específicamente se centra en mostrar información sobre mapas geográficos, por lo que los contenidos siempre han de ser comparables por zonas. El gran atractivo de

- ✓ **Valor del dato**: la finalidad última de los procesos de *big data* es crear valor, ya sea entendido como oportunidades económicas o como innovación; es éste valor del dato, el que ha hecho posible el emprendimiento del *big data*.

El *big data* llego para quedarse, ya que sus beneficios parecen superar los riesgos que conlleva a los datos de las personas. Ese beneficio es "el poder ofrecer una visión cada vez más precisa de las fluctuaciones y rendimientos de todo tipo de recursos, permitir realizar adaptaciones experimentales a cualquier escala de un proceso y conocer su impacto en tiempo casi real, ayudar a conocer mejor la demanda y así realizar una segmentación mucho más ajustada de la oferta para cada bien o servicio, o acelerar la innovación y la prestación de servicios cada vez más innovadores y más eficientes. Los datos para obtener estos conocimientos provendrán tanto de las personas como de los objetos, y con mayor énfasis a medida que el denominado internet de las cosas se generalice. Sin embargo, las previsiones estiman que tan solo el 0,5% de la información será efectivamente procesada."[10]

Los riesgos del *big data* que anuncia la doctrina son: (i) el riesgo de caer en conclusiones erróneas que nadie revisa, ya que el *big data* permite extraer patrones que posteriormente serán predicciones; (ii) el riesgo que para las personas pueda tener tomar decisiones automatizadas sin un sesgo humano, y que dichas decisiones no den lugar a justificación; y (iii) el riesgo para la privacidad de las personas y para el tratamiento de sus datos, lo cual se podría resolver a través de la transformación del dato, pasando de ser información que permite identificar a una persona en particular entre un universo, a una información anónima.

Este último aspecto que es analizado con profundidad por la autora Elena Gil, en su estudio, se puede resumir en un párrafo por ella escrito: "El *big data* desafía las normas de protección de datos al facilitar la re-identificación de los sujetos, ya no solo a partir de los datos pseudónimos, sino también a partir de datos que considerábamos anónimos. Es decir, las técnicas de anonimización ya no siempre son suficientes con la llegada del *big data*. Esto supone volver al debate de base de qué datos son personales y cuáles no personales." [11] En

---

CartoDB, desde mi punto de vista, es que, además de ser abierto, aprovecha su servicio para mostrar contenidos que hoy son muy relevantes, como los *tuits*, de manera fácilmente entendible pero a la vez muy potente. Con algunas funciones similares a *CartoDB* encontramos a *Google Fusion Tables*, otra herramienta sencilla con API avanzada que no requiere conocimientos avanzados y que genera gráficas y mapas con información presentada de manera más arcaica y simple que *CartoDB*, pero también comprensible, incluyendo la gestión de capas en datos geográficos. Por último, otra herramienta que se beneficia del enorme avance del *Big Data* es *Tableau Public*, ideal para mostrar información detallada de análisis en mapas interactivos o en gráficos de barras que también permite importar de Excel, por lo que la mitad del trabajo está hecho. Es muy sencilla y rápida, y permite a cualquier persona generar en poco tiempo un gráfico estético y publicable en una web." **Las mejores herramientas para visualizar grandes cantidades de datos**. [Disponible en línea] https://hipertextual.com/presentado-por/bbva/visualizacion-de-datos (Última consulta: 10/11/2016).

[10] GIL, Elena: **Big data, privacidad y protección**…, ob. cit., pp. 28-29.

[11] "Tradicionalmente, la anonimización consistía en un proceso de dos fases principales. En primer lugar despojar a los conjuntos de datos de todos los rasgos identificadores personales (PII por sus siglas en inglés *personal identificable information*), como pueden ser nombre, dirección, fecha de nacimiento o número de seguridad social. En segundo lugar, se modificaban o eliminaban otras categorías de datos que podían actuar como identificadores en dicho contexto concreto (por ejemplo, un banco eliminaría los números de tarjeta de crédito, y una universidad eliminaría los números de identificación de sus estudiantes). De este modo, el

nuestro caso, este tema será analizado de manera independiente en un subcapítulo único, desde la relación existe entre la protección de datos y el *big data* de las Redes Sociales, ya que la doctrina en la materia ha llamado la atención sobre la posible vulneración de los datos personales con el uso de estas.

2. Relación entre las redes sociales y el *big data*:

A manera de entrada en contexto, se pudiera pensar que las Redes Sociales constituyen un acontecimiento reciente, lo cierto es que se trata de un hecho que viene manifestándose desde hace décadas. Queda claro que las Redes Sociales comenzaron a surgir sólo a partir de la consolidación de la red Internet, aproximadamente en 1995. Es desde entonces cuando comienzan a emerger muchos de los grandes servicios que dominan actualmente el mercado virtual, tales como los de correo electrónico, almacenamiento de documentos, intercambio de archivos y compras virtuales, así como cientos de servicios menores y anuncios publicitarios. Si a finales de la primera década del siglo XXI no entendíamos como habíamos vivido sin Internet, hoy no sabemos cómo manejar nuestras relaciones sociales sin estas redes de comunicación global.[12]

"Las Redes Sociales son sin duda alguna las principales plataformas de comunicación en los medios sociales, porque son las que mejor permiten a los usuarios relacionarse entre sí, mediante el intercambio de experiencias y eventos de su vida diaria y la interconexión entre diferentes grupos de amigos de cada usuario."[13] En este orden de ideas, el Grupo Europeo de Autoridades de Protección de Datos,[14] en el documento sobre redes sociales online, denominado: *Opinión 5/2009*[15] las han definido como "las plataformas de comunicación en línea que permiten a individuos unir o crear las redes de usuarios de la misma opinión" y cuyas características comúnmente establecidas son: 1. Invitan a usuarios a proporcionar datos personales con el objetivo de generar una descripción de ellos o "el perfil". 2. Los servicios

---

resultado aunaba lo mejor de ambos lados: los datos continuaban siendo útiles, y podían ser analizados, compartidos o puestos a disposición del público al tiempo que los individuos no podían ser identificados, y por lo tanto se protegía su privacidad. La anonimización aseguraba la privacidad. Sin embargo, con los nuevos avances, esta situación cambia. El *big data*, al incrementar la cantidad y diversidad de la información, facilita la reidentificación de individuos, incluso después de haber sido anonimizados." GIL, Elena: **Big data, privacidad y protección**…, ob. cit., p. 83.

[12] En lo personal, la importancia del estudio de las Redes Sociales y sus implicaciones desde la perspectiva jurídica se me manifestó con ocasión de servir de tutora de una tesis presentada para obtener el título de abogado por dos estudiantes de la Universidad Metropolitana, en ese estudio titulado: *Análisis de la relación jurídica entre la red social Facebook y el Usuario*, Joel Kohn Salama y Jorge González Belfort, sus autores, no sólo analizaron el peculiar origen de la famosa red social, sino adelantaron conceptos que bien pueden abrir la puerta a la realización de numerosos trabajos en el área del Derecho de las Obligaciones y del Derecho de Consumo, algunos de los cuales fueron anotados por en el trabajo de mi autoría: **La responsabilidad de los proveedores de servicio en las redes sociales**, publicado en la Revista Derecho y Tecnología de la Universidad Católica del Táchira, No. 14, año 2013.

[13] BONNELLY RICART, Rafael: **La Huella Social: Cómo los usuarios tomaron control de Internet.** Ediciones de El Nacional. Caracas, 2011. p. 41.

[14] Ver sobre las actividades del Grupo Europeo de Autoridades de Protección de Datos, en http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm (Última consulta: 19 agosto 2016)

[15] Grupo Europeo de Autoridades de Protección de Datos, Opinión 5/2009, [Disponible en línea] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf (Última consulta: 19 agosto 2016)

de Redes Sociales también proporcionan los instrumentos que permiten a usuarios fijar su propio material (el contenido generado por el usuario puede ser una fotografía o una entrada de diario, la música o el clip vídeo o se vincula a otro sitios). 3. La "interconexión social" permiten a cada usuario crear una lista de contactos, con la cual los usuarios pueden interactuar recíprocamente. Así las Redes Sociales generan la mayor parte de su ingreso por la publicidad que se muestra junto a las páginas Web de la Red Social a la cual tienen acceso los usuarios. Se destaca que los usuarios que fijan grandes cantidades de información sobre sus intereses, en sus perfiles ofrecen un mercado refinado a anunciantes que desean colocar publicidad basada en aquella información.

Así tenemos que el núcleo de las actividades de algunas Redes Sociales, tales como *Twitter* y *Facebook*, consiste en una interfaz social que permite a los usuarios que se encuentran registrados en la misma, a través de la creación de una cuenta, relacionarse y entrar en contacto con los demás usuarios de inmediato al navegar en la página. La interfaz puede permitir igualmente compartir determinados tipos de archivos, específicamente contenido de tipo visual, así como archivos musicales y direcciones web, todo ello integrado con el diseño y la orientación de la creatividad. De la misma manera, las Redes Sociales pueden incorporar otros servicios como el chat o sala de conversación, los juegos online, la posibilidad de enviar regalos en combinación con mensajes, mensajería privada y toda una serie de elementos lúdicos.

Siendo que el número de usuarios de estas Redes Sociales es cada vez mayor y la cantidad de información personal que suben a través de esos portales son inconmensurables, los encargados en el procesamiento de datos se dieron a la tarea de inventar una formula o herramienta que permitiera acceder y usar esa información. Así aparece el insumo para el *big data*, que hace referencia directa a las gigantescas cantidades de información digital controlada por compañías, autoridades y otras organizaciones, y que están sujetas a un análisis extenso basado en el uso de algoritmos. Tal como apunta la autora Elena Gil, en su libro: *Big data, privacidad y protección de datos*, no es una tecnología en sí misma, sino más bien un planteamiento de trabajo para la obtención de valor y de beneficios como consecuencia del tratamiento de los grandes volúmenes de datos que se están generando día a día.[16]

Esta relación simbiótica entre Redes Sociales y *big data* queda claramente presentada cuando vemos que a la fecha éstas han alcanzado un número importante de usuarios,[17] convirtiendo a estas redes en el foco de atención de anunciantes y proveedores de todo tipo de bienes y servicios interesados en llegar a interactuar con esos potenciales consumidores y usuarios de

[16] GIL, Elena: **Big data, privacidad y protección**…, ob. cit.

[17] "Según el análisis efectuado por *ComScore*, y para hacernos una idea de la dimensión del fenómeno, sólo el servicio de red social *Facebook*, el sexto sitio más visitado del mundo, registra 275 millones de visitas al mes. En Europa, el pasado mes de febrero, unos 100 millones de personas habrían accedido al servicio *Facebook*, que supone cuatro de cada cien minutos pasados en línea y representa más del 30 % del tiempo total invertido en sitios de RSC, frente a sólo un 12 % el año anterior." Dictamen del Comité Económico y Social Europeo sobre el tema «Repercusión de las redes sociales de comunicación e interacción en el ciudadano/consumidor», Ponente: Jorge Pegado Liz, [Disponible en línea] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:128:0069:0073:ES:PDF (Última consulta: 19/8/2016)

sus marcas y productos. Así uno de los elementos más exitosos de muchas de las Redes Sociales ha sido su capacidad para anticipar que cierta información de los usuarios (si no toda), debía estar al alcance de los anunciantes para permitirle a sus respectivos asesores publicitarios diseñar mejores campañas en función de los gustos personales de los usuarios.

La generalidad de las Redes Sociales que actualmente son utilizadas cuentan con una estructura similar, donde podemos identificar al menos dos personajes que interactúan en la red: 1. El proveedor de la Red Social, aquella persona natural o jurídica, que proporcionan la infraestructura de la Red Social; y 2. El usuario de la Red Social: aquella persona natural o jurídica, que crea una cuenta de Red Social. Entre estos dos actores se desarrollan distintos tipos de relaciones, todas basadas en la confianza que se tiene en el uso de la Red Social, sobre todo porque las Redes Sociales se inician y se mantienen a través de suministrar y compartir información entre los usuarios sus amigos o seguidores, información que ha sido solicitada y que se encuentra depositada en los servidores del proveedor de la Red Social.

1. El Proveedor de la Red Social: es importante ubicar al Proveedor de la Red Social dentro de los Proveedores de Servicios de Internet, también conocidos como "ISP" (en inglés *Internet Service Provider*), son empresas encargadas de prestar el servicio de acceso a la Internet.

Siguiendo la clasificación anotada por algunos autores[18], podemos distinguir claramente dos tipos de Proveedores de Servicios de Internet, a saber:

1. *Los Proveedores de Acceso a Internet*, conocidos como "IAP" (en inglés *Internet Access Providers*), que hacen posible la entrada a la red, con independencia de los portales a que se acceda o de la información que sea buscada. Por una cuota o pago mensual, el proveedor da un paquete de software, un nombre de usuario, una contraseña y un número de teléfono de acceso, a través de un módem o banda ancha estos proveedores simplemente permiten navegar por el *World Wide Web*, el *USENET*, y enviar y recibir correo electrónico. En Venezuela podemos citar por ejemplo las siguientes empresas prestadoras del servicio: Compañía Anónima Teléfonos de Venezuela (CANTV) y Movistar, entre otras.

2. Los *Proveedores de Alojamiento en Internet*, también conocidos como "HSP" (en inglés *Host Services Providers)*, almacenan y mantienen los contenidos en un servidor con el fin de que los usuarios al conectarse a Internet accedan a esos contenidos o los recuperen. La utilización de los servicios ofrecidos por los Proveedores de Alojamiento, se centran en el alojamiento Web, requerido para publicar un sitio Web, los cuales constan de varios archivos de datos que conforman las páginas navegables de un sitio en línea.

[18] LIPSZYC, Delia. Responsabilidad de los proveedores de servicios en línea por las infracciones del derecho de autor y derechos conexos en el entorno digital: análisis de la jurisprudencia internacional. Asunción: OMPI, SGAE, Ministerio de Industria y Comercio de la República del Paraguay, noviembre de 2005. (En: XI Curso Académico Regional OMPI/SGAE) citado por: David Felipe Álvarez Amézquita, Julio Cesar Padilla Herrera, Andrea Liliana Garzón Zuluaga y Laura Yolanda Muñoz Hernández. **Proveedores de Servicios de Internet y de contenidos, responsabilidad civil y derechos de autor**. En: Studiositas, edición de diciembre de 2009, 4(3): 51-64, [Disponible en línea] en: htt://dialnet.unirioja.es/descarga/articulo/3658940.pdf (Última consulta: 21/08/2016).

> Principalmente, el servicio de alojamiento Web es almacenar los archivos en un servidor de datos que carga directamente a la Web, proporcionando conectividad a Internet y permite a los usuarios acceder a su sitio a través de su nombre de dominio elegido; sin embargo, los servicios de alojamiento Web pueden variar enormemente, desde la pequeña escala de alojamiento de archivos para páginas web personales a alojamiento más completos con base de datos y soporte de script.[19]

Por su parte, la *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico*[20] de España, utiliza la expresión «Prestador de servicios» o «prestador» definiéndolo como "persona física o jurídica que proporciona un servicio de la sociedad de la información." Se definen los «Servicios de la sociedad de la información» como "todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios. Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes: 1. La contratación de bienes o servicios por vía electrónica. 2. La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales. 3. La gestión de compras en la red por grupos de personas. 4. El envío de comunicaciones comerciales. 5. El suministro de información por vía telemática. 6. El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual."

Luego, la Ley 34/2002 establece de manera separada el «Servicio de intermediación» como una especie dentro de los Servicios de la Sociedad de la Información, que facilita la prestación o utilización de otros servicios de dicha sociedad o el acceso a la información. Se describen como Servicios de Intermediación los siguientes: a) la provisión de servicios de acceso a Internet, b) la transmisión de datos por redes de telecomunicaciones, c) la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, d) el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y e) la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet.

De una lectura del contenido de citada legislación española, se pueden clasificar a los Prestadores de los Servicios de la Sociedad de la Información en los siguientes tipos:

1. *Los Operadores de Redes y Proveedores de Acceso*, aquellos que prestan servicios de intermediación que consiste en trasmitir por una red de telecomunicaciones datos facilitados por el destinatario del servicio o faciliten acceso a dicha red.
2. *Los Prestadores de Servicio de Transmisión*, aquellos que transmitan por una red de telecomunicaciones datos facilitados por el destinatario del servicio y, con la única

[19]Para más información sobre servicios de alojamiento Web se puede consultar: http://web-hosting-review.toptenreviews.com/

[20]Ley Española 34/2002 de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. [Disponible en línea] http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf [Última consulta: 22/08/2016).

finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal.

3. *Los Prestadores de Servicio Albergar*, aquellos que albergan datos proporcionados por el destinatario de este servicio.
4. *Los Prestadores de Servicios de Enlace*, aquellos que facilitan enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos.

Ahora bien, a lo luz de lo mencionado, se pueden identificar a los Proveedores de Servicios de Redes Sociales, como un tipo muy especial de Proveedor de Servicio de Internet o de Prestador de Servicios de la Sociedad de la Información, así y de conformidad con la citada *Opinión 5/2009* del Grupo Europeo de Autoridades de Protección de Datos, los Proveedores de Servicios de Red Social son "reguladores de datos" y proporcionan el medio para el tratamiento de los datos del usuario, junto a todos los servicios "básicos" relacionados con la dirección de usuario (por ejemplo: el registro y la tachadura o eliminación de cuentas). Los Proveedores de Servicios de Red Social también determinan el empleo que puede ser hecho de datos de usuario para anunciar y comercializar objetivos –incluyendo la publicidad proporcionada a terceros.[21]

2. El Usuario de la Red Social: cuando se utiliza la palabra "Usuario" nos estamos refiriendo a una categoría propia de personas, es decir, aquellas que se encuentran reguladas de manera especial y en algunos casos excepción por el Derecho de Consumo.

El Usuario de las Redes Sociales es aquella persona natural o jurídica que utiliza, por cualquier motivo, los servicios de las Redes Sociales. En este sentido, se podría incorporar a la denominación de «Destinatario del servicio» o «destinatario» que otorga la Ley Española 34/2002, para la: "persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información."

Los Usuarios de las Redes Sociales han sido clasificados a través de su "perfil tecnográfico" tomando en consideración las actividades que éstos desarrollan en las redes y su nivel de participación, así tenemos:[22]

1. *Los creadores*: aquellos que se caracterizan desarrollar todas o algunas de las siguientes actividades: publicar en blogs, tener sus propias páginas web, crear y subir videos y/o música tanto propia como de otros, y escribir y publicar artículos.
2. *Los conversadores*: aquellos que se caracterizan principalmente por actualizar sus perfiles constantemente en todas las Redes Sociales en las que participan.
3. *Los críticos*: aquellos que se caracterizan por crear entradas y comentarios sobre productos y servicios en la red.
4. *Los coleccionistas:* aquellos que se caracterizan por utilizar los buscadores sociales de noticias y demás servicios de distribución de contenidos-
5. *Los que se apuntan:* aquellos que se inscriben en alguna Red Social y mantienen su perfil sin actualización.

[21]http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf
[22] BONNELLY RICART, Rafael: **La Huella Social:**…, ob. cit., pp. 31-32.

6. *Los espectadores:* aquellos que se caracterizan por leer, escuchas y ver comentarios y productos de los demás usuarios.
7. *Los inactivos:* aquellos a quienes no le importa o no le interesa el mundo digital y lo que ocurra en éste, aunque tienen acceso al mismo.

De la clasificación anotada podemos destacar, como lo hacen los autores,[23] que ciertos sujetos que frecuentan la red son simples usuarios que navegan en busca de información; otros (que cada vez se confunden más con los anteriores) son propietarios o licenciatarios de información en forma de contenidos protegidos, lo que tienen en común todo tipo de usuario, es que todos ellos dispensan información a la Red Social desde el momento que se registran para acceder a ella.

3.- Protección de datos del *big data* proveniente de redes sociales:

Ahora bien, ¿qué está pasando con el derecho a la privacidad y la protección de los datos personales en las Redes Sociales?, para abordar este tema, anotaremos las precisiones realizadas por Mariliana Rico Carrillo, sobre la base de las numerosas demandas en contra de los proveedores de servicios de redes sociales han motivado la modificación de las reglas de funcionamiento técnicas originales de algunas Redes Sociales.

La profesora Rico Carrillo dedica su estudio al caso de *Facebook*, y los cambios en las políticas de privacidad del *Facebook* que ha tenido que acometer en los últimos años, circunstancia que obedece a las ya citada demandas entabladas en contra de la compañía por violación del derecho a la privacidad. "En la actualidad, podemos afirmar que si existen políticas de privacidad *Facebook* –y también en otras RSI– en tanto que su funcionamiento que permite crear cuentas protegidas y los propios usuarios pueden establecer el nivel de privacidad en la red. *Facebook* cuentan con mecanismos que permiten a los usuarios determinar el tipo de información visible para el público en general y elegir que verán sus contactos y que no. El problema que se presenta en este ámbito es que la mayoría de las personas que se dan de alta no se toman el tiempo de leer las políticas de privacidad de la página –algunos ni siquiera saben que existen– y que la configuración original por defecto permite a quien acceda a Internet, visualizar la información de carácter personal suministrada por el usuario."[24]

En cuanto a la protección de los datos personales, debemos tener presente que los usuarios de las Redes Sociales pueden ver comprometidos sus datos personales, por tres situaciones distintas:

1º **con el registro como usuario**, ya que en ese momento es necesario el suministro de ciertos datos de carácter personal, durante la actividad en la red los usuarios también publican información personal y familiar e información de terceros. Estos datos pueden

[23] ÁLVAREZ AMÉZQUITA, David Felipe Julio Cesar Padilla Herrera, Andrea Liliana Garzón Zuluaga y Laura Yolanda Muñoz Hernández: **Proveedores de Servicios de Internet**…, ob. cit., p. 52.
[24] RICO CARRILLO, Mariliana: **El ejercicio de los derechos fundamentales y las libertades públicas a través de Facebook**. Revista Derecho y Tecnología de la Universidad Católica del Táchira, No. 14, año 2013. p. 117-118.

ser captados tanto por los proveedores de servicio como por el resto de los usuarios de la red, situación que plantea la aplicación de la normativa sobre protección de datos personales a estos sujetos.
La profesora Mariliana Rico Carrillo, establece que en estos casos para que se dé lugar a la aplicación de la normativa española sobre protección de datos será necesario el cumplimiento de tres (3) requisitos:
(i) que se trate de datos de carácter personal,

(ii) que el usuario de la red ostente la cualidad de interesado,

(iii) que realmente se produzca un tratamiento de datos en los términos indicados en la ley.

2º con la realización de actividades por el usuario una vez registrado o que ha creado su cuenta, en particular se trata de la información que es colocada de manera voluntaria por el usuario de la red, que puede ser accedida y/o utilizada por terceros, en perjuicio de la privacidad de su creador.

3º con la cancelación de la cuenta, se refieren específicamente a la problemática que causa la indexación de los perfiles en los diferentes buscadores, ya que aunque los usuarios se hayan dado de baja de la Redes Sociales, su información no se desincorpora automáticamente en las bases de datos de los buscadores.

En la búsqueda de la protección de los datos de los usuarios de las Redes Sociales, las leyes que regulan la materia, han incorporado ciertos compromisos que los responsables de los ficheros de datos recogidos y almacenados deben cumplir, tales como el principio de responsabilidad (*accountability*) o el principio de privacidad por defecto.

El principio de responsabilidad (*accountability*) conlleva la obligación por parte del responsable del fichero de datos de aplicar los principios de la protección de datos. La inclusión de dicho principio en las legislaciones nacionales sobre protección de datos se centraría en dos elementos principales: i) la necesidad de que el responsable del tratamiento adopte medidas adecuadas y eficaces para aplicar los principios de protección de datos; y ii) la necesidad de demostrar, si así se requiere por parte de la autoridad de control independiente o por el propio titular de los datos, que se han adoptado medidas adecuadas y eficaces; así pues, el responsable del tratamiento de datos deberá aportar pruebas.[25]

[25] Grupo de Trabajo de Protección de Datos del Artículo 29. Dictamen 3/2010 sobre el principio de responsabilidad. Adoptado el 13 de julio de 2010. [Disponible en línea] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_es.pdf (Última consulta: 01/11/2016) Este Grupo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata de un organismo europeo, con carácter consultivo e independiente, para la protección de datos y el derecho a la intimidad. Sus funciones se describen en el artículo 30 de la Directiva 95/46/CE y en el artículo 15 de la Directiva 2002/58/CE. Desempeña las labores de secretaría la Dirección C (Derechos Fundamentales y Ciudadanía de la Unión) de la Comisión Europea, Dirección General de Justicia, B-1049 Bruselas, Bélgica, despacho LX-46 01/190. Página web: http://ec.europa.eu/justice/policies/privacy/index_en.htm (Última consulta: 19/11/2016)

Por su parte, el principio de privacidad por diseño (*Privacy by Design*), parte del concepto fue acuñado en la década de los noventa por Ann Cavoukian, Comisionada de Información y Privacidad de Ontario, Canadá; y refiere tanto a una filosofía como a un enfoque por el cual la privacidad se encuentra integrada en el diseño tecnológico mismo, consistente con la arquitectura del sistema de información y con el modelo de negocios. Se presenta como una forma de asegurar que la privacidad va a estar garantizada ante los cambios tecnológicos.[26]

Y finalmente citaremos el principio de privacidad por defecto (*Privacy by Default*), que para algunos autores forma parte de la privacidad por diseño, no obstante, en nuestra consideración se trata de un principio autónomo que conduce a que la necesidad de que la persona otorgue su consentimiento para compartir sus datos. Así, la privacidad por defecto se refiere a que cualquier sistema ha de estar configurado de forma que, por defecto otorgue una mayor protección a la privacidad de las personas, de modo que, no se comparta la información del usuario salvo que éste realice una acción o cambie su configuración. La privacidad por defecto otorga un mayor control sobre la propia información ya que, el usuario está protegido aunque no haga ninguna acción y decide libremente cuándo, cómo y con quién, comparte sus datos.[27]

A esta lista de principios también se les suma otras prácticas deseables que deben adoptar las Redes Sociales para la protección de los datos personales, tales como la incorporación de códigos de conductas para los usuarios, la identificación clara y precisa sobre las políticas de almacenamiento y de las llamadas *Cookies*,[28] entre otras; el tratamiento exhaustivo de todas estas harían nuestro trabajo infinito o de imposible publicación, ya que mientras yo escribo y usted lee se están creando nuevas Redes Sociales y nuevas aplicaciones tecnológicas con igualmente nuevos retos para la ciencia jurídica en cuanto a los derechos de protección de los datos de carácter personal.

CONCLUSIÓN:

El uso de la tecnología para crear y compartir información personal, es algo que marca estos tiempos, lejos quedaron aquellos álbumes de fotos familiares casi de color amarillo o los diarios con llave que guardaban los mayores secretos de las niñas; ahora toda esa información se encuentra en la red; produciendo un cambio en nuestra psiquis, ya que si antes nos angustiaba que la gente supiera esa información, ahora nos entristecemos si en el *Facebook* no tenemos amigos o si el número de *link* es escaso en las fotos publicadas.

---

[26] Ver más sobre *Privacy by Design* en el trabajo de profesora BRIAN NOUGRÈRES, Ana: **La protección inteligente de los datos personales: *Privacy by Design* (PbD).** Universidad de los Andes. Facultad de Derecho (Bogotá, Colombia) No. 1 Julio - Diciembre de 2012. [Disponible en línea] https://habeasdatacolombia.uniandes.edu.co/wp-content/uploads/ok6_-Ana-Brian-Nougreres_FINAL.pdf (Última consulta: 19/11/2016)

[27] VIVET TAÑA, Laura: **Big Data y *Privacy by Design* (PbD)**. Observatorio Iberoamericano de Protección de Datos. [Disponible en línea] http://oiprodat.com/2014/07/23/big-data-y-privacy-by-design-pbd/ (Última consulta: 01/11/2016).

[28] Cookies es una pequeña información enviada por un sitio web y almacenada en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario, de allí los problemas en materia de protección de datos de carácter personal.

Así como ha dicho Manuel Castell, "Vivimos en un mundo de extraordinaria capacidad comunicativa, que es la actividad más fundamental, pero en un mundo que al mismo tiempo –las instituciones, las organizaciones- la organización de la sociedad está muy por detrás de los que podríamos hacer."[29] Las instituciones jurídicas están llamadas a acometer la tarea de legislar para la complejidad de las situaciones que se dan en esta sociedad de redes.

Uno de los principales esfuerzos para tratar de poner al día a la sociedad con respecto a los avances tecnológicos, se inicia en la Resolución 56/183 de fecha 21 de diciembre de 2001 de la Asamblea General de las Naciones Unidas[30] que aprobó la celebración de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), que concluyó en la elaboración de una *Declaración de Principios para Construir la Sociedad de la Información* como un desafío global para el nuevo milenio.

Dentro de estos principios destacaban que las relaciones existentes en la Sociedad Red debían estar enmarcadas en el respeto a la paz y los valores fundamentales de libertad, igualdad, solidaridad, tolerancia, responsabilidad compartida y respeto a la naturaleza; reconociendo la importancia de la ética para la Sociedad Red, para fomentar la justicia, así como la dignidad y el valor de la persona humana.

Debiéndose acordar la protección más amplia posible a la familia y permitir que ésta desempeñe su papel cardinal en la sociedad. También, el uso de las tecnologías de información y comunicación en la creación de contenidos respetando los Derechos Humanos preexistentes y las libertades fundamentales de todos los individuos, lo que incluye la privacidad personal y el derecho a la libertad de opción, conciencia y religión de conformidad con los instrumentos internacionales relevantes.

Atendiendo al papel de todos los actores de la Sociedad Red, ya que no se refiere a un Estado en particular y sus relaciones con sus ciudadanos, sino a todas las personas que convergen en esta sociedad, y su deber de adoptar las acciones y medidas preventivas apropiadas, con arreglo al derecho, para impedir la utilización abusiva de las tecnologías de información y comunicación, tales como actos ilícitos o de otro tipo motivados por el racismo, la discriminación racial, la xenofobia, y las formas conexas de intolerancia, el odio, la violencia, todo tipo de maltrato de niños, incluidas la pedofilia y la pornografía infantil, así como la trata y la explotación de seres humanos.

Por supuesto, la incorporación a través de la regulación nacional de las estrategias que permitan garantizar la protección de datos personales, enmarcados en los principios fundamentales recogidos en los derechos ARCO; es decir, acceso, rectificación, cancelación u oposición de información, así como la seguridad, custodia y consentimiento para la transmisión.

---

[29] CASTELL, Manuel: **Sociedad Red.** Video publicado el 17 de enero de 2014. [Disponible en línea] https//:www.youtube.com/6afd6fef-0de2-44f3-b271-da882744c75f (Última consulta: 19/11/2016).

[30] Asamblea General de las Naciones Unidas: **Resolución 56/183**. 21 de diciembre de 2001. [Disponible en línea] http://www.itu.int/net/wsis/docs/background/resolutions/56_183_unga_2002-es.pdf (Última consulta: 01/11/2016)

Los principios de protección desarrollados tanto por la doctrina como por la jurisprudencia mundial, nunca como ahora resultan tan relevantes para proteger la privacidad e intimidad de las personas, sobre todo cuando estamos utilizando cada vez más, y de manera casi imprescindible, de las tecnologías de la información.

En este sentido, la Cumbre Mundial sobre la Sociedad de la Información acordó que "para el 2015 todas las poblaciones de la Tierra deberán estar incorporadas al uso de las Tecnologías de Información y Comunicación con una visión más solidaria y de responsabilidad en el uso y los contenidos que son desarrollados en la Sociedad de la Información", parece que nuestro país está en mora al cumplimiento de este acuerdo, pero como dice el adagio popular…*nunca es tarde cuando la dicha es buena*.

GESTIÓN DE CAMBIO Y BRECHA DIGITAL EN SOCIEDADES VULNERABLES

Por: ***Katty Pérez Ordóñez y***
Krishna Julio Espinoza
Perú

De conformidad con el Primer objetivo de la Agenda Digital para América Latina y el Caribe (e-LAC2018) que demanda "masificar y universalizar el acceso a los servicios digitales y producir contenidos, argumentando la inclusión de los grupos vulnerables", es nuestro propósito desarrollar, con una especial referencia, un procedimiento digital que direccione "LA PRODUCCION DE CONTENIDOS" con el afán de promover nuevas alternativas de acceso a las Tics, con contenidos que promuevan la gestión del cambio en favor del desarrollo regional y nacional. Pues, los estudios socio-económicos y las estadísticas oficiales señalan que en las regiones agro extractivas de América Latina, existen dos problemas centrales que acrecientan el malestar social: La pobreza campesina y de los estratos urbanos marginales, y la desocupación y sub-ocupación de técnicos y profesionales de nivel medio y universitario. Estos problemas se pueden solucionar, desarrollando un Proyecto Nacional para la Educación y Capacitación Digital permanente, destinada a aquella población vulnerable que mayoritariamente habita en comunidades campesinas y barriadas urbanas marginales de las principales ciudades del país.

Según el Banco Mundial (BM), la Brecha digital en el Perú, es una de las más altas de América Latina. Un informe recogido el 15 de enero del 2016, sostiene que "si bien internet, la telefonía móvil y otras tecnologías digitales se están extendiendo rápidamente en todo el mundo en desarrollo, los dividendos digitales esperados -mayor conocimiento, más empleo y mejores servicios públicos- están por debajo de las expectativas y el 60& de la población mundial, sigue sin poder participar en la economía digital."

El Índice de Adopción Digital (IAD-BM) al mostrar un rango de porcentaje de 0 a 1 (donde 0 constituye la mayor brecha digital y 1, la menor) el Perú obtiene un índice de 0.51, es decir; el nivel más alto de América Latina, que solo supera a Paraguay y Bolivia. En las variables evaluadas, el Estado peruano muestra una mayor adopción con un índice de 0.65 y la ciudadanía con un índice de 0.49, los negocios con 0.39 y de ellos el 56% cuentan con un WebSite y el acceso a Internet en los hogares constituye el 30% de la población.

Por su parte, el Organización Mundial de Comercio, al sostener que, "la inclusión social propone la creación de entornos favorables en los e-servicios, e-comercio, la administración pública digital, la modernización del acceso a los recursos tecnológicos y la brecha digital, se miden teniendo en cuenta una variedad de factores económicos, sociales, políticos y culturales. Siento que para un país en vías de desarrollo, la tele densidad en líneas fijas es inferior al 20% y en países desarrollados supera el 80%".

La Unión Internacional de Telecomunicaciones (www.itu.ch) señala que el índice de acceso digital (IAD) está diseñado sobre la base de cuatro factores:

- La infraestructura, se mide tomando la densidad telefónica móvil y fija.

- La asequibilidad, se mide a partir del precio del servicio de acceso a internet
- El conocimiento, se mide con el índice de alfabetización de adultos y el promedio de matrícula escolar de primaria y secundaria
- La calidad, se mide tomando el ancho de banda internacional de internet (per cápita) y el número de abonados de banda ancha por cada 100 habitantes.

Para Volkow (2003) "La brecha digital es un concepto social que presenta tres dimensiones: 1) el Comercio electrónico. 2) La sociedad de la información, y 3) Gobierno electrónico". Sin embargo, y dados los usos actuales, falta un apartado importante que cobra gran importancia en las TIC y que es el e-aprendizaje, es decir, el uso de internet para la adquisición de competencias laborales. En tanto las valoraciones en la lucha contra la brecha digital son: la coherencia, la pertenencia y la relevancia de las acciones y tener en cuenta cuatro aspectos: infraestructuras; habilidades y competencias; oferta de información y cambios en las acciones de inclusión.

Maya Álvarez (2008) nos dice que el concepto de Cultura Digital, en cambio de Brecha digital, "está englobando diversos temas y a menudo mezclan dos aspectos que tienen diferencias importantes, el primer aspecto hace referencia al hecho de incorporar a nuestras vidas los instrumentos y herramientas digitales, el otro aspecto tiene que ver con la cultura derivada de la que conocemos como sociedad del conocimiento y los procesos productivos", en cuyo contexto comparativo, en el área de nuestro estudio no se ha incorporado al modo de vida campesino y urbano marginal los instrumentos y herramientas digitales, menos la cultura derivada de la sociedad del conocimiento en vista que la pequeña y mediana empresa, la producción artesanal y artística, así como las actividades agropecuarias mayoritariamente no utilizan ni siquiera el teléfono móvil para el proceso productivo, como solo para la comunicación telefónica y actividades distractivas.

Pues, como agrega el mismo autor, "…existen nuevos elementos que están teniendo un impacto importante y que ofrecen nuevas oportunidades: el alto nivel de penetración inalámbrica en el mundo, mejor y mayores anchos de banda, aplicaciones como las Web 2.0 que están transformando el alcance de Internet en la estructura económica y social: weblogs, wikis, podcasts, webservices etc. Esto define una de las características más peculiares de la tecnología: el avance vertiginoso y continuado al que hay que hacer frente y que precisa de una actitud y capacitación precisa para hacerles frente".

El término que está alcanzando una gran proyección social es el de Web 2.0 o Web de Nueva Generación (WebNG). dado por la evolución de una categoría de herramientas, servicios y programas que se denominan de software social, pero con la peculiaridad que no es producida por los ingenieros sino construida en la red. En esta línea está la explosión de blogs en Internet, los espacios de gestión de redes sociales, el auge de la imagen y la TV a través de Internet, el fenómeno Second Life etc.

De allí que el uso y accesibilidad de las Tics y su aplicación a los procesos productivos en nuestro país, originaria masivamente la obtención de un mayor valor agregado de la

producción andina y marginal de acuerdo a las ventajas comparativas de cada ecosistema. Influiría en una mayor especialización de la fuerza laboral y mejoraría su productividad, su competitividad e ingresos, puesto que la producción estaría íntimamente ligada a los requerimientos del mercado y de los consumidores, además de la seguridad y el cumplimiento de todas las contingencias de salubridad que exige la figura de los negocios por internet.

El procedimiento de la Educación digital y la capacitación exclusiva mediante la alfabetización digital orientada a poblaciones vulnerables, hasta la actualidad, no ha dado resultados positivos, en vista que la Gestión del cambio tecnológico, inclusive utilizando el e-Learning solidario propuesto por Peña Cabrera (2004) no cuenta con un amparo o justificación que fundamente la gestión del cambio, basado en la producción material de bienes y servicios, al observar por ejemplo, que dicho e-Learning solidario, está dirigido exclusivamente a "la sensibilización de la sociedad sobre temáticas disciplinarias del ámbito de la solidaridad, la cooperación, el desarrollo, la cultura de paz y la sostenibilidad, etc.".

En cambio, debió estar dirigido a la formación y capacitación del propio personal laborioso, de las cooperantes y productores vinculados a los ámbitos de la pequeña y mediana empresa, la producción agropecuaria de comunidades y la artesanía marginal. Además de definir el e-Learning como el conjunto de actividades necesarias para la puesta en marcha y uso de un entorno de formación a distancia por internet (online) mediante el uso de las tecnologías de información y comunicaciones. Caracteriza el e-Learning con una doble dimensión, por un lado, el aspecto pedagógico que debe adaptar los procesos enseñanza-aprendizaje a las características de la tecnología que constituye un conjunto de herramientas y aplicaciones SOFTWARE en formato web, que se denominan plataformas virtuales o plataformas de tele formación o e-Learning.

TIPOS DE BRECHA DIGITAL

La unión Internacional de Telecomunicaciones, reconoce que existen tres tipos de brecha digital:
Brecha de acceso, que está basada en la diferencia entre los que acceden y no acceden a las Tics.
Brecha de uso, basada en la diferencia de los que saben y no saben usar las Tics.
Brecha de calidad de uso, basada en las diferencias entre los usuarios.

Sin embargo, estas diferencias están referidas a los problemas de conectividad que hoy se amplia, dada la preocupación por la capacitación y educación digital para sostener diferencias en el uso a partir del aprendizaje, que conlleva a la transformación de la información en conocimiento, situación que conlleva la implementación de nuevas estrategias y metodologías de aprendizaje, que en su generalidad propician las innovaciones tecnológicas, los intelectuales, profesionales y estudiantes universitarios, específicamente tesistas. Este tipo de brecha digital se denomina "Brecha Cognitiva", que a propósito de "cambiar de mente y la forma de hacer las cosas" y dominar los avances tecnológicos, se puede forzar y convivir con la inteligencia artificial, la computación cognitiva, la realidad

virtual, los wearables, beatcons, sensores digitales y plataformas de creatividad *Machine Learning*, biotecnologías, Smart industries, robótica y automatización.

Desde que la brecha digital se basa en la posibilidad o nivel de acceso a las Tics, para Pippa Norris (citado por Espósito Caballero en "Brecha Digital, Desigualdad y Pobreza en la Sociedad del Conocimiento") se trata de un fenómeno que implica tres aspecto principales: La Brecha Global (que se presenta entre distintos países), la Brecha Social (que ocurre al interior de una nación) y la Brecha Democrática (que se refiere a lo que existe entre quienes participan y quienes no participan de los asuntos públicos en línea.

En forma específica, el investigador holandés Jan Van Dijk, identifica cuatro dimensiones en el acceso: "a motivación para acceder, el acceso material, las competencias para el acceso y el acceso para usos avanzados… puede apreciarse que la Brecha digital en cuanto conexión a la Red, es significativa, entre y dentro de cada región. África lleva la peor parte teniendo el 14.31% de la población mundial, solo el 5.35% de su población cuenta con acceso al servicio. Esta situación se da incluso en el mundo desarrollado, pues puede apreciarse que en Europa el número con acceso al servicio está por debajo del 50% de su población. Es significativo que solo el 21.92% de la población mundial tiene acceso a internet.

El 51.76% ya utiliza telefonía móvil y hay un ordenador por cada ocho personas. El único continente que aprueba en accesibilidad es Europa, con un índice de 0.55, América queda en 0.40, Asia en 0.38, Oceanía en 0.33 y África en 0.20. Solo el 2.5% de la población mundial tiene una conexión de banda ancha a internet y la mayoría están en América del Norte y Europa (donde el porcentaje es de 5.6% y 5.4% respectivamente) mientras que en África la proporción no llega ni al 0.1%."

Según Maya Álvarez (Gaceta Antropológica 2008, 24 (2)) existen tres tipos de brecha digital: Brecha de Género, se refiere a la relación de internautas por sexo, donde claramente se observa a nivel mundial el dominio de los hombres en 53.7% frente el 49.0% de mujeres.

Brecha Territorial, referente a la diferencia de uso entre zonas rurales y urbanas para la diversificación de las actividades económicas. Brecha Generacional, que se refiere a la conectividad por edades, niños, jóvenes, adultos mayores, etc.

Según Internet World Stats, actualizado a diciembre de 2008, hay algo más de 1,400 millones de internautas de los que el 60% viven en los países industrializados. En Europa hay 384 millones de usuarios mientras que en áfrica hay 51 millones (https://www.internetworldstats.com/stats.htm) sin embargo hay un crecimiento espectacular en Asia en los últimos años que colocan a este continente en la cabeza del número de usuarios de Internet. Si atendemos al grado de penetración en la población de internet podemos ver que África presenta menos de un 5%, mientras en el polo opuesto Norteamérica está en un 73% o Europa en un 48%.

GRADO DE PENETRACION CONTINENTAL DE INTERNET

WORLD INTERNET USAGE AND POPULATION STATISTICS DEC 31, 2017 - Update						
World Regions	Population (2018 Est.)	Population % of World	Internet Users 31 Dec 2017	Penetration Rate (% Pop.)	Growth 2000-2018	Internet Users %
Africa	1,287,914,329	16.9 %	453,329,534	35.2 %	9,941 %	10.9 %
Asia	4,207,588,157	55.1 %	2,023,630,194	48.1 %	1,670 %	48.7 %
Europe	827,650,849	10.8 %	704,833,752	85.2 %	570 %	17.0 %
Latin America / Caribbean	652,047,996	8.5 %	437,001,277	67.0 %	2,318 %	10.5 %
Middle East	254,438,981	3.3 %	164,037,259	64.5 %	4,893 %	3.9 %
North America	363,844,662	4.8 %	345,660,847	95.0 %	219 %	8.3 %
Oceania / Australia	41,273,454	0.6 %	28,439,277	68.9 %	273 %	0.7 %
WORLD TOTAL	7,634,758,428	100.0 %	4,156,932,140	54.4 %	1,052 %	100.0 %

Fuente: https://www.internetworldstats.com/stats.htm

Otros autores identifican varios tipos de brecha o diferencias en el acceso a las Tics, siendo las más comunes, la brecha de género, brecha territorial y brecha generacional. En cambio la Unión Internacional de Telecomunicaciones propone que hay tres tipos de brecha digital: la de acceso, basada en la diferencia entre las personas que pueden acceder y las que no a las TIC; la de uso, basada en las personas que saben utilizarlas y las que no; y las de la calidad del uso, basada en las diferencias entre los mismos usuarios. Es obvio que el concepto de brecha digital se ha modificado con los años, ya que, en un principio se refería a los problemas de conectividad y después de eso se empieza la introducir la preocupación por la capacitación y educación requeridas para utilizar las TIC, así como el uso de los recursos tecnológicos y es por esto que, muchas de las organizaciones internacionales han definido una política de desarrollo orientada a la reducción de la brecha digital, la misma que hoy se concierte en Brecha Cognitiva, que enfatiza la importancia de transformar la información en conocimiento, gracias al continuo cambio y transformación de la tecnología digital.

Finalmente, el papel de la Brecha digital en la configuración de la sociedad del conocimiento, constituye un indicador de las desigualdades y diferencias referidas al nivel del acceso y uso de las Tics. Espósito Caballero (2011) dice, es una expresión que hace referencia a la diferencia socio económica entre aquellas comunidades que tienen internet y aquellas que no. Aunque tales desigualdades también se pueden referir a todas las nuevas tecnologías de información y comunicación (TIC) como el computador personal, el teléfono móvil, la banda ancha y otros dispositivos. Como tal, la Brecha digital, se basa en diferencias previas al acceso a las tecnologías. Este término hace referencia a las diferencias que hay entre grupos según su capacidad para utilizar las Tics de forma eficaz, debido a los distintos niveles de alfabetización y capacidad tecnológica.

De allí, que la Cumbre Mundial sobre la Sociedad de la Información (CMSI) que creo la *Comunication Rights in the Information Society* (CRIS) enfatiza que "el rol de las nuevas tecnologías como herramientas de comunicación y valoraciones comunes entre grupos, individuos y organizaciones sociales, no considera ni las barreras culturales y lingüísticas, ni

las relaciones de dependencia y subordinación técnica, económica y política entre y dentro del norte y sur del mundo". En tanto la Brecha Digital puede medir las desigualdades provenientes del nivel de acceso y uso considerando las diferencias, distancias o dimensiones de la desigualdad que puede manifestarse entre personas ricas y pobres, entre poblaciones, regiones y lugares de residencia, especialmente en áreas geográficas extensas, como es el caso de las distancias entre comunidades y poblaciones aborígenes y residentes de las zonas periféricas de las principales ciudades del Perú. .

POBREZA Y ACCESO A LAS TICS

El problema de la pobreza y la exclusión social y digital en el Perú, constituyen fenómenos que acrecientan la división de la sociedad entre los beneficiarios del desarrollo tecnológico moderno y los excluidos que conforman los márgenes de la Brecha Digital y que sobreviven en condiciones inferiores al logro de un salario mínimo vital (mortal) por cuanto su "modo" de producción y de trabajo se realiza en condiciones de precariedad y carencias extremas que diseminan sus consecuencias sobre el hambre y la falta de educación, salud y trabajo, en tanto dicha pobreza, además es entendida como carencia de recursos productivos y tecnológicos, como ausencia de elementos esenciales para la subsistencia, como insuficiencia de medios, instrumentos y herramientas necesarias para combatir la desocupación, la explotación y la desdicha de subsistir en un país con desigualdades, donde un pobre apenas puede vivir con S/. 3.30 por día o S/. 338.00 mensuales, mientras en congresista o ministra puede gozar de un sueldo mayor a los S/. 1,000.00 diarios, más las dádivas de la corrupción, las asesorías y el poder ilimitado. Pues, según las metodologías de medición de la pobreza, se es pobre extremo cuando lo se logra satisfacer siquiera una de las necesidades básicas de educación, salud, vivienda y servicios de agua, desagüe, electricidad, telefonía y comunicaciones, etc. Y cuando en el Perú se utiliza el gasto como indicador de bienestar, las recientes noticias (abril 2018) nos dicen que la pobreza monetaria en el Perú sube por primera vez en este milenio, y fue Lima donde se registró el mayor incremento (la mitad del total nacional).

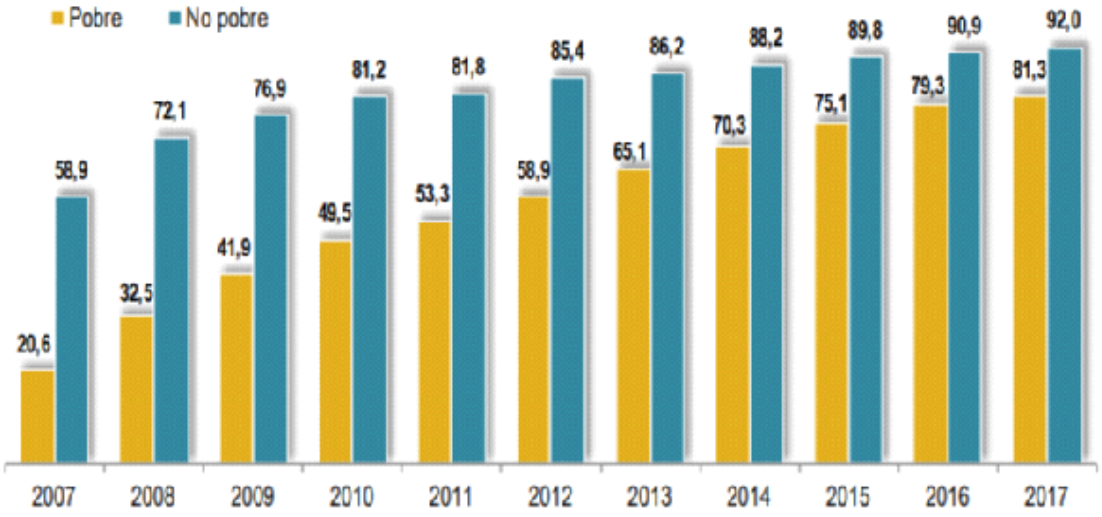
La pobreza monetaria afectó al 21.7% de la población del país en el 2017, informó el Instituto Nacional de Estadística e Informática (INEI). Es decir, 375 mil peruanos abandonaron la clase media y pasaron a la pobreza en el último año, un punto porcentual más que en la medición anterior de la Encuesta Nacional de Hogares (Enaho) cuando fue de 20.7% y para no faltar a la verdad, en mayo de 2018 subió el impuesto al consumo selectivo en una tasa de dos puntos porcentuales

Bajo estas condiciones que delimitan con la tragedia humana, percibimos una doble contradicción, al proponer el aminoramiento de la Brecha Digital como medio de inclusión social, precisamente, educando y capacitando a la población pobre, marginal y excluida. Pero si este sector de la población "no tiene ni para comer", ¿Cómo? Y ¿Para qué? Integrarla en la sociedad del conocimiento y la inteligencia virtual y precisamente, el cómo sugiere una alianza estratégica del Derecho Informático y un Proyecto Nacional para la educación y capacitación digital permanente, ligado a la pequeña y mediana producción agropecuaria, manufacturera y artesanal de comunidades campesinas y estratos urbanos marginales. Y el ¿Para qué? Para integrar e incluir masivamente a la población vulnerable al proceso de producción de la modernidad digitalizada, para mejorar sus capacidades laborales mediante la optimización de los recursos y herramientas creativas que proporcionan las Tics.

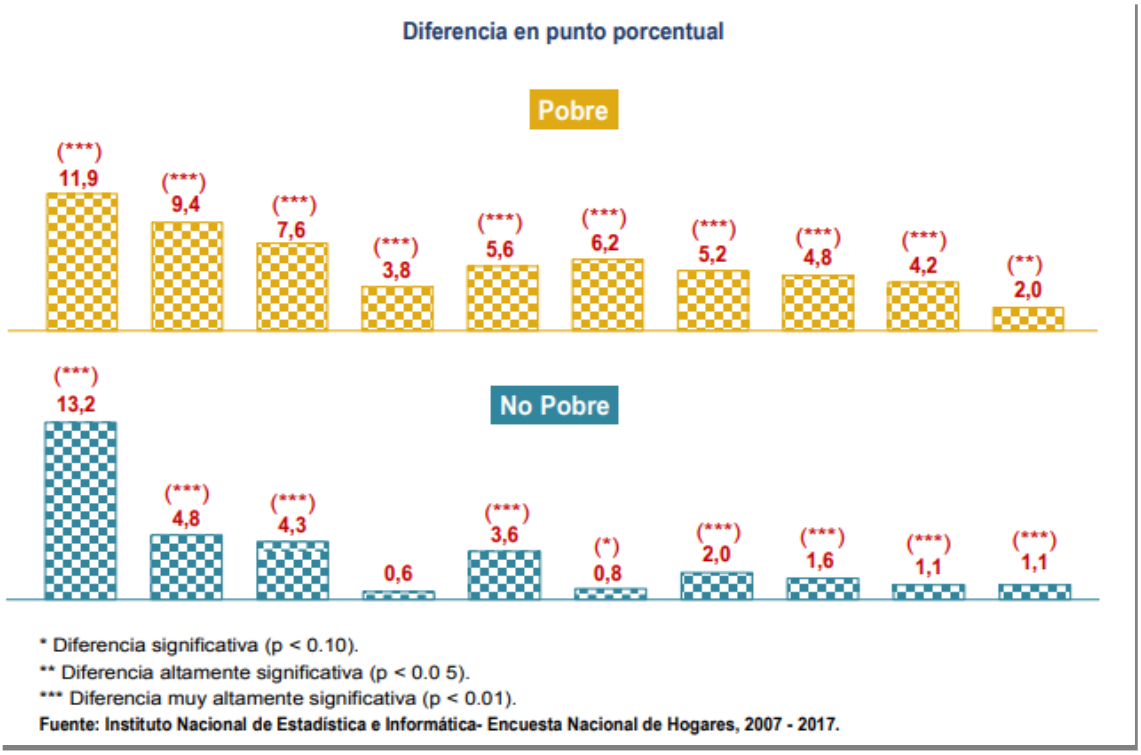
Porque no se trata de la cuestión del cambio del modelo industrial clásico a un módulo tecnológicamente robotizado y automatizado, sino de la Gestión de Cabio Ocupacional Integrado (en su complejidad) por la infraestructura de interconexión y conectividad y el aprendizaje del uso de información como herramienta de trabajo para la producción de bienes y servicios digitalizados.

Ahora bien, la información sobre Tecnologías de Información y Comunicación (TIC) según condición de pobreza de los hogares, proporcionada por el INEI permite conocer el nivel de acceso a estos medios y determinar la brecha digital existente entre los pobres y los no pobres. Al comparar los resultados con el año 2016, se observa un incremento en los hogares pobres con acceso a las tecnologías de información y comunicaciones. Aumentó en 2,0 puntos porcentuales los hogares que tienen al menos un miembro con celular, al pasar de 79,3% a 81,3%, siendo este crecimiento altamente significativo. También se incrementa en 1,1 puntos porcentuales los que tienen televisión por cable y acceso al servicio de internet (11,3% a 12,4% y 3,0% a 4,1% respectivamente). En general el incremento observado entre los hogares pobres a las TIC, acorta la brecha existente entre los hogares pobres y no pobres. Esta misma tendencia se observa entre los hogares no pobres, donde también aumentó el acceso a las TIC. En relación al uso de teléfono fijo, se observa una reducción tanto en los hogares pobres (0,1%) y no pobres (1,7%).

PERÚ: HOGARES CON ALGÚN MIEMBRO CON CELULAR, SEGÚN CONDICIÓN DE POBREZA, 2007 – 2017
(Porcentaje)



Fuente: Instituto Nacional de Estadística e Informática - Encuesta Nacional de Hogares, 2007-2017.



GESTIÓN DE CAMBIO

Uno de los instrumentos generadores de la Gestión del Cambio en el continente, constituye la Agenda Digital para América Latina y el Caribe (e-LAC2018) cuya misión es "desarrollar un ecosistema digital en América Latina y el Caribe, donde uno de los factores críticos que ambicionan el desarrollo digital, es el despliegue de la banda ancha y la construcción de capacidades y habilidades". Ecosistema digital, cuyo diagnóstico, para el caso peruano, señala que "El acceso a las Tics en el Perú, se ha caracterizado por presentar grandes diferencias entre zonas geográficas, por áreas urbanas y rurales." Esto se debe a que el país presenta una geografía bastante accidentada, así como una población dispersa, lo cual limita el despliegue de las redes de telecomunicaciones, especialmente en las zonas de Sierra y Selva, que es donde se encuentra presente la población rural. Pues, según el Instituto Nacional de Estadística e Informática (INEI) la población peruana asciende a 31'151,000 habitantes al 2015, el 22% de las cuales pertenece a la población rural pobre.

PERÚ: EVOLUCIÓN DE LOS HOGARES CON ACCESO A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES, SEGÚN CONDICIÓN DE POBREZA, 2007-2017

(Porcentaje respecto del total de hogares de cada condición de pobreza)

Condición de pobreza/ Tecnología de Información y Comunicaciones	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Diferencia (en puntos porcentuales) 2017-2016	Diferencia (en puntos porcentuales) 2017-2007
Pobre													
Con teléfono fijo	7,8	7,3	6,5	6,6	6,1	6,2	6,4	5,0	4,1	3,2	3,1	-0,1	-4,7
Con algún miembro con celular	20,6	32,5	41,9	49,5	53,3	58,9	65,1	70,3	75,1	79,3	81,3	2,0	60,7
Con Tv. cable	3,1	3,7	4,3	4,9	7,9	7,6	9,7	10,7	10,8	11,3	12,4	1,1	9,3
Con Internet	0,1	0,2	0,2	0,6	1,3	1,6	2,5	2,4	2,3	3,0	4,1	1,1	4,0
Pobre extremo													
Con teléfono fijo	0,2	0,5	0,1	0,5	1,2	0,9	0,6	0,8	0,5	0,6	0,1	-0,5	-0,1
Con algún miembro con celular	3,2	8,8	20,3	27,1	32,9	40,0	45,6	54,8	61,1	66,8	69,3	2,5	66,1
Con Tv. cable	0,3	0,4	0,0	0,7	1,3	1,0	2,7	1,8	2,6	1,7	2,7	1,0	2,4
Con Internet	0,0	0,0	0,0	0,0	0,0	0,0	0,1	0,1	0,0	0,0	0,3	0,3	0,3
Pobre no extremo													
Con teléfono fijo	10,3	10,0	9,1	8,6	7,5	7,6	7,8	5,9	4,9	3,7	3,7	0,0	-6,6
Con algún miembro con celular	26,5	41,8	50,3	56,7	59,1	64,2	69,8	73,8	78,2	82,0	83,6	1,6	57,1
Con Tv. cable	4,1	4,9	6,0	6,3	9,9	9,4	11,4	12,8	12,6	13,3	14,4	1,1	10,3
Con Internet	0,1	0,3	0,3	0,8	1,6	2,1	3,1	2,9	2,8	3,6	4,8	1,2	4,7
No pobre													
Con teléfono fijo	44,2	43,1	42,1	38,7	37,0	35,7	34,1	31,8	28,9	27,6	25,9	-1,7	-18,3
Con algún miembro con celular	58,9	72,1	76,9	81,2	81,8	85,4	86,2	88,2	89,8	90,9	92,0	1,1	33,1
Con Tv. cable	24,9	27,5	30,5	33,3	36,4	38,5	39,4	41,6	42,3	42,2	42,7	0,5	17,8
Con Internet	10,3	12,5	15,3	17,3	20,9	25,2	26,8	28,2	27,7	31,1	33,2	2,1	22,9

Fuente: Instituto Nacional de Estadística e Informática - Encuesta Nacional de Hogares, 2007-2017.

Sin embargo, se aprecia un ligero desplazamiento de las redes clásicas Radio y TV, por el uso masivo de los "Smartphone", especialmente en la población estudiantil y comercial regional de universidades, tecnológicos, secundarios y primaria. Teléfonos celulares que permiten acceder a mayores aplicaciones y contenidos, pues el acceso al servicio de TV por cable se ha incrementado también pasando del 10.3% en el 2005 al 45.9% en el 2018. El caso del acceso a los Bienes y Servicios Tics de telefonía fija, TV por cable, computadoras e internet, se abarca una gran Brecha Digital entre ámbitos geográficos resaltando el acceso al servicio de TV por cable, al contar con una tasa de acceso de 18% en el área rural (que hace uso de Tecnología Satelital) que también facilita el crecimiento del mercado de internet.

Para el tercer trimestre del 2015, se realizó un total de 17'487,000 conexiones (fijas y móviles) según las estadísticas reportadas por el Dialogo Regional Sobre Sociedad de la Información (DIRSI) sobre la velocidad de descarga de banda ancha fija del servicio brindado que pasó de 2.14 Mbps en el 2019 a 12.66 Mbps en el 2015. Según la encuesta Nacional de Hogares

(Enaho) el acceso a los servicios de internet en el periodo 2007-2014 aumentó en un 9.0%, mientras el porcentaje de hogares en zonas rurales accedió al servicio sólo en un 5%.

El acceso al servicio de internet fijo, ha logrado avances de extensión o alcance muy relativos, en la medida en que a los hogares se les confiere el acceso a un paquete (teléfono fijo, cable e internet) observándose un incremento del servicio por cable (HFC) que brinda servicios de TV, internet y telefonía fija, en forma paralela al Fondo de Inversión en Telecomunicaciones (FITEL) oferta a nivel nacional, la implementación de Internet en zonas rurales, a través del proyecto "Red Dorsal Nacional de Fibra Óptica que consiste en el diseño, despliegue y cooperación de una red de Fibra Óptica interconectada a Lima, 22 capitales de Región y 180 Capitales de provincia, con un tendido de 45 mil Km en infraestructura de telecomunicaciones.

Debido a la masificación del uso de terminales móviles se demuestra el crecimiento del número de conexiones de banda ancha móvil, con un alcance de 15'524 mil a diciembre del 2015. Destacando el uso de la tecnología 4G-LTE en todas las empresas prestadoras de servicio la información brindada por Telefónica, América Móvil y Entel Perú, muestran que el incremento de Internet Móvil, ha pasado la valla del 22% al 46% el 2015.

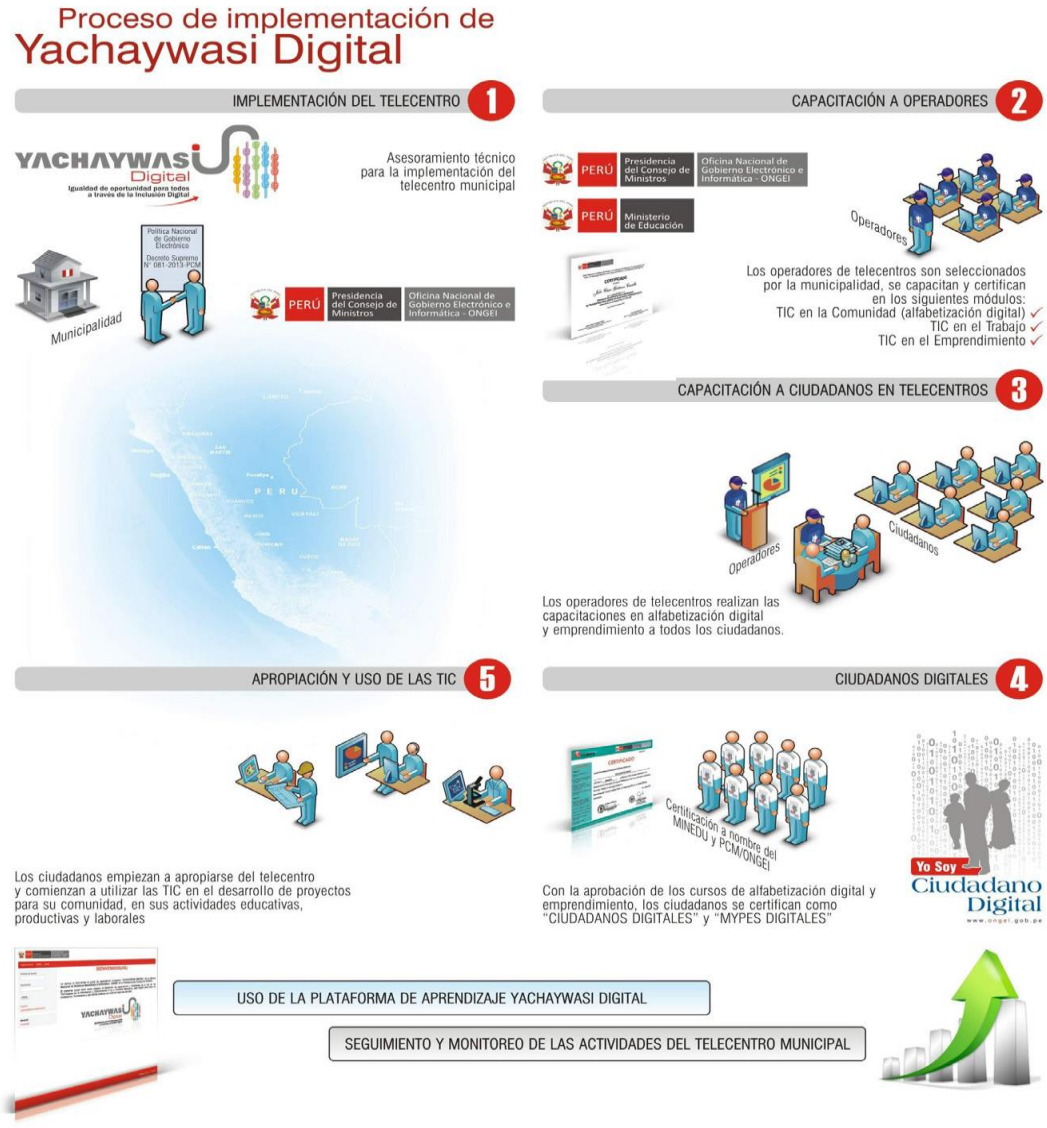
Ahora bien, la Política Nacional de Gobierno Electrónico (2013-2017) que postula "fomentar la inclusión digital de todos los ciudadanos, principalmente de los sectores vulnerables, a través de la generación de capacidades y promoción de la innovación tecnológica, respetando la diversidad cultural y medio ambiente".

En el caso del Proyecto de Inclusión Digital del VRAEM, se observa que es una ventana de oportunidad en el campo normativo, y considerando los efectos que se producirían, se decidió implementar un proyecto de inclusión digital que se encuentra actualmente como piloto en la zona del VRAEM, el cual se desarrolla a través de la creación de espacios de aprendizaje dotados de tecnología y acceso a Internet denominados Yachaywasi o Casa del Saber Digital.

El proyecto de inclusión digital tiene como objetivo desarrollar capacidades en los ciudadanos en el uso y aprovechamiento de las Tecnologías de la Información y Comunicación, así como el desarrollo de las habilidades de pensamiento crítico y colaboración a través de la creación de telecentros, capacitándolos en Programas de Alfabetización Digital, Gobierno Electrónico, emprendedurismo, entre otros, permitiendo reducir la Brecha Digital y apoyando la inclusión social.

El Yachaywasi Digital, promueve el aprendizaje a través del desarrollo de proyectos aplicables a la comunidad por parte de los ciudadanos, además capacita a los jóvenes, mujeres y productores en temas de *marketing* digital, comercio electrónico, constitución de empresas en línea, entre otros, se cuenta con una plataforma *e-Learning*, accesible y de fácil uso, que sirve para el desarrollo de cursos virtuales, así como medio de asesoramiento y seguimiento en línea a los ciudadanos.

Todos los módulos están dirigidos a la población en general y con completamente gratuitos, Citamos por ejemplo: El proceso de implementación de Proyecto Yachaywasi Digital



Fuente: http://www.yachaywasi.org/proyectos/

ESTRATEGIAS JURÍDICAS PARA LOGRAR EL AMINORAMIENTO DE LA BRECHA DIGITAL

En vista que hasta la actualidad no se ha logrado aminorar la Brecha Digital, porque los Programas y Proyectos tienen características experimentales y porque no existe ningún instrumento jurídico que regule la Educación y Capacitación Digital permanente de la población especialmente vulnerable y que se halla en estado de analfabetismo digital. Recurriremos a los Organismos e Instancias que tienen incidencia y competencias estructurales, para que en el Marco Regulatorio de su Jurisdicción, Competencia y Dominio, puedan adoptar y demandar Las Modificatorias y/o Agregados jurídicos para la Educación y Capacitación Digital Permanente, en vista de su relación directa con la población vulnerable,

como el Convenio 169 de la OIT, El Ministerio de Educación del Perú, la Ley 28015 Promoción de Formación de Micro y Pequeñas Empresas (MYPES), la Ley de Comunidades Campesinas, y la Ley General del Ambiente Nº 28611.

En lo que concierne al *Convenio 169 de la OIT*, Consta en la Legislación sobre Pueblos Indígenas con Rango Constitucional, que el Convenio 169 de la OIT, es el instrumento internacional más importante sobre el respeto de los Derecho Humanos de los pueblos indígenas, comunidades campesinas, comunidades nativas, rondas campesinas, pueblos afroperuanos y otros colectivos que se auto identifiquen como indígenas o tribales, aquellos pueblos marginados que hoy la historia tipifica como comunidades atrasadas, incomunicadas y abandonadas por el Estado. Recurrimos a esta instancia mundial, para que, en el Marco Legal de su Dominio pueda Insertar-integrar las Categorías de Educación y Capacitación Digital Permanente, destinada a la Reducción-disminución de la Brecha Digital.

Por tanto, será pertinente acceder a la Dirección General de la Oficina Internacional del Trabajo para la Formalización y Registro de Petición Especial (seguramente canalizada por el Parlamento Andino) Para su Inclusión en el Capítulo 4 del Convenio, que versa sobre: "Ciencia, Tecnología y Educación" Artículo 129, de los Medios de Comunicación, que debe decir: Los medios de comunicación social del Estado y los privados en aplicación de los principios contenidos en la presente es, Fomentar y apoyar las acciones tendientes a <u>la educación y capacitación digital permanente</u>, con miras al mejoramiento tecnológico de la sociedad. Y, como quiera que la OIT garantiza la identidad, autonomía y desarrollo, en los Lineamientos Orientadores de la Educación Ambiental, Art. 127.2.; se puede agregar en el Inciso J) Fomentar y estimular la Educación para el desarrollo de la identidad cultural propia, educación bilingüe, uso y desarrollo de idiomas propios y ACCESO A LAS TICS PARA EL MEJORAMIENTO DE LA CALIDAD DE VIDA DE LA POBLACIÓN VULNERABLE.

La justificación y reforzamiento de los conceptos Educación y Capacitación Digital Permanente, para su inclusión en el Convenio 169 (Ratificado por el Perú mediante Resolución Legislativa Nº 26253) se halla en el propio Art. 2.1.- Los gobiernos deberán asumir la responsabilidad de desarrollar, con la participación de los pueblos interesados, una acción coordinada y sistemática, con miras a proteger las deudas de esos pueblos y a garantizar el respeto de su integridad.
Art. 5.C.- Al aplicar las disposiciones del presente convenio, deberán adoptarse medidas encaminadas a aclarar las dificultades que experimenten dichos pueblos, al afrontar nuevas condiciones de vida y de trabajo.

Ahora bien, el Decreto Legislativo de Promoción y Formación de Micro y Pequeñas Empresas 28015, en el Art. I del Título I, demanda que: *"El presente D.L. tiene por objetivo la promoción de la competitividad, formalización y desarrollo de las micro y pequeñas empresas para la ampliación del Mercado Interno y Externo de éstas en el marco del proceso de formación del empleo, <u>inclusión social</u> y formalización de la economía, para el acceso progresivo del empleo en condiciones de dignidad y suficiencia".* Este dispositivo, no hace ninguna referencia acerca de la Educación y Capacitación digital, por lo que, proponemos incluir en el Título V.- *"Promoción para el Desarrollo y la Competitividad"*, Art. 37, en el siguiente sentido: *"Fomento a la creación de Centros de Alfabetización, Capacitación y acceso a las Tics, para mejorar y ampliar las redes de importación y exportación del mercado*

global". Los trámites que corresponden deberán realizarse ante el Ministerio de Trabajo y Promoción del Empleo que constituye el sector administrativo para la atención de las demandas de rectificación e inclusión jurídica ante el Congreso de la Republica. Por cuanto:

ESTADÍSTICA DE LA MICRO, PEQUEÑA Y MEDIANA EMPRESA (MIPYME)

Más de 1.5 millones de Mipyme formales operan en el mercado peruano en el 2014:

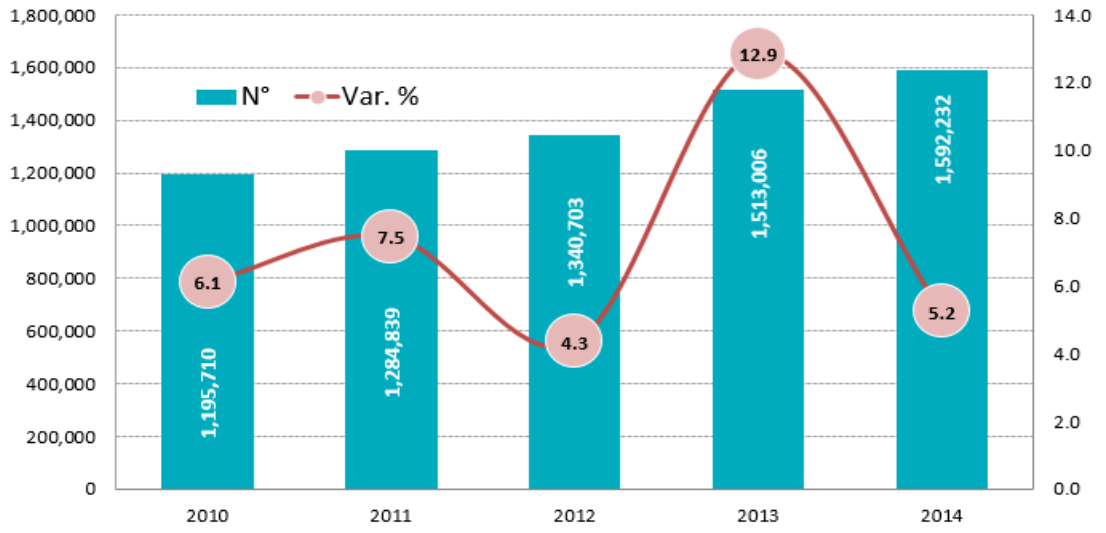
Este segmento empresarial representa el 99.5% del total de empresas formales en la economía peruana - el 94.9% son microempresas, 4.5% pequeña y 0.2% mediana-. De las cuales el 85.2% de ellas se dedican a la actividad de comercio y servicios, y el resto (14.8%) a la actividad productiva (manufactura, construcción, agropecuario, minería y pesca).

Las Mipyme generan alrededor del 60% de la PEA ocupada, considerándose como la fuente generadora del empleo. Asimismo, 10 de cada 100 personas de la PEA ocupada son conductoras de una Mipyme formal

En los últimos cinco años (2010-2014) el número de empresas formales de este segmento se ha incrementado a un ritmo promedio anual de 7.4%. Sin embargo, aún persiste un alto porcentaje de informalidad, ya que el 56% de las MYPE no están inscritas en SUNAT.

En cuanto a las operaciones financieras, sólo el 6% de las Mipyme acceden al sistema financiero regulado. El crecimiento de los créditos destinados al estrato empresarial Mipyme continuó hacia finales del 2014; no obstante, la participación de las colocaciones hacia este estrato crediticio ha empezado a retroceder hasta llegar a su nivel más bajo en el 2014 de los últimos cuatro años (10.8%).

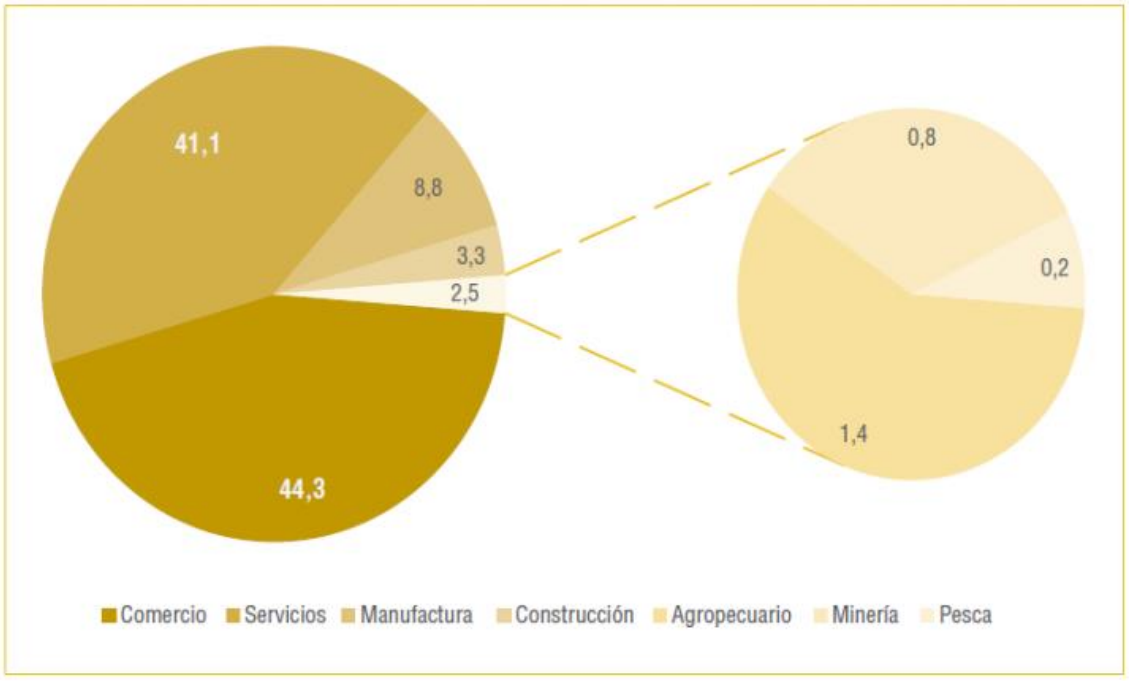
Evolución de las Mipyme formales, 2010-14



Nota: El estrato empresarial es determinado de acuerdo con la Ley N° 30056
Fuente: Sunat, Registro Único del Contribuyente 2010-2014 / Elaboración: PRODUCE –DEMI

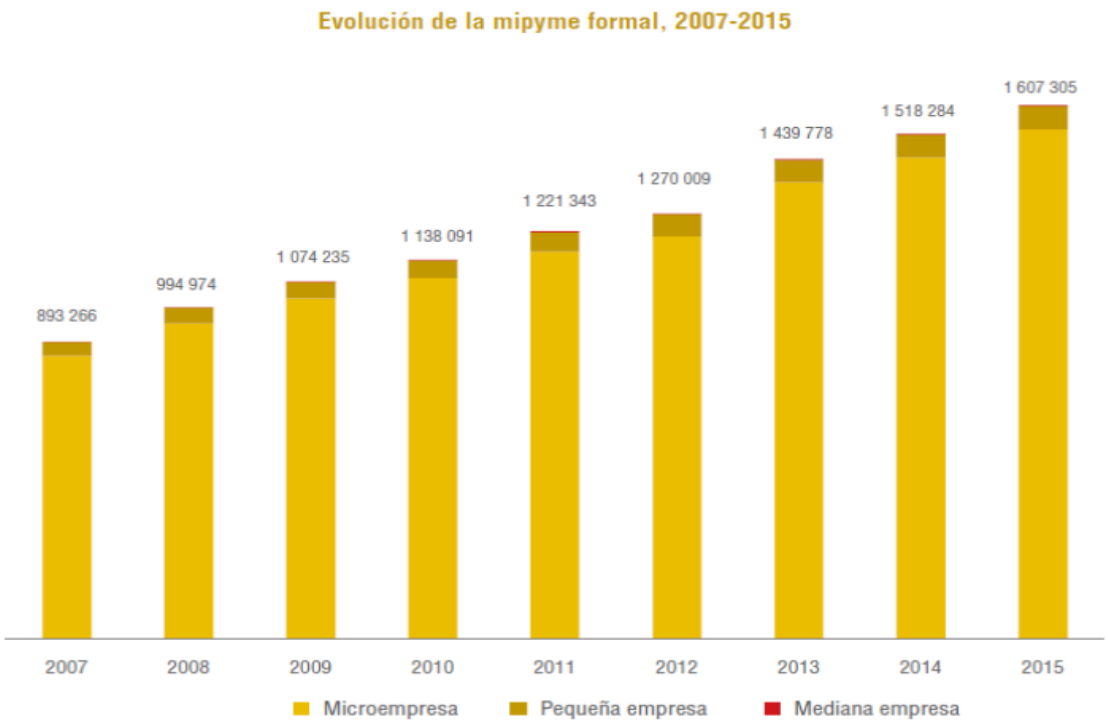
También, se puede apreciar la sectorización de las MYPES por el rubro a que se dedican y se puede apreciar que el 44.3% de ellas se dedican al comercio, mientras que el 41.1% a los servicios y un 8.8% a la construcción, mientras que en menor proporción se dedican al sector agropecuario, minería y al sector de la pesca.

Perú: Mipyme formales, según sector económico, 2010 y 2015



Fuente: Sunat, Registro Único del Contribuyente 2015
Elaboración: PRODUCE - Dirección de Estudios Económicos de Mype e Industria (DEMI)

La evolución de las MYPES desde al año 2007 al año 2015 casi ha duplicado el número de MYPES que existían en el 2007, pasando de 893,266 a 1’607,305 como número de PYMES.



DEFINICIÓN DE UNA MYPE.

La legislación peruana, según el artículo 2 de la ley 28015, define a la PYME (Pequeña y Micro Empresa) como: "...la unidad económica constituida por una persona natural o jurídica, bajo cualquier forma de organización o gestión empresarial contemplada en la legislación vigente, que tiene como objeto desarrollar actividades de extracción, transformación, producción, comercialización de bienes o prestación de servicios (…) debiendo contar con las siguientes características:

Según el artículo 3 de la Ley 28015, las MYPES se diferencias por dos rubros:

Microempresa:

Número total de trabajadores entre uno (1) y diez (10).
Niveles de ventas anuales no mayores a 15 0 UIT.

Pequeña empresa:

Número total de trabajadores hasta un máximo de cincuenta (50).
Niveles de ventas anuales entre 51 y 85 0 UIT"3.

ESTADO DE LA MYPES FORMALES EN LA ACTUALIDAD.

La estructura empresarial peruana del 2015 y 2016 no presenta cambios sustanciales respecto de lo que ha venido ocurriendo en el pasado: la gran mayoría de las empresas son microempresas (95,0%). El estrato de las MYPE presenta una baja participación, con 4,3% de pequeñas empresas y 0,2% de medianas empresas.

Del total de empresas formales 1'607,305 (95%) son micro empresas, 72,264 son pequeñas empresas (4.3%), 2,712 son medianas empresas y solo 8,781 representan a las grandes empresas.
Otra característica más de Las MYPES, es que concentran el 60% de la población económicamente activa (PEA), siendo la microempresa la que más empleos genera con un 53 % y el restante 7% pertenece a la PEA de la pequeña empresa.

Finalmente, en la Ley de Educación se debe agregar en el capítulo correspondiente, la obligatoriedad para cursar y aprobar las materias de Alfabetización Básica Digital en primaria,; Digitalización Intermedia en Secundaria y Digitalización Académica e Investigación en Institutos Superiores y Universidades.

CONCLUSIONES

PRIMERA.

La Brecha Digital en el Perú, abarca el 60% de la población. Y, de acuerdo con la Unión Internacional de Telecomunicaciones, advertimos la presencia de tres tipos de Brecha Digital: Brecha de Acceso. Formas caracterizadas por tener (o no) la oportunidad de ingresar al universo virtual de las Tics.

Brecha de Uso. Personas que saben utilizar (o no) los contenidos (conocimientos) digitales para sus actividades académicas, trabajo, cultura, deportes, ocio, etc.
Brecha de Calidad de Uso. Caracteriza a las personas por grados de integración de las Tics a un modo de vida, en tanto dependen del continuo mejoramiento de la calidad de conocimientos en las Tics.

Asociamos a esta conclusión, las tesis que sostienen la presencia de:

- El analfabetismo virtual, que clasifica a las personas que no tienen ningún conocimiento acerca del "abecedario digital", conforman la brecha de acceso (de los que no); es decir, de los que han nacido antes de la aparición de las computadoras

- Población Migrante, conformada por personas allegadas que manipulan mediante la tecnología, semejante a la brecha de uso.

- Población Nativa, aquella que la nacido al mismo tiempo del auge virtual y que puede aproximarse a la población que conforma la brecha de calidad de uso.

SEGUNDA.

La Gestión del Cambio hacia la Cultura Digital en el Perú, se realiza por medio de la interrelación Estado – Empresas Internacionales. Sin embargo, para contribuir con la masificación eficaz del uso de las Tics, se hace necesaria la intervención del Derecho Informático, para que recomiende a las instancias y organismos nacionales e internacionales relacionados con la población vulnerable (caso comunidades campesinas y urbano marginales) para que en su ordenamiento jurídico correspondiente, se disponga la Enseñanza y Capacitación Digital Permanente de las Tics.

Por lo que sugerimos (como ejemplo), las inclusiones y modificatorias en el Convenio 169-OIT, Ley de Educación, Mypes y Comunidades Campesinas.

BIBLIOGRAFÍA.

Volkov, N. "La Brecha Digital: u concepto social con cuatro dimensiones" Boletín de Política Informática, México, Nº 6

Maya Álvarez, Pedro, "La Brecha Digital, brecha social. Los recursos humanos en el desarrollo y la capacitación a través del aprendizaje digital" Gaceta de Antropología 45. http://hdl.handle.net/10481/6963

"GOBIERNO ELECTRÓNICO Y DIGITALIZACIÓN DEL ARCHIVO DE TÍTULOS Y PARTIDAS EN EL SISTEMA NACIONAL DE LOS REGISTROS PÚBLICOS DEL PERÚ: DE LA CULTURA PAPEL A LA CULTURA DIGITAL"

Por: ***Pedro Quiroz Allemant (*)***
Perú

DEDICATORIA:

Dedicado a los millones de usuarios de los Registros Públicos, a quienes nos debemos y por quienes seguiremos trabajando, con el objeto de lograr con eficiencia un verdadero servicio público moderno y de vanguardia.

PRESENTACIÓN DEL PROBLEMA:

Desde el año 1888 el Perú cuenta con el archivo de propiedad inmueble, al cual se han ido agregando otros registros; dicho proceso se ha efectuado en forma empírica, para tal efecto se han scaneado tomos y fichas kardex, sin otorgar autenticidad al Implementar el sistema.

Entre los años 1992 y 1994 se escanearon los tomos antiguos y las fichas kardex para pasar a un sistema de Partidas Electrónicas, donde se ingresaron las imágenes existentes y se continuó con los asientos electrónicos; generándose el problema de iniciar el proceso de autenticación electrónica del archivo digital obrante en Registros Públicos, en vista que el proceso de digitalización no se realizó de forma adecuada.

Otro problema, paralelo al mencionado es el que ocurre con la presentación de nuevos Títulos, actividad que se podría realizar en línea, tal como funciona el proyecto piloto de Constitución de empresas en Línea, operación que viene ocurriendo sólo en algunas Notarías Públicas de Lima.

En tal sentido, planteamos las siguientes interrogantes:

1. ¿Cómo lograr el proceso de autenticación electrónica del archivo digital de los Registros Públicos, habiéndose realizado un proceso de digitalización sin los requisitos de Ley?

2. ¿Es posible implementar un sistema en línea para la presentación ante el Registro Público de los nuevos Títulos con la participación de los Fedatarios Informáticos?

   En tal sentido, es importante que algún día se logre que el archivo digital del Sistema Nacional de los Registros Públicos sea certificado por Fedatarios Juramentados con Especialización en Informática (Fedatarios Informáticos), con lo cual se tendría realmente un sistema seguro, inalterable, auténtico, durable, disponible, almacenable, transferible y utilizable como medio de prueba.

OBJETIVOS:

a) Objetivos generales.

- Proponer un marco legal para lograr un adecuado proceso de autenticación electrónica de los Títulos Archivados y las Partidas Registrales del Sistema Nacional de los Registros Públicos al haberse realizado un proceso de digitalización sin los requisitos de Ley.

b) Objetivos específicos.

- Generar un marco legal para facilitar la presentación de nuevos Títulos en línea, para todas las zonas registrales del Sistema Nacional de los Registros Públicos.
- Proponer la implementación de un proceso de digitalización con valor legal para todas las zonas registrales del Sistema Nacional de los Registros Públicos.
- Implementar lineamientos que permitan lograr certeza sobre la autenticidad de los documentos obrantes en el Archivo Registral de la Superintendencia Nacional de los Registros Públicos, los cuales al ser pasados a microformas y ser debidamente fedateados los cuales formarán el Archivo Registral Digitalizado (ARDI), pudiendo en base a ese archivo expedirse la publicidad de los mismos con mayor seguridad y rapidez.
- Establecer los lineamientos a fin de asegurar la fidelidad y autenticidad de los documentos que conforman el Archivo Registral (Tomos, Fichas, Partidas Electrónicas y Títulos Archivados); transfiriendo dicho archivo a formato digital otorgándole a cada documento digitalizado la calidad de original.

HIPÓTESIS:

- El proceso de autenticación electrónica del archivo digital de los Registros Públicos, debe realizarse a partir de un proceso jurídico informático que lleve a la certeza de la operación electrónica para lo cual deberá generarse un marco normativo adecuado y un sistema seguro que incorpore Microformas Digitales, Firmas Digitales entre otros aspectos técnicos.

- Por el grado de avance técnico y jurídico si es posible implementar un sistema en línea para la presentación ante el Registro Público de los nuevos Títulos con la participación de los Fedatarios Informáticos y, por lo tanto, dar inicio a un proceso de autenticidad electrónica del archivo digital existente en los Registros Públicos.

LA ERA DE LA DIGITALIZACIÓN DE LOS TÍTULOS ARCHIVADOS Y PARTIDAS REGISTRALES.

Desde el año 1994, que se dictó la Ley de creación de la Superintendencia Nacional de los Registros Públicos (SUNARP) del Perú, la convierte en la entidad rectora de todas las oficinas de registros públicos del Perú, integrando en sus procesos, el desarrollo de tecnología de la información con la finalidad de cumplir con la visión de la organización. Siendo la función principal de la SUNARP, preservar la seguridad jurídica en sus dos vertientes: la seguridad jurídica estática, es decir proteger al derecho habiente, o la relación que existe entre

un sujeto y una cosa, frente a los ataques de terceros, y la seguridad jurídica dinámica, o de tráfico, procurando brindar protección a los terceros que se ven involucrados en la circulación de los bienes.

El uso de la tecnología en la SUNARP

El de las Tecnologías de la Información están en pleno apogeo. La era informática con el uso de la computadora, agilizando los procesos de captura y expedición de información y la internet; han desarrollado la comunicación a niveles nunca antes esperados y, como consecuencia de ello, el comercio electrónico es, hoy en día, una de las formas más eficientes para realizar transacciones; pues se vale de la existencia de interconexión en tiempo real, información segura y obtenible en forma rápida. No obstante, lo anteriormente indicado, Mario Rosario Guaylupo[1] precisa que *"... la inquietud que surge, es si las Tecnologías de la Información puede ser aplicada en las instituciones públicas, y, más aún si puede ser aplicada en el procedimiento registral..."*.

El valor seguridad jurídica tiene una justificación económica, ya que reduce costos en la transferencia de bienes, es por ello que surgen los Registros Públicos en general. El profesor Alfredo Bullard[2], señala que *"... un sistema de propiedad coherente debe dar al adquirente la certeza de poder excluir a cualquier otro pretendido adquirente, es decir, una posibilidad de exclusión total..."*.

Debemos considerar los mecanismos que pueden utilizarse a los efectos de poder para alcanzar un nivel óptimo de seguridad, siendo por ello imprescindible la implementación y el uso de las nuevas tecnologías.

LA DIGITALIZACIÓN DE LOS SERVICIOS PÚBLICOS DEL ESTADO Y LA PRESENTACIÓN DE TÍTULOS REGISTRALES EN LÍNEA: UNA PROPUESTA DE AVANZADA

En la década de los '90 se implantó un proceso de escaneo de los tomos antiguos y las fichas kardex para pasar a un sistema de Partidas Electrónicas, donde se ingresaron las imágenes existentes y se continuaron con los asientos electrónicos, generándose un problema complejo de iniciar el proceso de autenticación electrónica del archivo digital obrante en todo el Sistema Nacional de los Registros Públicos, en vista que el proceso de digitalización no se realizó en forma adecuada y menos con la intervención de Fedatarios Informáticos Juramentados, toda vez que en aquella época no existían.

Sin embargo, desde que entraron en funciones los Fedatarios Informáticos Juramentados nula ha sido su participación en los Registros Públicos, quizá por temor a dar un paso trascendental

[1] ROSARIO GUAYLUPO, Mario Antonio, Los desafíos de la Sunarp en la era de la tecnología de la información (nuevos productos de la Sunarp). Blog de la Revista Electrónica El Visir. PUCP 13/12/2010.

[2] BULLARD GONZÁLES, Alfredo. Los sistemas de transferencia de Propiedad. Derecho y Economía. El análisis económico de las instituciones legales. Palestra 2003.Página Nº 148 y 149.

en la era de la modernización, a pesar de contar con recursos económicos y financieros suficientes.

Otro problema paralelo al mencionado es el que ocurre con la presentación de nuevos Títulos, actividad que se podría realizar en línea, tal como funciona en el proyecto piloto de Constitución de Empresas en Línea, el cual funciona sólo con algunas Notarías Públicas de Lima.

Con la situación antes descrita el Decreto Supremo Nº 070-2011-PCM modifica el Reglamento de la Ley Nº 27269 – Ley de Firmas y Certificados Digitales, que establece normas aplicables al procedimiento registral en virtud al Decreto Legislativo Nº 681 y sus ampliatorias.

En el artículo 4º del referido Decreto Supremo se establece que en forma progresiva la SUNARP deberá adoptar las acciones que permitan obtener microformas a partir de los asientos de inscripción suscritos con firma electrónica, conforme a lo establecido en al Decreto Legislativo Nº 681, así como las regulaciones específicas que dicte el Ministerio de Justicia y derechos Humanos, de acuerdo a lo previsto en el Decreto Legislativo Nº 827, para lo cual deberá expedirse la Resolución del Titular de la SUNARP en la que se precise la fecha a partir de la cual los asientos de inscripción empezarán a ser micrograbados para su ulterior almacenamiento en microarchivos.

Finalmente, se debe destacar que en el artículo 5º del mismo Decreto Supremo bajo análisis, se establece que los partes notariales firmados digitalmente en el marco de la Infraestructura Oficial de Firma Electrónica (IOFE), constituyen instrumento legal con valor suficiente para que hayan sido expedidos conforme el Decreto Legislativo Nº 1049 – Ley del Notariado y su Reglamento, y sean presentados respetando los lineamientos contenidos en los convenios que suscriban los Colegios de Notarios o la Junta de Decanos de los Colegios de Notarios con la SUNARP.

LA CONSTITUCIÓN DE EMPRESAS "ON LINE"[3]

Sin lugar a dudas en los últimos tiempos la Superintendencia Nacional de los Registros Públicos – SUNARP, ha establecido una singular medida de fomento y apoyo a los Empresarios Peruanos: sean de la Micro, Pequeña, Mediana ó Gran Empresa.

Se trata del servicio de "Constitución de Empresas en Línea", el mismo que se realiza en un plazo no mayor a 72 horas y ha sido concebido como una herramienta donde se resalta la importancia de la formalización, dirigida fundamentalmente a los Empresarios de la Micro y Pequeña Empresa que deseen constituirse como Persona Jurídica.

Definitivamente, la celeridad en los trámites para constituirse como Persona Jurídica permite ser competitivos en un mercado tan deprimido y por otro lado permite también lograr un reconocimiento y por ende prestigio.

[3] Resolución No. 359-2008-SUNARP-SN y RESOLUCIÓN MINISTERIAL Nº 137-2008-PCM

Asimismo, la herramienta antes descrita brinda la posibilidad de acceder al sistema financiero y así ser sujetos de crédito, a los efectos de invertir y hacer que sus negocios crezcan.

De otro lado, así se está permitiendo el libre acceso a nuevos mercados tanto a nivel local como internacional, sobre todo con la singular oportunidad que representa en la actualidad la suscripción de los Tratados de Libre Comercio – TLC de nuestro país –el Perú- con diversos países.

Es importante destacar el esfuerzo conjunto de la Presidencia del Consejo de Ministros – PCM, del Registro Nacional de Identificación y el Estado Civil - RENIEC, de la Superintendencia Nacional de Administración Tributaria – SUNAT, del Colegio de Notarios de Lima y de la misma SUNARP.

Los resultados son notorios, ya que trae un beneficio adicional: la obtención en forma automática del Registro Único del Contribuyente – R.U.C., así como la Clave SOL (Sistema de Operaciones en Línea). Cabe precisar que esos trámites antes tenían una duración promedio de 20 días y hoy se han desechado todas las barreras burocráticas existentes anteriormente.

Anhelamos que ese sistema se consolide día a día y sobretodo que sea extensivo a más Notarias, ya que en forma experimental está operando sólo en algunos despachos notariales.

Finalmente, esa iniciativa le ha valido a la SUNARP, para que la Universidad Peruana de Ciencias Aplicadas – UPC, el Diario "El Comercio", Radio Programas del Perú – RPP y Andina de Televisión – ATV, le otorgaran el "Premio a la Creatividad Empresarial 2008" – Categoría: Informática, en su versión Décimo Tercera.

Procesos Usuario – Notaria

- Usuario inicia el Tramite
- El Notario de fe de la identidad, capacidad, libertad y conocimiento de los otorgantes y valida en línea con RENIEC la identidad.
- El solicitante paga los derechos desde la notaria.
- Notario remite parte electrónico con firma digital a SUNARP y parte físico de respaldo con código de barras.
- Zona Registral recibe el parte electrónico para iniciar el trámite.

Procesos en Registro

- Caja Única (Presentación de Títulos
- Módulo de Verificador (validación Documento Físico – Electrónico)
- Proceso de migración de Datos
- Calificación Registral
- Proyecto de Inscripción
- Generación de Asiento Electrónico / Anotación de Inscripción

- Replicación a la EXTRANET, obtención del RUC y visualización de la Anotación de Inscripción (vía extranet)

Módulo de Caja Única

Modulo que permite realizar la presentación y/o cobro del expediente, teniendo como dato de ingresa el año y Nº de la Hoja de Presentación generado desde la notaria.

Muestra información referida al pago efectuado por la notaria, esta información deberá ser manejada internamente como un depósito (no efectivo); adicionalmente al gravar se dará inicio a la generación del Nº de Titulo.

Módulo Verificador.

La notaria envía parte físico a SUNARP conteniendo un código de barras de seguridad para su validación.

Módulo Verificador.

- Previamente se ejecuta la validación/verificación del código de barras de seguridad contenido en el parte físico contra la información electrónica recepcionada.
- El Sistema como resultado de la validación / verificación emita una esquela que acompaña al título en el proceso de calificación.

Proceso de Migración de Datos.

- Generado el Nro. de Titulo en el SIR, se ejecutan los procedimientos de las tablas temporales al SIR (Actos, Contratantes, Razón Social, Seguimiento de Títulos, Pagos Efectuados, etc.

- Ventajas:

- Reduce el Tiempo de verificación en el área de digitación, ya que la información es derivada de manera automática a la carga laboral del registrador
- La labor del asistente registral y/o registrador es beneficiada con la carga automática de datos, adicionalmente se tiene acceso al documento electrónico (escritura pública) enviado por el notario.

Calificación Registral.

- Pantalla del Registrador, donde se muestra la carga laboral, así como la de calificación donde se muestran los datos migrados.
- Pantalla del Registrador, donde aparecen los datos migrados de la Razón Social, Contratantes, Monto de Capital, etc.
- Pantalla del Registrador, donde se muestra la opción de visualizar el documento (Escritura Pública), así como generar el proyecto de inscripción.
- Documentos: Escritura Pública a ser utilizada durante el proceso de calificación y copia de la anotación generada por el SIR.

Estado de Titulo – Extranet.

- SUNARP, Solicita en línea a SUNAT la generación del RUC-
- SUNAT genera electrónicamente el número de RUC, la cual es remitida a SUNARP.
- SUNARP publica en su portal la constancia de inscripción que contiene el Nº de Partida – Nº. de RUC y lo remite al Notario.
- El solicitante recoge en la notaria el testimonio con constancia de inscripción, RUC y Clave SOL.
- A través de la Extranet se podrá consultar es estado del título y generar la respectiva anotación de inscripción, donde deberá figurar el Nº de la Partida Registral y Nº. RUC para ser entregada al usuario.

SUNARP – PILARES CENTRALES DE LA POLÍTICA DE MODERNIZACIÓN DE LA GESTIÓN PÚBLICA EN LA ZONA REGISTRAL N° IX – SEDE LIMA

GOBIERNO ELECTRÓNICO - GESTIÓN POR PROCESOS – SIMPLIFICACIÓN ADMINISTRATIVA Y ORGANIZACIÓN INSTITUCIONAL

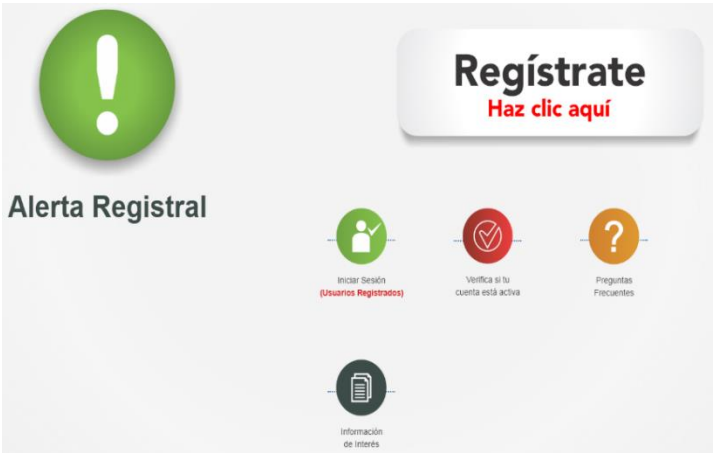
En los últimos años la SUNARP ha venido creando nuevos productos a los cuales el público usuario puede acceder a través de su página web: www.sunarp.gob.pe.

ALERTA REGISTRAL:

Desde el año 2013 ha demostrado ser uno de los servicios de mayor demanda por parte de los ciudadanos. Se accede a través del portal institucional. Es de eficiente utilidad en la lucha contra el fraude inmobiliario, sino también, porque permite mantener informados a los usuarios con interés en determinadas partidas registrales de todos los registros: Propiedad Inmueble, Jurídicas y Naturales y Vehicular, en la medida que comunica por correo electrónico cualquier movimiento que estas pueden sufrir en el ámbito de la presentación de títulos al registro.

Desde este año se ha ampliado a los servicios de publicidad[4].

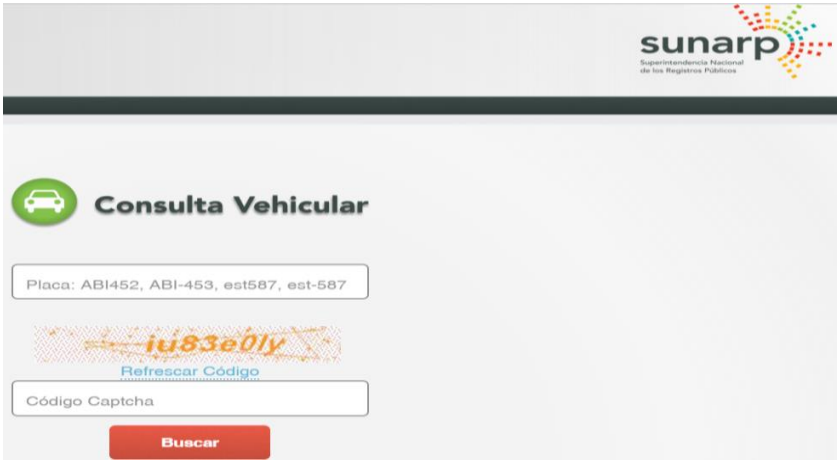
[4] Resolución N° 027-2018-SUNARP/SN.



También es importante destacar que está permitido que el público usuario pueda tomar fotografías de los documentos que obran en los Títulos Archivados de los diferentes Registros.

CONSULTA VEHICULAR

Otro servicio gratuito a disposición del publico usuario en la Consulta Vehicular, a la cual se puede acceder igualmente desde el portal institucional y de forma gratuita.



INSCRIPCIÓN EN EL REGISTRO DE MANDATOS Y PODERES

Uno de los últimos servicios innovadores es la incorporación de todos los actos inscribibles del Registro de Mandatos y Poderes a través de la presentación electrónica de títulos con firma digital mediante el Sistema de Intermediación Digital – SID - SUNARP[5]

CONCLUSIONES

1 Las ventajas de la digitalización de las partidas registrales y títulos archivados, tendrán un impacto favorable en los ciudadanos que acceden los Registros Públicos: podrán solicitar todas las reproducciones que requiera, vía impresión simple o impresión literal, sin que el documento original (físico en su caso), se altere o deteriore. Además, de la celeridad en la atención.

[5] Resolución N° 167-2018-SUNARP/SN .

2 La implementación de dichos proyectos en forma sistemática, servirán para otorgar mayor seguridad jurídica a la ciudadanía en general, logrando que la SUNARP facilite las transacciones a un menor costo.

3 La implementación de nuevos proyectos, trae como consecuencia la reducción de los costos de transacción de los operadores registrales; debiendo puntualizar también que en este caso, esta modernización no sólo busca mejorar el servicio a la ciudadanía en general, sino también otorgar al usuario interno, Registradores, mayor confianza que realizan sus labores con mayor seguridad

4 Con este servicio se permitirá que los usuarios puedan presentar sus títulos sin necesidad de suscribir en forma manual los formularios de solicitudes de inscripción y publicidad. Los usuarios podrán acceder a dichos formularios e ingresar la información a través de medios mecanizados, para luego imprimirlos.

5 Se evitará que los usuarios que presentan en forma masiva títulos, como es el caso de los Notarios, tengan que ingresar manualmente los datos en dichos documentos, reduciendo las horas hombre en dicho trabajo, y coadyuvando así también en la reducción de gastos administrativos en papel de la SUNARP

6 Se evitará el proceso interno de digitación donde se bloquean las partidas y se consignan datos del título antes de ser derivados los títulos al Registrador, ya que se aprovecha la información estructurada que ingresará el usuario en dichos formularios

7 Es un documento digital, que se encuentra grabado en un medio físico ***técnicamente idóneo*** y puede ser reproducido en copias impresas, en esencia iguales al documento original.

8 Las imágenes obtenidas mediante este sistema tienen ***valor probatorio legal***; reemplazan al documento en papel, permiten su destrucción y pueden ser distribuidas.

9 Inversión altamente rentable.

10 Reducción de costos operativos.

11 Liberación de recursos involucrados en el tratamiento documental.

12 Automatización de los procesos involucrados.

13 Validez legal de la documentación (fedatarios en todos los procesos de conversión).

14 Distribución de la información a cualquier lugar y en tiempo real (Información en línea).

15 Garantía total de seguridad e integridad de su información.

Nuevas Tecnologías de Información, Comunicación e Interacción, y nuevos Derechos Fundamentales

Por: ***Catarina Sarmento e Castro***
Portugal

Introducción

Lo presente texto tiene por objetivo, de un lado, chamar la atención para nuevos derechos de los ciudadanos, que deben fortalecer su defesa en resultado de los peligros provocados por la utilización, por si, o por otros, de siempre renovadas tecnologías de información, de comunicación e interacción, que todos los días acercan su vida. Estas, frecuentemente de innegable utilidad para su cuotidiano, unas veces, aumentan la vigilancia en relación a su vida personal, otras, enflaquecen lo dominio del ciudadano con relación à su información personal, o reducen su controlo con conexión a decisiones que le respectan.

Nos vamos, a este propósito, a destacar lo derecho à la desconexión de lo trabajador que, resultado de la omnipresencia de la tecnología, está constantemente solicitado à trabajar, con prejuicio de importantes derechos fundamentales como el derecho al ocio, al descanso, al relacionamiento con su familia, o está siendo vigiado en su labor. Haremos también referencia al derecho a conocer el algoritmo, de importancia creciente en razón del incremento de su utilización como mecanismo promotor de decisiones automatizadas con reflejo en la vida de los ciudadanos.

De otro lado, se pretende, también, destacar nuevos derechos que obligan los Estados a prestar nuevas utilidades a los ciudadanos en su relación con las nuevas tecnologías, indispensables, entre otros, al desarrollo de sus derechos de personalidad y ciudadanía. Aquí defenderemos la existencia de un Derecho al *Internet*, y de un Derecho al relacionamiento electrónico de lo ciudadano con la Administración Pública.

I. Las tecnologías de información, comunicación e interacción, sus riesgos, y los nuevos derechos de protección

1. Derecho a la desconexión del trabajador

La omnipresencia de los medios de comunicación en la relación laboral faculta al empleador un contacto permanente con su trabajador: por email, por teléfono, por SMS, por WhatsApp, por controlo GPS de su vehículo... Esa nueva realidad está dificultando la distinción entre periodos de ocio o de descanso y de trabajo, y está haciendo peligrar la conciliación de la vida de trabajo con la vida personal e familiar.[1] La solución para rechazar estas violaciones

[1] En Brasil, eso ha sido reconocido: Acórdão do Tribunal Superior do Trabalho, publicado a 27 de outubro de 2017, processo AIRR - 2058-43.2012.5.02.0464, en http://aplicacao4.tst.jus.br/consultaProcessual/consultaTstNumUnica.do?consulta=Consultar&conscsjt=&numeroTst=2058&digitoTst=43&anoTst=2012&orgaoTst=5&tribunalTst=02&varaTst=0464&submit=Consultar. En Brasil: RESEDÁ, Salomão, «O direito à desconexão: uma realidade no teletrabalho», *Revista de Direito do Trabalho*, São Paulo, Brasil, n.º 126, 2007, p. 157 e ss., disponible en http://www.egov.ufsc.br/portal/sites/default/files/anexos/23040-23042-1-PB.pdf;

de derechos fundamentales de ciudadano como persona y, en especial, como trabajador[2], es la consagración de un derecho à la desconexión. Eso es un derecho à la desconexión en los momentos privados, fuera de la jornada de trabajo.
La desconexión es garantía de un descanso efectivo, físico y psicológico, que debe asegurar un tiempo libre real, importante para la salud, desarrollo personal, familiar e social, asociado à la limitación de la jornada de trabajo[3].

2. Derecho a conocer el algoritmo

Otro derecho que se impone reconocer, para garantía del ciudadano, en virtud de las posibles consecuencias de las nuevas tecnologías es el derecho a conocer el algoritmo. El algoritmo es un conjunto de instrucciones, codificadas por un programador para que lo computador lo pueda alcanzar, que indican, con grande precisión, al computador lo que debe hacer. La información es introducida en el computador y ese presenta la solución dictada por lo algoritmo. La respuesta del computador auxilia tareas mui variadas, como las de gestión interna, automatizada, de importantes funciones – privadas, en la industria, financieras, o comercio, y públicas, en la Administración o judiciales, -, mas también comanda decisiones que pueden cambiar, directamente, nuestras vidas, produciendo efectos inmediatos en la esfera jurídica de los ciudadanos. Como para concedernos un permiso para ejercicio de una actividad, o para negarnos un crédito bancario.

La importancia de las decisiones automatizadas, basadas en perfil personal construido por computador[4], hay sido destacada en 1988, pela *Commission National de l'Informatique et des Libertés (CNIL)* francesa, que hay decidido que los derechos de los ciudadanos habían sido perjudicados con la utilización de metodología de *credit scoring*, que fijaba puntos, de modo automático, atendiendo a ciertas circunstancias personales de lo candidato al crédito. De eses puntos resultaba, o no, la concesión de crédito.[5] El Reglamento (europeo) general de protección de datos (2016/679) se ocupó de crear reglas relativas a algoritmos de construcción de perfiles utilizados para tomar decisiones (artículo 22.º).

MAIOR, Jorge Luiz Souto, «Do direito à desconexão no trabalho», *Revista do Tribunal Regional do Trabalho da 15.ª Região*, en http://www.egov.ufsc.br/portal/sites/default/files/do_direito_a_desconexao_do_trabalho.pdf.

[1] Lo derecho a desconectarse en Francia: http://travail-emploi.gouv.fr/grands-dossiers/LoiTravail/quelles-sont-les-principales-mesures-de-la-loi-travail/article/droit-a-la-deconnexion, así como METTLING, Bruno, «Transformation numérique et vie au travail (Rapport)», *La Documentation Française*, Paris, Francia, 2015, en http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000646.pdf. Loi 2016-1088, de 8 de agosto, en http://travail-emploi.gouv.fr/IMG/pdf/loi_no2016-1088_du_8_aout_2016_version_initiale.pdf.

[2] Protegidos, por ejemplo, por artículo 59.º, n.º 1, alinea b), da constitución portuguesa, que concilia empleo con la vida familiar e una organización do trabajo en condiciones socialmente dignificantes; o la alinea c), que establece que lo trabajo debe ser prestado en condiciones de higiene, seguridad e salud; o alinea d), consagrando un derecho al reposo e al ocio.

[3] SARMENTO e CASTRO, Catarina, «As novas tecnologias e a relação laboral», Revista do Centro de Estudos Judiciários, Lisboa, Portugal, 2018 (en publicación).

[4] Sobre perfis: SARMENTO E CASTRO, Catarina, «A Jurisprudência do Tribunal de Justiça da União Europeia, o Regulamento Geral sobre a Proteção de Dados Pessoais e as Novas Perspetivas para o Direito ao Esquecimento na Europa», *Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos*, Volumen I, Almedina, Coimbra, Portugal, 2016, pp. 1047 e ss.; CÓRDOBA CASTROVERDE, Diego/DÍEZ-PICAZO GIMÉNEZ, Ignácio, «Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico», El Derecho a la Privacidad en un Nuevo Entorno Tecnológico, Centro de Estudios Políticos y Constitucionales (Tribunal Constitucional), Madrid, España, 2016, p 99 e ss.

[5] GENTOT, Michel, «La Protection des Données personnelles à la croisée des chemins», *Société d'Information et Vie Privée*, Tomo 3, Cahiers des Sciences Morales et Politiques, PUF, Paris, Francia, p. 24 e ss., disponible en: https://www.asmp.fr/travaux/gpw/internetvieprivee/rapport3/chapitr1.pdf, consultado

Para poder contestarse decisiones basadas en algoritmos, conocer la lógica de su construcción es mui importante. La defesa de lo ciudadano depende de esto. La transparencia de lo algoritmo – así, en especial, cuando define un perfil de una persona y fundamenta decisiones impactantes, por ejemplo – es fundamental. Lo derecho à la información sobre tratamiento de datos personales también debe incluir esos esclarecimientos[6].

Además, la complexidad de los algoritmos utilizados no para de crecer, ampliando la dificultad de lo ciudadano para comprender su lógica, mismo cuando capacitado para utilizar las tecnologías[7]. De algoritmos que comandan computadores diciéndoles lo que hacer, de forma pormenorizada, – como pilotar aviones, fornecer dinero en cajero automático, organizar un sistema de atendimiento al público, regar una propiedad agrícola, alertar para un evento – los algoritmos se transformaran en algoritmos evolutivos, de aprendizaje automática, que estudian nuestros gustos, comportamientos y una multiplicidad de datos, que alimentan su aprendizaje e conforman los resultados. La programación, como la conocíamos, que, por ejemplo, dictaba decisiones automáticas, exigía una descripción pormenorizada de todas las condiciones que pudieran ocurrir. Los algoritmos de aprendizaje se adaptan a sí mismos, se modifican, para hacer sugerencias de hoteles y vuelos, libros y música, o conducir un automóvil.

Así, como hay sustentado MARC ROTENBERG, presidente del *Electronic Privacy Information Center* (EPIC), lo conocimiento de esas fórmulas matemáticas utilizadas por los computadores (como la información destinada a decidir sobre nosotros) es un derecho fundamental.
En virtud de la dificultad de comprehender el algoritmo, una autoridad independiente debe crearse para intermediar la información al ciudadano, de manera a tornarla inteligible.

En conclusión, esos nuevos derechos – de desconexión, a conocer el algoritmo - tienen por objetivo garantizar la protección de aspectos de la personalidad de lo ciudadano amenazadas.

II. Nuevas tecnologías y definición de nuevos derechos de contenido asociado à la evolución tecnológica y sus potencialidades

En el último apartado (I) se hay hecho referencia a los nuevos derechos que deben proteger lo ciudadano con relación à las agresiones conducidas por las nuevas tecnologías, algunos de esos mereciendo dignidad constitucional. Todavía, la utilización de las nuevas tecnologías de información, de comunicación e de interacción también favorece los derechos.

Eso ocurre, por ejemplo, cuando las nuevas tecnologías incrementan lo desarrollo de derechos previamente existentes, como lo derecho a la información administrativa (facilitando el acceso, ahora *online*), el derecho à participación política y administrativa (con la presentación de peticiones en línea, la votación a través de *Internet*, o la respuesta *online* à demandas que auxilian la decisión de las autoridades administrativas), los derechos de lo

[6] También lo escribió ALVES LEAL, Ana, «Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação», FinTech – Desafios da tecnologia financeira, Almedina, Coimbra, Portugal, 2017, p. 128.
[7] Como expone DOMINGOS, Pedro, A revolução do algoritmo mestre, Manuscrito, Lisboa, Portugal, 2017.

consumidor (mejorando la difusión de información, propiciando la institución de libros de reclamación en línea, o a través de lo ejercicio del derecho a la portabilidad de los datos personales para cambiar operadora de música en *streaming*), entre tantos otros ejemplos. En virtud de potenciaren nuevas formas de su realización, las nuevas tecnologías facilitan la concretización de derechos preexistentes.

Todavía, las tecnologías propician, también, lo impulso de nuevos derechos, de contenido moldado por sus circunstancias, como lo derecho à *Internet* o el Derecho al acceso electrónico a la Administración Pública. Esos son derechos a nuevas funcionalidades e nuevos bienes, indispensables al desarrollo del ciudadano, de su personalidad, de su actividad ciudadana e al incremento de otros derechos. A ellos dedicaremos las próximas líneas.

La referencia al poder transformador de las tecnologías de información, de comunicación y de interacción con relación a la esfera jurídica del ciudadano no estaría completa si no se prestaba atención à que las nuevas tecnologías también facilitan lo cumplimento de deberes jurídicos, algunos con tradición constitucional, como el deber fundamental de pagar impuestos, que hoy puede ser concretizado en línea y, en algunos casos, sin mismo necesitarse de realizar la entrega de un formulario declarativo, todo se haciendo, de forma automática, junto de la Administración fiscal, con un *click*.

1. Derecho fundamental à *Internet*

Lo derecho à *Internet* es un derecho dotado de jusfundamentalidad[8].
Este es un derecho amplificador de otros derechos. Esa es su característica más ampliamente reconocida. La utilización de *Internet* incrementa la concretización de derechos, algunos de los cuales reconocidos como derechos fundamentales. Se pensamos à lo derecho de colocar contenidos en línea, dirigidos à múltiplos destinatarios, y presentados por una multiplicidad de atores, comprehendemos que la *Internet* posibilita la expansión de la libertad de expresión. Al mismo tiempo, las prohibiciones impuestas por algunos estados à divulgación de contenidos en línea pueden traducir imposiciones de censura, violadores de esos derechos e libertades de, por ejemplo, manifestar su opinión, o de exhibir una cualquier creación.

También el bloqueo de acceso al contenido puede, en ciertas circunstancias, considerar-se atentatorio de lo derecho à información. Este ocurre porque la *Internet* también debe servir à difundir e recibir información, incluso, información administrativa. Lo acceso a esta información propicia la transparencia de la actividad administrativa asociada, por ejemplo, à información estadística[9], ambiental, del consumidor. Eso es decir que el derecho à Internet es un derecho à los contenidos de la Internet.

[8] En favor de un derecho fundamental à Internet: SARMENTO E CASTRO, Catarina, «O Direito à Internet», Cyberlaw by CIJIC, Lisboa, Portugal, n.º 2, junio 2016, disponible en http://www.cijic.org/wp-content/uploads/2016/06/DIREITO----INTERNET_Catarina-Sarmento-e-Castro.pdf.; SARMENTO e CASTRO, Catarina, «40 anos de "Utilização da Informática" - o artigo 35.º da Constituição da República Portuguesa», Epública – Revista Electrónica de Direito Público, Volumen 4, n.º 1, Lisboa, Portugal, 2017, disponible en http://e-publica.pt/anteriores.html.

[9] SARMENTO e CASTRO, Catarina, «A Limitação do Segredo Estatístico: Segredo Estatístico *Versus* Publicidade», Indicadores Locais de Desenvolvimento Sustentável. O Caso de Estarreja (Coord. Sara Moreno Pires, Alexandra Aragão, Teresa Fidélis, Irineu Mendes), Instituto Jurídico da Faculdade de Direito, 2016, en https://www.researchgate.net/publication/313360327_A_limitacao_do_segredo_estatistico_segredo_estatistico_versus_publicidade_The_limitation_of_statistical_confidentiality_statistical_confidentiality_versus_publicity

Cuando se utiliza la *Internet*, se puede acceder, entre otros, a servicios de cultura (para comprar un ingreso, para solicitar un apoyo), de educación (utilizando o e-*learning*; presentando solicitudes o inscripciones en cursos), de salud (a través de la institución de registros personales de salud, aceptando inscripciones en consultas médicas, creando recetas médicas en línea), siendo potenciados derechos fundamentales.

Todavía, siendo un derecho ampliador de otros derechos, este derecho es, también, un derecho dotado de contenido propio, que se debe valorar como derecho fundamental. En un cierto sentido, este es un derecho de acceso à la rede de las redes, un derecho de acceder à los medios tecnológicos, à la infra-estructura que permite la conectividad permanente de todos con la información, y de todos con todos.

Mas es, también, un derecho de relacionar-se digitalmente, de participar en las redes sociales, de participar en la estructura social que opera a través de la infra-estructura técnica. Eso es, hoy, para grande parte de los ciudadanos, indispensable al desarrollo de su personalidad y, así mismo, a su felicidad, de que hace parte su relacionamiento social en línea. Como nosotros, alguna doctrina lo ven considerando un derecho fundamental. Veja-se, por ejemplo, la doctrina española, italiana, francesa e brasileira[10].
Por su parte, algunas ordines jurídicas, como la portuguesa, consagran un derecho fundamental à la Internet en lo texto de la Constitución. En artículo 35.º, n.º 6, la norma fundamental establece a todos se garantiza lo acceso à las redes informáticas[11].
Mas este debe ser, también, un derecho fundamental a valorar por la jurisprudencia. Algunos tribunales han empezado a reconocerlo, por ejemplo, en Costa Rica: en 2010, la Corte Suprema aceptó un derecho fundamental a *Internet*.

2. Derecho fundamental al acceso electrónico a la Administración Pública.

La caracterización de lo derecho à *Internet* como derecho amplificador de derechos, incluso de los derechos de lo ciudadano en cuanto administrado, permite comprehender que lo derecho de acceso electrónico à la Administración es, hoy, una necesidad fundamental para

[10] DÍAZ PINTOS, G, «En favor de un Derecho Fundamental de Acceso à la Red», Persona y Derecho, Vol. 45, 2001, p. 323 e ss. (337), en http://dadun.unav.edu/handle/10171/14366 (2 de janeiro de 2016); FROSINI, Vittorio, «L'Orizzonte Giuridico dell'Internet», Diritto dell'Informazione e dell'Informática, n.º 271, 2002, p.275; FROSINI, Tommaso Edoardo, «Il Diritto Costituzionale di Accesso a Internet", Rivista Telemática Giuridica dell'Associazione Italiana dei Costituzionalisti, n.º1, 2011, p. 1 e ss.; Idem, «Nuevas Tecnologías y Constitucionalismo», Revista Derecho del Estado, n.º 15, dezembro 2003, p. 29 e ss.; MARINO, Laure, «Le Droit d'Accès à l'Internet, Nouveau Droit Fondamental», *Rec. Dalloz*, 2009, p. 2045; ROQUES-BONNET, Marie-Charlotte, Le Droit Peut-il Ignorer la Révolution Numérique?, Éditions Michalon, Paris, Francia, 2010; GOULART, Guilherme Damasio, «O Impacto das Novas Tecnologias nos Direitos Humanos e Fundamentais: o acesso à Internet e a Liberdade de Expressão», *Revista Direitos Emergentes na Sociedade Global*, Vol. I, n.º 1, Janeiro-Junho 2012, p. 145 e ss. (p. 153), en http://ssrn.com/abstract=2156402.

[11] Varios autores se refieren al artículo 35.º, incluso a su evolución, mas su análisis aún no contempla esta visión de lo derecho fundamental a Internet: GOMES CANOTILHO, José Joaquim / MOREIRA, Vital, Constituição da República Portuguesa Anotada, Volumen I, 4.º Edición, Coimbra Editora, Coimbra, 2007, pp. 547 e ss.; RIBEIRO DE FARIA, Paula, «Anotação ao Artigo 35.º da Constituição», en MIRANDA, Jorge/MEDEIROS, Rui, Constituição Portuguesa Anotada, Tomo I, 2.ª Edición, Coimbra Editora, Coimbra, Portugal, 2010, pp. 779 e ss. (pp. 802 e ss.); MAGALHÃES, José, Dicionário da Revisão Constitucional, Publicações Europa-América, Lisboa, Portugal, 1989, pp. 374-375; SOUSA PINHEIRO, Alexandre, Privacy e Protecção de Dados Pessoais: a Construção Dogmática do Direito à Identidade Informacional, Associação Académica da Faculdade de Direito de Lisboa, Lisboa, 2015, pp. 665 e ss.

los ciudadanos, tanto para cumplir sus obligaciones, como para utilizar los bienes e los servicios atribuidos pela Administración.
La utilización de mecanismos de información y de comunicación faculta à la Administración una actuación más célere, más transparente, más económica, más sencilla y más eficiente. Eso es posible ja que la tecnología facilita, por ejemplo, la troca de información automatizada entre servicios administrativos, y entre estos y lo ciudadano, lo trabajo administrativo en rede, la resolución multicanal de solicitudes, la reorganización de las estructuras administrativas de front-office y de back office, la simplificación de los procedimientos administrativos, las decisiones administrativas automatizadas, la reducción de tiempos de decisión administrativa y la reducción de la distancia geográfica.

Una grande importancia tiene, en esto contexto, la posibilidad de comunicación facilitada entre los ciudadanos y la Administración para presentación de solicitudes, de informaciones o de documentos, o para recibir, de forma célere y sencilla, respuesta de la Administración, por ejemplo, en forma de información o de decisión[12]. De lo acceso electrónico de lo ciudadano à la organización administrativa depende, por ejemplo, la concretización de importantes derechos fundamentales, como lo acceso à información administrativa, o lo mejor acceso à la salud o à prestaciones de asistencia social.

Conclusión

Lo camino recorrido nos hay podido demonstrar la relación de proximidad entre la marcha tecnológica y la necesaria evolución de los derechos que la acompaña. A estos derechos à la desconexión, al conocimiento del algoritmo, à Internet, al acceso/relacionamiento electrónico à/con la Administración Pública, sería posible juntar otros, como, por ejemplo, el derecho à la autodeterminación informativa y el derecho al olvido.

La tecnología crea riesgos, que la orden jurídica debe ayudar a rechazar o a minorar, mas, también, propicia lo desarrollo de derechos preexistentes, auxilia el cumplimiento de deberes y potencia lo reconocimiento de derechos con contenidos innovadores conexos con los nuevos mecanismos de información, comunicación y interacción.

Bibliografía

ALVES LEAL, Ana, «Aspetos jurídicos da análise de dados na Internet (*big data analytics*) nos setores bancário e financeiro: proteção de dados pessoais e deveres de informação», FinTech – Desafios da tecnologia financeira, Almedina, Coimbra, Portugal, 2017
CÓRDOBA CASTROVERDE, Diego/DÍEZ-PICAZO GIMÉNEZ, Ignácio, «Reflexiones sobre los retos de la protección de la privacidad en un entorno tecnológico», *El Derecho a la Privacidad en un Nuevo Entorno Tecnológico*, Centro de Estudios Políticos y Constitucionales (Tribunal Constitucional), Madrid, España, 2016, p 99 e ss.

[12] Sobre el tema: VALERO TORRIJOS, Julián, *El régimen jurídico de la e-Administración*, Editorial Comares, 2.ª Edição, Granada, 2007.

DÍAZ PINTOS, G, «En favor de un Derecho Fundamental de Acceso à la Red», Persona y Derecho, Vol. 45, 2001, p. 323 e ss. (337), en http://dadun.unav.edu/handle/10171/14366 (2 de janeiro de 2016);
DOMINGOS, Pedro, A revolução do algoritmo mestre, Manuscrito, Lisboa, Portugal, 2017.
FROSINI, Vittorio, «L'Orizzonte Giuridico dell'Internet», Diritto dell'Informazione e dell'Informática, n.º 271, 2002, p.275;
FROSINI, Tommaso Edoardo, «Il Diritto Costituzionale di Accesso a Internet", Rivista Telemática Giuridica dell'Associazione Italiana dei Costituzionalisti, n.º1, 2011, p. 1 e ss.;
FROSINI, Tommaso Edoardo, «Nuevas Tecnologías y Constitucionalismo», Revista Derecho del Estado, n.º 15, dezembro 2003, p. 29 e ss.;
GOERLICH PESET, José María, «Protección de la Privacidad de los Trabajadores en el Nuevo Entorno Tecnológico: Inquietudes y Paradojas», El Derecho a la Privacidad en un Nuevo Entorno Tecnológico, Centro de Estudios Políticos y Constitucionales (Tribunal Constitucional), Madrid, España, 2016, p. 123 e ss..
GOMES CANOTILHO, José Joaquim / MOREIRA, Vital, *Constituição da República Portuguesa Anotada*, Volumen I, 4.º Edición, Coimbra Editora, Coimbra, 2007, pp. 547 e ss.
GOULART, Guilherme Damasio, «O Impacto das Novas Tecnologias nos Direitos Humanos e Fundamentais: o acesso à Internet e a Liberdade de Expressão», *Revista Direitos Emergentes na Sociedade Global*, Vol. I, n.º 1, Janeiro-Junho 2012, p. 145 e ss. (p. 153), en http://ssrn.com/abstract=2156402.
MAGALHÃES, José, *Dicionário da Revisão Constitucional*, Publicações Europa-América, Lisboa, Portugal, 1989, pp. 374-375.
MAIOR, Jorge Luiz Souto, «Do direito à desconexão no trabalho», *Revista do Tribunal Regional do Trabalho da 15.º Região*, en http://www.egov.ufsc.br/portal/sites/default/files/do_direito_a_desconexao_do_trabalho.pdf
.
http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/154000646.pdf.
MARINO, Laure, «Le Droit d'Accès à l'Internet, Nouveau Droit Fondamental», *Rec. Dalloz*, 2009, p. 2045;
METTLING, Bruno, «Transformation numérique et vie au travail (Rapport)», *La Documentation Française*, Paris, Francia, 2015, en
MOREIRA, Teresa Coelho, A Privacidade dos Trabalhadores e as Novas Tecnologias de Informação e Comunicação: Contributo para os Limites do Poder de Controlo Electrónico do Trabalhador, Almedina, Coimbra, Portugal, 2010;
MOREIRA, Teresa Coelho, «As Novas Tecnologias de Informação e Comunicação: um Admirável Mundo Novo do Trabalho?», Estudos de Homenagem ao Prof. Doutor Jorge Miranda, Volume VI, Coimbra Editora, Coimbra, Portugal, 2012, pp. 953 e ss.;
MOREIRA, Teresa Coelho, «A Privacidade dos Trabalhadores e a Utilização de Tecnologias de Identificação por Radiofrequência», Estudos em Homenagem ao Professor Doutor Heinrich Hörster, Almedina, Coimbra, Portugal, 2012, p. 145 e ss.;

RESEDÁ, Salomão, «O direito à desconexão: uma realidade no teletrabalho», *Revista de Direito do Trabalho*, São Paulo, Brasil, n.º 126, 2007, p. 157 e ss., disponible en http://www.egov.ufsc.br/portal/sites/default/files/anexos/23040-23042-1-PB.pdf;

RIBEIRO DE FARIA, Paula, «Anotação ao Artigo 35.º da Constituição», en MIRANDA, Jorge/MEDEIROS, Rui, *Constituição Portuguesa Anotada*, Tomo I, 2.ª Edición, Coimbra Editora, Coimbra, Portugal, 2010, pp. 779 e ss. (pp. 802 e ss.).
ROQUES-BONNET, Marie-Charlotte, Le Droit Peut-il Ignorer la Révolution Numérique?, Éditions Michalon, Paris, Francia, 2010;
SARMENTO E CASTRO, Catarina, «O Direito à Internet», *Cyberlaw by CIJIC*, n.º 2, junio 2016, disponible en http://www.cijic.org/wp-content/uploads/2016/06/DIREITO----INTERNET_Catarina-Sarmento-e-Castro.pdf.
SARMENTO E CASTRO, Catarina, «A Jurisprudência do Tribunal de Justiça da União Europeia, o Regulamento Geral sobre a Proteção de Dados Pessoais e as Novas Perspetivas para o Direito ao Esquecimento na Europa», *Estudos em Homenagem ao Conselheiro Presidente Rui Moura Ramos*, Volumen I, Almedina, Coimbra, Portugal, 2016, pp. 1047 e ss..
SARMENTO e CASTRO, Catarina, «As novas tecnologias e a relação laboral», Revista do Centro de Estudos Judiciários, Lisboa, Portugal, 2018 (en publicación).
SARMENTO e CASTRO, Catarina, «40 anos de "Utilização da Informática" - o artigo 35.º da Constituição da República Portuguesa», Epública – Revista Eletrónica de Direito Público, Volumen 4, n.º 1, Lisboa, Portugal, 2017, disponible en http://e-publica.pt/anteriores.html.
SARMENTO e CASTRO, Catarina, «A Limitação do Segredo Estatístico: Segredo Estatístico Versus Publicidade», Indicadores Locais de Desenvolvimento Sustentável. O Caso de Estarreja (Coord. Sara Moreno Pires, Alexandra Aragão, Teresa Fidélis, Irineu Mendes), Instituto Jurídico da Faculdade de Direito, 2016, en https://www.researchgate.net/publication/313360327_A_limitacao_do_segredo_estatistico_segredo_estatistico_versus_publicidade_The_limitation_of_statistical_confidentiality_statistical_confidentiality_versus_publicity.
SARMENTO e CASTRO, Catarina, «A Protecção dos Dados Pessoais dos Trabalhadores», Questões Laborais, Portugal, Ano IX, 2002, n.º 19, pp. 27 e ss., y n.º 20, pp. 139 e ss.;
SARMENTO e CASTRO, Catarina, «Surveillance and Monitoring - Portugal», en Employment Privacy Law in the European Union: Surveillance and Monitoring, Intersentia, Antuérpia, Bélgica, 2002*;*
SARMENTO e CASTRO, Catarina, «Human Ressources and Sensitive Data - Portugal», en Employment Privacy Law in the European Union: Human Ressources and Sensitive Data, Intersentia, Antuérpia, Bélgica, 2003, p. 235 e ss.;
SILVEIRA, Alessandra/CANOTILHO, Mariana, *Carta dos Direitos Fundamentais da União Europeia Comentada*, Almedina, Coimbra, Portugal, 2013, em especial, os comentários de Sophie Perez Fernandes (artigo 7.º) e Catarina Sarmento e Castro (artigo 8.º).
SOUSA PINHEIRO, Alexandre, *Privacy e Protecção de Dados Pessoais: a Construção Dogmática do Direito à Identidade Informacional*, Associação Académica da Faculdade de Direito de Lisboa, Lisboa, 2015, pp. 665 e ss.
VALERO TORRIJOS, Julián, *El régimen jurídico de la e-Administración*, Editorial Comares, 2.ª Edição, Granada, 2007.

IMPACTO DE LAS FOTOGRAFIAS PUBLICADAS SIN AUTORIZACIÓN EN LAS REDES SOCIALES CONFORME LA LEGISLACION PERUANA

Por: ***Edda Karen Céspedes Babilón***
Lima, Perú

I. INTRODUCCIÓN

En el apoteósico y actual crecimiento de las tecnologías, el uso masivo de las comunicaciones a través de las Redes Sociales, han invadido la vida de todos los individuos a nivel mundial, creando lazos y vínculos con informaciones y publicaciones que logran llegar a todos los ámbitos sociales, cumpliendo el objetivo de comunicación virtual, a corta y larga distancia.

El Perú no es ajeno a ello y se une a esta vorágine virtual donde las Redes Sociales cubren diferentes ámbitos de los ciudadanos, inundando sus diferentes entornos, ya sea en lo familiar, profesional, laboral, empresarial y social, convirtiéndose las Redes Sociales en un instrumento principal de comunicación, donde las personas además de intercambian información.

Sin embargo, esta vorágine tecnológica cuya utilización debe ser totalmente beneficiosa para el crecimiento y desarrollo del país, viene convirtiéndose, por su mal uso, en una herramienta de vulneración de los Derechos Humanos.

En este sentido, vamos a desarrollar en este artículo una de las afectaciones a los Derechos Fundamentales de la Persona, por la publicación inadecuada y no permitida de la fotografía de una persona, y asimismo dilucidar su protección, en la legislación peruana partiendo del Derecho Constitucional, Civil y la Ley 29733, Ley de Protección de Datos; al considerar la fotografía un "dato" calificado como "data sensible" por lo que la priorización de su tratamiento se debe dar en los diferentes ámbitos, sea social, jurídico o político en el afán de contribuir a la cautela del Derecho a la Intimidad y el respeto a la Privacidad, cuya violación debe determinar un estricto resarcimiento por el daño causado en contra de los derechos inherentes a la Persona. Quede claro que la problemática, parte del mal uso de las Tecnologías de la Información y Comunicaciones en los entornos digitales, donde las personas afectadas no han manifestado libremente su voluntad para permitir la publicación de su fotografía en las Redes Sociales.

Asimismo, es conveniente aplicar una visión amplia para establecer mayores alcances jurídicos en la Protección de la publicación de fotografías e imagen en la Redes Sociales y asimismo establecer claras Políticas Publicas de Prevención y Concientización Digital.

Cabe resaltar que el presente artículo forma parte de mi Tesis e investigación que vengo desarrollando en la Escuela de Post Grado, y que continuaré perfeccionando, para la obtención de mi Grado.

II. CONSIDERACIONES PREVIAS: FOTOGRAFIA E IMAGEN

La palabra fotografía proviene etimológicamente del griego: *foto* y *grafía* que significa "grabar con la luz", que viene a ser la técnica de obtener imágenes debido a la acción de la luz. Es decir, al referirse a la fotografía de una persona también podemos referirnos a la "imagen de una persona que refleja el rostro de la misma", sin extender la connotación a la imagen de una persona que se refleja en su hablar, vestir o comportamiento, que caracteriza e identifica a sendas personas. Recalco que, al referirnos a la imagen en este artículo, nos estamos refiriendo a la foto de una persona. En este caso, el artículo trata de la fotografía o imagen de una persona publicada indebidamente o sin autorización en las Redes Sociales.

Es menester destacar que las fotos de una persona pueden incluir situaciones privadas o reflejar espacios de la vida íntima, que incluyen desde su manera de vestir, lugar donde se encuentran, personas a su alrededor, horarios, acciones personales, etc. que pueden mellar la reputación (imagen) y el buen nombre de una persona, siendo esta acepción mucho más amplia y que puede coincidir como consecuencia de una fotografía publicada indebida o maliciosamente.

Estas y otras consideraciones serán analizadas para el desarrollo de este artículo que puede conllevar a una investigación más amplia, y que propondremos igualmente en otra oportunidad, para sus consideraciones o mejoras pertinentes.

Lo importante y como hemos visto en el párrafo anterior, es conocer el impacto y las consecuencias que puede ocasionar la publicación de una fotografía en las Redes Sociales sin su autorización del propietario de la fotografía, la cual mella indefectiblemente Derechos Humanos y específicamente Derechos personalísimos.

III. INFRACCIÓN A LA PRIVACIDAD E INTIMIDAD EN REDES SOCIALES – BASE LEGAL

El uso frecuente de las Redes Sociales ha determinado nuevos escenarios de debate respecto el uso de las fotografías que determina cuestionarse sobre los límites del Derecho de los usuarios en las Redes Sociales, que utilizan la fotografía de una persona sin previa autorización del titular; por lo que, resulta importante determinar la infracción y regulación de los alcances de Protección a la Publicación de Fotografías e Imagen, como Derecho Fundamental.

Desde todo punto de vista es siempre la Constitución, la "Madre" de nuestra legislación, y como tal, determina nuestros Derechos Fundamentales. En este sentido, determina como principio que el fin supremo de la sociedad y del Estado es "la persona humana" y como tal la sociedad y el Estado deben respetarse su dignidad.

La Constitución Política Del Perú, del 30 de Diciembre de 1993.

En el Título I, referente a los Derechos de la Persona y de la Sociedad; específicamente el Capítulo I Derechos Fundamentales de la Persona, que a la letra dice:

La Defensa de la persona humana: "Art. 1°.- La defensa de la persona humana y el respeto de su dignidad son el fin supremo de la sociedad y el Estado."

Este principio se ve muchísimas veces afectado en el entorno digital, donde las Redes Sociales manifiestan diferentes tipos de publicaciones que atentan contra la dignidad de la persona.

En este artículo queremos resaltar que el ser humano es el que ataca a otro ser humano, más allá del latinismo "*Homo Homini Iupus*" que pudiera significar "*El hombre es el lobo del hombre*" como primigeniamente Thomas Hobbes lo identifica en 1651. Actualmente, sigue perdiéndose la practicidad de la ética, la moral y los valores que como tal debe corresponderse asimismo y a los demás.

En este sentido, la dignidad de la persona puede ser afectada de diferentes maneras y en el caso de publicaciones desautorizadas de fotografías e imágenes que afectan la vida de las personas, se pueden vulnerar Derechos Fundamentales como la intromisión a la privacidad e intimidad.

Con el desarrollo de la computación y la informática, en el año de 1993 se incorporó a la Constitución, entre otras modificaciones el inciso 6, en el artículo 2:
"Art. 6°.- Que los servicios informáticos, computarizados o no, púbicos o privados, no suministren informaciones que afecten la intimidad personal y familiar […].

Este inciso 6, del numeral 2 de la Constitución contempla claramente la protección a la intimidad de la personal y su esfera familiar, pero no se manifiesta de forma expresa sobre el Derecho a la Privacidad de la persona, de la familia y a la esfera privada de amistades.

Al respecto, cabe resaltar que la Constitución peruana de forma genérica lleva intrínseco la protección del Derecho a la privacidad, en todo su relato.

Siguiendo con la temática; el Código Civil Peruano (D.L. N° 295) se contempla que, sin el consentimiento de la persona, no puede ponerse de manifiesto su vida personal, y aquí también, se puede entender que, como principio, lleva intrínseco la vida privada de la persona.

Codigo Civil Peruano.

La descripcion de la defensa a la privacidad se materializa en el Libro I, Derecho de las personas, Seccion Primera, referente a Personas Naturales.

Asimismo, el Título II, en referencia a los Derechos de la persona […]
Especificamente el "*Articulo 14 – Derecho a la intimidad personal y familiar:*

"La intimidad de la vida personal y familiar no puede ser puesta de manifiesto sin el asentimiento de la persona o si ésta ha muerto, sin el de sus descendientes, ascendientes o hermanos, excluyentemente y en este orden"

Asimismo la Ley 29733, Ley de Protección de Datos, publicada el 03 de julio de 2011 en el Diario Oficial El Peruano, tiene como objeto garantizar el derecho fundamental contemplado en la Constitución, a saber:
La perspectiva de la legislación Civil, siendo importante determinar los alcances de la Ley Nro. 29733 que regula lo concerniente a la Protección de los Datos Personales.

Ley de Protección de Datos Personales, N°29733.

En el título preliminar, especificamente en las Disposiciones Generales, del "Art. 1.- Objeto de la Ley: ***La presente Ley tiene el objetivo de garantizar el derecho fundamental a la proteccion de personas, previsto en el artículom 2, numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen*****"**

Este mismo cuerpo legislativo, reconoce en el Título VII, denominado Infracciones y Sanciones Administrativas, que articula:
Artículo 37.- "Procedimiento Sancionador"
Artículo 38.- Infracciones: leves, graves, muy graves.
Artículo 39.- Sanciones Administrativas y,
Articulo 40.- Multas coercitivas.

Reglamento de la Ley N° 29733, Ley de Protección de Datos Personales. Decreto Supremo N° 003-2013-JUS, (22 de marzo de 2013)
Título VI, Infracciones y sanciones:
Artículo 98, Procedimiento Fiscalizador y ss.
Articulo 115, Procedimiento Sancionador.
Articulo 124, Sanciones.

Código Penal del Perú, Decreto Legislativo N° 635.

Artículo 154, "Violacion de la intimidad"
"*El que viola la intimidad personal o familiar ya sea observando, escuchando o registrando un hecho, palabra, escrito o imagen, valiéndose de instrumentos, procesos técnicos u otros medios, será reprimido con pena privativa de la libertad no mayor de dos años*"
E incluso se agraba la pena, cuando "*el agente revela la intimidad conocida de la manera antes prevista* ***en el párrafo anterior (lo resaltado es nuestro)*** *la pena será no menor de uno ni mayor de tres años y de 30 a 120 días de multa*"
Para efectos de nuestro estudio, el párrafo tercero prescribe:
"*si utiliza algún medio de comunicación social, la pena privativa de libertad será no menor de dos ni mayor de cuatro años y de 60 a 185 días-multa*"

IV. LA IMAGEN EN EL DERECHO CIVIL

En efecto el Código Civil Peruano de 1984, concibe la proteccion del Derecho respecto a la imagen y a la intimidad de las personas (Sentencia reacía en el Expediente N° 01480-2003-HD/TC, de fecha 15 de julio de 20013, Tribunal Constitucional, Derecho ala intimidad como límite del Derecho al acceso a la infromación)

Es así, que el Artículo 15 del Código Civil Peruano señala:
"*Derecho a la imagen y voz. La imagen y la voz de una persona no pueden ser aprovechadas sin autorización expresa de ella o, si ha muerto, sin el asentimiento de su cónyuge, descendientes, ascendientes o hermanos, excluyentemente y en ese orden*"

Asimismo, la interpretación excepciona el asentimiento de la norma que no es necesario cuando el uso o la utilizacion de la imagen y de la voz justifiquen por la notoriedad de la persona, por el cargo que desempeñe, por los hechos de importancia o interés público o por motivos de índole científica, didáctica o cultural, y siempre que se relacione con hechos o ceremonias de interés general que se celebren en espacios público.

Sin embargo, como toda norma y toda excepción tiene un límite, no puede utilizarse la imagen de la persona cuando se atente contra su reputación, contra su honor, buen nombre y decoro del titular de la imagen.

Entonces, es el Código Civil Peruano que contempla la imagen como parte del Derecho de las Personas, y establece sus alcances.

Claro es manifestar que la afectación de la publicación de la imagen de la persona, puede acarrear una violación a su intimidad y vida privada; en tal sentido, debemos advertir que en la Constitución Peruana prevé este Derecho ante un mal uso de las tecnologías.

En este sentido, sabemos que las Redes Sociales brindan todo tipo de información y que el uso de las tecnologías puede ser muy dañino, si no tenemos conciencia del alcance de nuestras publicaciones y de la información que brindamos al respecto; porque cuando hablamos de información se incluyen todo tipo de datos que pueden ser personales y de gran perjuicio al ser humano, sobre todo cuando se trata de publicaciones maliciosas. Por lo tanto, la fotografía o imagen como tal, está contemplada dentro de lo que significa un "dato personal"

V. LEY DE PROTECCIÓN DE DATOS PERSONALES Y LA PROTECCIÓN A LA FOTOGRAFIA E IMAGEN COMO DATO PERSONAL Y COMO DATA SENSIBLE

La definicion legal de "dato" lo encontramos en la Ley N° 29733, Ley de Protección de Datos en el Perú y su Reglamento:

- **Ley de Protección De Datos Personales**, N° 29733, publicada el 03 de julio 2011 en el Diario Oficial "EL Peruano"

"*Artículo 2 Definiciones*
[…] 4. Datos Personales. Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados
Como sabemos en toda Ley debe complementarse con un reglamento, el cual detalla con mayor amplitud la definisión de "Datos Personales"

Reglamento de la Ley de Protección de Datos, Aprobado con Decreto Supremo N° 003-2013-JUS, de fecha 22 de marzo 2013; el cual entró en vigencia el 08 de mayo 2013.

Artículo 2.- Definiciones
[…] 4. Datos Personales: Es aquella información, numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados"

Es aquí, donde después de dos años de vigencia de la Ley N° 29733, se define con mayor claridad el significado legal de los "Datos Personales" incluyendo la información "fotográfica".

Como ya hemos visto, llamaremos indistintamente en este artículo a la "fotografía" como la "imagen publicada de una persona", ya que el resultado de una fotografía es una "imagen"

a. **LA FOTOGRAFIA O IMAGEN COMO DATA SENSIBLE**

Siendo escaso en nuestro país, la doctrina sobre el derecho de imagen y dada la actual revolución tecnológica está marcada en el sendero jurídico, su estudio e investigación para contribuir con los mecanismos necesarios que enriquezcan la legislación peruana en esta materia, partiendo desde su reconocimiento en la Constitución Política del Perú y las leyes pertinentes.

Una de las grandes interrogantes hasta hace poco en el Perú, era conocer jurídica y oficialmente la clasificación de la fotografía o imagen de una persona, e identificarla como dato personal; es así que, en el año 2017, la Dirección General de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, se manifestó con Oficio N° 213-2017-JUS/DGTAIPD de fecha 10 de octubre 2017, en respuesta a una consulta realizada por una empresa, sobre la fotografía, su concepto, características, y consentimiento. Por lo que, resumo las conclusiones al respecto:

- Los datos sensibles son los Datos Personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular, datos referidos al origen racial y étnico, ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales, afiliación sindical, e información relacionada a la salud o a la vida sexual

- Asimismo, el Reglamento de la Ley de Protección de Datos Personales LPDP, aprobado por Decreto supremo Nro. 013-2003-JUS, establece que un dato personal es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que puedan ser razonablemente utilizados. Y dentro de ellos agrupa a los datos sensibles que se refieren a la información que se relaciona con las características físicas, morales o emocionales, hechos o circunstancias de su vida afectiva o familiar, los hábitos personales que corresponden a la esfera más íntima, la información relativa a la salud física o mental u otras análogas que afecten su intimidad.

- Es decir, los datos sensibles, cumplen dos características básicas:
  - Son biométricos y
  - Hacen posible la identificación del titular

Así vemos que, la fotografía es considerada como un "Dato Sensible" y como tal merece una legislación adecuada, por cuanto el Ministerio de Justicia lo que hace es interpretar la Ley con el fin de responder una consulta realizada por una empresa, evidenciando de esta forma la necesidad de ampliar la legislación actual a mérito de tener una mejor herramienta jurídica sobre la Protección de la Imagen como Dato Sensible.
Por otro lado, es indispensable saber que el ámbito de aplicación de la Ley N° 29733 Ley de Protección de Datos en el Perú, sólo protege los Bancos de Datos de las Empresas e Instituciones Públicas o Privadas, a saber

- Ley N° 29733, ***Artículo 3. Ámbito de aplicación***
  La presente Ley es de aplicación a los Datos Personales contenidos o destinados a ser contenidos en bancos de Datos Personales de administracion pública y de administracion privada, cuyo tratamiento se realiza en el territorio nacional. Son objeto de especial proteccion de datos sensibles.

Las disposiciones de esta Ley no son de aplicación a los siguientes Datos Personales:

1. A los contenidos destinados a ser contenidos en nando de Datos Personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar.
2. A los contenido o destinados a ser contenidos en banco de datos de administracion pública, sólo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las comprenencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública y para el desarrollo de actividades en materia penal para la investigacion y represion del delito.

Si bien es cierto, el Reglamento, resalta que son de especial proteccion los "datos sensibles"; también, esta legislación aclara que la Ley no es de aplicación a los bancos de Datos Personales creados por personas naturales referentes a la vida privada o familiar.

Sin embargo podemos apreciar que al ámbito de aplicación que indica el Reglamento es mucho mas amplio y podría absolver algunas de nuestras interrogantes, veamos:

- Decreto Supremo N° 003-2013-Jus, Reglamento De La Ley 29733 Ey De Protección De Datos, de fecha 22 de Marzo 2013, el cual entró en vigencia el 08 de mayo 2013.

Artículo 3.- Ámbito de aplicación
El presente reglamento es de aplicación al tratamiento de los Datos Personales contenido en un banco de Datos Personales o destinados a ser contenido en banco de Datos Personales.
Conforme a lo dispuesto por el numeral 6 del artículo 2 de la Constitucion Política del Perú y el artículo 3 de la Ley, el presente reglamento se aplicará a toda modalidad de tratamiento de

Datos Personales, ya sea efectuado por personas naturales, entidades públicas o instituciones del sector privado e independientemente del soporte en el que se encuentren.

Es así, que la existencia de normas o regímenes particulares o especiales, aún cuando incluyan regulaciones sobre Datos Personales, no excluye a las entidades públicas o instituciones privadas a las que dichos regímenes se aplican del ámbito de aplicación de la Ley y del presente reglamento.
Lo dispuesto en el párrafo precedente no implica la derogatoria o inaplicacion de las normas particulares, en tanto su aplicación no genere la afectacion del derecho a la proteccion de Datos Personales.

Siguiendo el desarrollo de los derechos que la Ley de Protección de Datos Personales del Perú, indica, es necesario tambien mencionar, el artículo del Derecho a la Indemnización. Podemos observar lo que la Ley N° 29733, indica al respecto:

"***Artículo 25. Derecho a ser indemnizado***

El titular de Datos Personales que sea afectado a consecuencia del incumplimiento de la presente Ley por el titular o por el encargado del banco de Datos Personales o por terceros, tiene derecho a obtener la indemnización correspondiente, conforme a Ley."

Y aquí volvemos a referirnos que tiene Derecho la persona afectada y/o dañada a una indemnización cuando se trata de un Banco de Datos; es decir, podemos aclarar la figura jurídica en tanto el titular es afectado por haber utilizado sin autorización sus Datos Personales, y entendiéndose que forma parte de una relación y lista de personas que pertenecen a una Empresa o Institución. Sin embargo, es necesario siempre el consentimiento expreso del titular, sin lo cual el Derecho queda inminente a denuncia, trámite e indemnización respectiva. Es por ello, que agotar la vía administrativa conlleva a un requisito indispensable e ineludible para proceder a ese Derecho.

Hasta aquí vemos que parece vislumbrarse un tema controversial para el objetivo de este artículo que conlleva la defensa de los Derechos de la Persona y que asimismo nos toca, en consecuencia, investigar las herramientas juridicas, sociales y políticas, aplicables para la defensa del abuso de publicaciones y comentarios de imágenes de personas en las Redes Sociales, que pueden apreciarse en diferentes situaciones, lugares y hechos, donde nuestra vida privada debe ser respetada sin aceptar ningún tipo de intromisiones que la afecten.

Si bien, podemos adelantar que es de libre decisión formar parte de una Red Social también es necesario conocer de su buen uso y consecuencias al respecto.

VI. PERO, QUÉ SUCEDE, ¿CUANDO LA FOTOGRAFÍA DE UNA PERSONA ES PUBLICADA EN ALGUNA RED SOCIAL SIN AUTORIZACIÓN PREVIA, AFECTANDO SU VIDA PRIVADA Y CAUSÁNDOLE INCLUSO UN GRAVE DAÑO?

En el actual mundo que vivimos, la comunicación virtual, como hemos mencionado, ha abarcado casi la totalidad de la interacción entre los seres humanos; pues, son muchas las

horas que las personas están conectadas con el procesador o la *Laptop*; y principalmente, se ha masificado el uso de los celulares, cuyos propietarios, por lo general pasan su día "chateando", ocupados en las Redes Sociales e interconectándose con diferentes personas. Esta vorágine de Internet y las Nuevas Tecnologías trae como reto, el capacitarse debidamente para utilizar las herramientas tecnológicas de manera positiva, porque fueron creadas para mejorar la vida de las personas y el desarrollo de nuestra sociedad.

Sin embargo, es muy lamentable que se llegue a un grado extremo de utilizar las Redes Sociales, como una obligación de comunicación que llega a extremos de absorber nuestra propia vida y la falta de respeto por la vida de los demás. Caso curioso es el de aquellas personas que utilizan una Red Social como Diario Personal para publicar todo lo que hacen, y en el mismo sentido, se sienten atraídas de irrumpir en la vida de los demás; en una palabra "estar constantemente conectados a la Red", se convierte en una prioridad, una necesidad y hasta una "urgencia", que se debe controlar a bien de no caer en la robotización.

Lamentablemente, muchas de las publicaciones de videos e imágenes en algunas Redes Sociales, como *Facebook, Instagram, YouTube,* etc. se hacen masivas indiscriminadamente, y puede causar graves daños al afectado. Como un simple ejemplo mencionaremos el de una persona que viaja para cumplir una función laboral y es sorprendido por la publicación de una foto en el momento que compartía un "brindis" en plena travesía; en este caso, la persona que publica la foto puede ser un extraño que además agrega un comentario mal intencionado y malicioso respecto a ello, causando un daño colateral debido a la publicación de la imagen no autorizada y además del comentario dañoso o nocivo.

Este tipo de personas que no tienen ningún respeto por la vida privada y que mal utilizan las Redes Sociales con el ánimo de desprestigiar a sus colaterales resultan una "lacra" para la sociedad, porque sin fundamento alguno y violando los derechos inherentes a la persona, mienten, estafan, calumnian y, muchas veces, no tienen límite, para destruir moralmente a la persona, valiéndose de herramientas tan útiles como son las tecnologías, que las convierten en un arma letal e irreparable.

En este sentido, nos enfrentamos al detrimento de los valores en el ser humano; y es nuestra responsabilidad, no dejarnos absorber ni creer sólo por lo que vemos; es primordial elegir el respeto por los Derechos Fundamentales de la Persona, respetando la vida privada, los sentimientos y los valores de cada cual, para no afectar ni verse afectados por las consecuencias de sus malos actos. Cabe a colación la reseña que hace el periodista español Justino Sinova al libro de "Homo Videns" de Giovanni Sartori, quien además de hacer un llamado a la invasión de la multimedia, hace un llamado a despabilarnos y salvar nuestra cultura "*…una invitación a buscar la realidad en la maraña de la sobreinformación y de la imagen, que a veces desconcierta y "también miente" […]* [1]

En la actualidad parece ser una acción diaria y normal la publicación de imágenes y videos desautorizados, y pocos nos sorprendemos ante su difusión en las Redes Sociales, porque

[1] Sartori, Giovanni "Homo Videns – La Sociedad Teledirigida", Editorial Debolsillo (punto de lectura) - Año de edición 2012.

parece que, se ha convertido en un tema de "costumbre", pero como bien menciona el autor Gil Villilengua[2], este accionar, no puede dejar de ser un desafío en el enfoque jurídico.

Este enfoque jurídico debe contemplar la magnitud del daño causado por la intromisión de terceros en nuestra vida privada y la publicación de nuestra imagen en las Redes Sociales, pero la magnitud del Daño resultar ser *metacuantificable puesto que,* sólo puede ser medible por la misma persona afectada o perjudicada y es ahí donde la Ley tendría que aplicar un castigo severo al respecto.

VII. INDEMNIZACION Y RESARCIMIENTO

Es menester conocer primero la diferencia entre los conceptos de indemnización y resarcimiento.

En este sentido, tomaré un resumen del artículo publicado por el portal jurídico Legis.pe[3], respecto al análisis al Código Civil Peruano el cual no establece una clara distinción entre indemnización y resarcimiento (Ver artículos 1321, 1969, 1970 y siguientes) es por ello, que debemos recurrir a la doctrina, y en esta oportunidad, mencionaremos brevemente al Dr. Jorge Beltrán:

"El ***resarcimiento*** *se refiere a la compensación que debe asumir un sujeto, quien se encuentra en una situación jurídica subjetiva de desventaja, tras haber ocasionado una consecuencia dañosa siempre que se haya demostrado la existencia de cada uno de los* ***elementos de la responsabilidad civil****, mientras que la* ***indemnización*** *se refiere a la compensación, de* ***fuente legal****, que se impone por la contingencia atendida por el ordenamiento jurídico*."

Cabe aclarar que para muchos estudiosos no existe diferenciación, y para otros existe una variación al respecto, por lo que, prefiero quedarme con esta definición, que considero bastante clara al respecto y estoy de acuerdo con esta conceptualización, sin perjuicio de entrar en una mayor profundización al respecto, que evocaremos en otra oportunidad y con fines estrictamente académicos y productivos para el saber jurídico.

VIII. ¿CÓMO SE PODRÍA MEDIR EL DAÑO MORAL CAUSADO POR LA PUBLICACIÓN NO AUTORIZADA DE LA FOTO O LA IMAGEN EN REDES SOCIALES?

El Código Civil Peruano reconoce dos tipos de daño, el daño patrimonial y el extramatrimonial. El presente estudio se circunscribe dentro del segundo tipo de daño extrapatrimonial, que vendría a ser el daño ocasionado a la persona en sí misma; o mejor dicho, la afectación recae sobre la subjetividad de ella. Como una subdivisión de ésta, se tiene el Daño Moral y el Daño a la Persona.

[2] Gil V., L., *Los derechos al honor, a la intimidad y a la propia imagen en las redes sociales: La difusión no consentida de imágenes* (ISSN 1695-078x ed.). REDUR, 2016.
[3] https://legis.pe/es-lo-mismo-indemnizacion-que-resarcimiento/

El Código Civil Peruano respecto al Daño Moral, prescribe:
Artículo 1984.- "*El Daño Moral es indemnizado considerando su magnitud y el menoscabo producido a la víctima o a su familia"*

No cabe duda de que como medida eficaz de defensa de los Derechos de la Personalidad puede considerarse el Artículo 1984, del Código Civil el cual se refiere al Daño Moral "*El Daño Moral es indemnizado considerando su magnitud y el menoscabo producido a la víctima o a su familia*" es decir, este hecho bien conocido en la doctrina ha tenido siempre mucha dificultad en ubicar el Daño Moral dentro de las categorías de la responsabilidad extracontractual.

En efecto, si consideramos al Daño Moral como un daño extrapatrimonial en este caso no puede ser reparado patrimonialmente mediante una indemnización porque, *per definitionem*, es inapreciable en dinero (para los Romanos *Litis aestimatio*) Pero no cabe duda de que tenemos que entender esta noción en el sentido de un daño patrimonial o económico.

Otro de los análisis versa sobre la indemnización según el Código Civil Peruano:

Artículo 1985.- "*La indemnización comprende las consecuencias que deriven de la acción u omisión generadora del daño, incluyendo el lucro cesante, el daño a la persona y el Daño Moral, debiendo existir una relación de causalidad adecuada entre el hecho y el daño producido. El monto de la indemnización devenga intereses legales desde la fecha en que se produjo el daño*".

A consecuencia legal, una indemnización *"que se derive de la acción y omisión generadora del daño; incluyendo el lucro cesante, el daño a la persona y el Daño Moral*" Por lo que, ante una acción (hecho de publicar una fotografía o imagen) puede generar una afectación (en Redes Sociales y sin autorización). En este sentido, para nuestra investigación en "concreto" es necesaria la existencia de una causalidad adecuada entre el hecho y el daño producido.

Para efecto del presente aporte, el Daño Moral se entiende a la lesión a los sentimientos de la víctima y que produce un gran dolor, una afección o un sufrimiento, ejemplo: publicar una foto de una persona en un escenario íntimo, obviamente sin el consentimiento del titular de la foto. Este ejemplo, nos refresca las indistintas violaciones a los Derechos Humanos, cuando se han publicado imágenes o fotos en escenas totalmente comprometedoras y lesivas para él o la propietaria de la foto; acontecimientos que incluso han derivado en casos extremos como suicidios.

Por tanto, al Daño Moral le corresponde el resarcimiento.

IX. ¿ENTONCES COMO PODEMOS EJERCER NUESTRO DERECHO DE RESARCIMIENTO?

En realidad ni la Ley ni alguna normatividad establece el procedimiento para interponer este tipo de recurso, a fin de lograr el resarcimiento y de existir un daño objetivizado.

Es necesario implementar mecanismos procesales para acceder a la justicia ante cualquier tipo de vulneración de los Derechos Fundamentales, por la publicación no autorizada de la foto en las Redes Sociales, es por ello, que el planteamiento del presente artículo busca la intervención de:

- Ministerio de Justicia y Derechos Humanos del Perú.
- La Autoridad para la Protección de Datos del Perú.
- El Poder Judicial, a través, de sus juzgados especializados en Derecho.
- Los órganos reguladores del servicios y defensa de usuarios (servicio de las Redes Sociales)
- Colegio de Abogados de Lima.

X. CONCIENTIZACIÓN DIGITAL, PREVENIR ANTES QUE LAMENTAR, LA PRIVACIDAD EMPIEZA POR UNO MISMO

La palabra "concientizar" significa provocar que alguien tome conciencia de algo, y la "conciencia" es propia del ser humano, es decir, se trata de mostrar o hacer conocer una verdad, así como las consecuencias de las propias decisiones, profundizando en el conocimiento de la realidad.[4]

En este sentido, cuando tratamos de conceptuar el término de "Concientización Digital" estamos refiriéndonos a tomar conciencia del uso e impacto de las Tecnologías. Este concepto es mucho más amplio que la "Educación Digital", que se encarga de aplicar las Tecnologías de la Información y Comunicaciones – TIC, al proceso de enseñanza y aprendizaje, en favor de lograr las metas y objetivos de cada disciplina.

Por tanto, a consecuencias de las investigaciones y los estudios realizados propongo la siguiente definición: "La Concientización Digital versa en el Saber Humano, conocer, analizar, reflexionar e interiorizar el impacto del desarrollo de las ciencias tecnológicas y de innovación que interactúan con nuestras vidas; conociendo a plenitud sus efectos y consecuencias en la vida de las personas: familiar, social, profesional, empresarial, etc., como así el cambio que ha originado en nuestras sociedades a nivel mundial".

El trabajo de la "Concientización Digital" es arduo, continuo y de constante mejora, el cual incluye la educación, y prevención en las consecuencias para la sociedad. Si bien es cierto, que este impacto debería ser un cambio y mejora en nuestras vidas, también es cierto que debe incluir necesariamente, el conocimiento y modo de prevenir temas tan fatales, como el *Grooming*, *Ciberbullying*, *ciberdelincuencia*, etc., con mecanismos, herramientas y procedimientos que deben partir por la implantación y ejecución de Políticas Públicas con el trabajo unificado de las Instituciones Privadas, el Estado y la Sociedad en su conjunto.

Hay muchas personas que tenemos la vocación de instruir y compartir conocimientos, partiendo por utilizar las Redes Sociales y los entornos digitales en general, en favor de la "Concientización Digital", pero a pesar que podemos ser muchas, resulta insuficiente si no tenemos el apoyo político y las normatividad adecuada que hagan realidad nuestra misión.

[4] http://quesignificado.com/concientizar/

Hay mucho por versar y mucho por hacer, sin embargo, partir por el respeto a los Derechos Humanos, en nuestra vida cotidiana y en el uso de las Tecnologías, desde nuestros hogares, escuelas, campos universitarios, etc., es prevenir la delincuencia y forjar, seres humanos conscientes de nuestra realidad digital en favor del crecimiento y desarrollo de nuestro país.

XI. CONCLUSIONES

- El obligado a resguardar sus derechos fundamentales, en el uso y en la administración de la foto y la imagen, parte por uno mismo y después, es el Estado el llamado a garantizarla.
- La afectación moral por el uso no autorizado de la foto en las Redes Sociales puede acarrear consecuencias irreversibles para el propietario de la foto, debido a que su consumación es inmediata o de efecto consumado.
- Implementar Políticas Públicas para concientizar a la población en el uso de las Tecnologías Digital, Redes Sociales y Derechos Humanos.
- Plantear Reformas Educativas con la participación del Ministerio de Economía y Finanzas, el Ministerio de Educación, Ministerio de Cultura, Ministerio de Justicia y Derechos Humanos, Ministerio de la Mujer y Poblaciones Vulnerables, Entidades Dependientes y órganos *ad hoc* que viabilicen, aseguren y garanticen la inviolabilidad de los Derechos Humanos en las Redes Sociales, con énfasis en la concientización del daño que implica publicar una foto no autorizada en las Redes Sociales.

XII. BIBLIOGRAFÍA Y FUENTES REFERENCIALES

- Alfabetización Digital https://www.alfabetizaciondigital.redem.org/importancia-de-las-redes-sociales-en-el-entorno-digital/
- Beltrán Pacheco, Jorge Alberto. "Eclipse: cuando se confunde el Derecho Laboral con el Derecho Civil". *Dialogo con la Jurisprudencia*, N° 143, Gaceta Jurídica, Lima 2010.
- Alpa, G. *Nuevo Tratado de la Responsabilidad Civil,*Jurista Editores, Lima, 2006.
- *ALPA, Guido, Nuevo Tratado de la Responsabilidad Civil, Jurista Editores, Lima, 2006.*
- Azurmendi, A. *El derecho a la propia imagen: Su identidad y aproximación al derecho a la información*, Civitas SA., Madrid,1997.
- Busto, J. M., *La antijuricidad del daño resarcible en la responsabilidad civil extracontractual*, Tecnos, Madrid, 1998.
- Corte de Apelaciones de Valparaíso, Derecho a la propia imagen. *Derecho y jurisprudencia y Gaceta de los tribunales*, 1997.
- De Cupis, A. *El Daño – Teoría General de la Responsabilidad Civil,* Bosch, 1995.
- De Trazegnies, F., *La responsabilidad extracontractual,* PUCP, Lima, 1988.
- Fernández, X., & Serrano, O. R., *Responsabilidad civil extraccontractual por el uso de vehículos automotores,* Facultad de Ciencias Jurídicas y Socioeconómicas, Bogotá, 1988.
- Gil V., L., *Los derechos al honor, a la intimidad y a la propia imagen en las redes sociales: La difusión no consentida de imágenes* (ISSN 1695-078x ed.). REDUR, 2016.

- Gil Villilengua, L. “Los derechos al honor, a la intimidad, y a la propia imagen en las redes sociales: La difusión no consentida de imágenes”. – Universidad de Rioja: REDUR. Doi: ISSN 1695-078x, 2016.
- LEGIS.PE ¿Es lo mismo indemnización que resarcimiento? https://legis.pe/es-lo-mismo-indemnizacion-que-resarcimiento/
- Sartori, Giovanni “Homo Videns – La Sociedad Teledirigida”, Editorial Debolsillo (punto de lectura) - Año de edición 2012
- LEGIS.PE Plataforma virtual que promueve el debate y la discusión de temas político-jurídicos. Directora: Sandra Gutiérrez Iquise. https://legis.pe/es-lo-mismo-indemnizacion-que-resarcimiento/

IMPLEMENTACIÓN DE LAS TECNOLOGÍAS (TIC) EN LA BÚSQUEDA DE MAYOR EFICACIA PROCESAL EN LA ADMINISTRACIÓN DE JUSTICIA.

Por: ***Cristian Arteaga***
Colombia

Introducción

La humanidad y el derecho han sufrido grandes cambios a partir de su desarrollo histórico donde han surgido las más importantes cartas de derechos que se encaminaron a proclamar derechos y libertades individuales de las personas, no obstante, estos derechos comienzan a verse materializado de una manera más generalizada a partir de la finalización de la segunda guerra mundial, en razón, con el surgimiento de los estados sociales.

Por otro lado, el mundo también ha sido testigo de los grandes cambios causados por un fenómeno tan importante en la sociedad como lo ha sido la revolución tecnológica, que trajo consigo un desarrollo exponencial en las diferentes áreas del conocimiento, para mejorar la aplicación de las mismas, no obstante, la realidad de Colombia parece no haber evolucionado con el mundo, esto se puede ver en la gran deficiencia que tiene la rama judicial a la hora de dar solución rápida a los casos que se presentan diariamente a ella atentando de esta manera al principio de celeridad procesal, por ende, las personas se abstienen de acudir a la administración de justicia prestada del estado ya sea por razones económicas o de tiempo, prefiriendo así hacer justicia a mano propia.

Por esa razón, se necesita un estudio minucioso que le facilite al distrito judicial de Villavicencio implementar las nuevas tecnologías a su alcance en las diferentes dependencias judiciales, buscando así maximizar el servicio prestado por las mismas.

Marco normativo

En la presente sección se expone la normatividad nacional en materia de inmersión de las TIC en la Administración de justicia en búsqueda de desarrollo y buena prestación del servicio de justicia.

Constitucional

A nivel nacional, algunos fundamentos constitucionales en torno a la necesidad del desarrollo de la administración de justicia se encuentran en: (I) el preámbulo de la constitución de 1991 el cual establece que es un fin del estado asegurar la justicia, la libertad y la paz, dentro de un marco normativo, para lo que se hace evidente la necesidad utilizar los recursos electrónicos de los que dispone el estado.

Importante es tener claro que el carácter vinculante del preámbulo constitucional se establece en la sentencia C/ 477/ 05; (II) El artículo 2 estipula que son fines esenciales del estado servir a la comunidad y garantizar la efectividad de los principios, derechos y deberes consagrados

en la constitución, por ende, para poder cumplir esta obligación en relación a los administrados debe evitar el colapso del sistema judicial por medio de las TIC; (III) En virtud del artículo 229 se garantiza el derecho de toda persona para acceder a la administración de justicia, derecho que se garantizaría de manera progresiva con la inmersión de las TIC en la administración de justicia, en el entendido de que esto aumentaría la cobertura del servicio; (IV) finalmente, el literal b del artículo 152 constituye que la administración de justicia se debe regular por ley estatutaria, haciendo claridad de la importancia del buen servicio de justicia.

Leyes

En lo referente a otras normas, Colombia promulgo la ley 270 de 1996. Estatutaria de la administración de justicia, la cual se abre como otro instrumento normativo, que en su artículo segundo insta al estado garantizar a los asociados el acceso a la justicia, además, en su artículo 4 se encarga de garantizar el célere funcionamiento de este servicio, pues, de ello depende directamente que sean protegidas las garantías y libertades de los administrados. Por otro lado, el artículo 7 establece la cláusula de la eficiencia en la administración de justicia, en otras palabras, que los funcionarios y empleados de la rama judicial deben ser diligentes con la sustanciación de los temas que estén a su cargo, para lo cual es necesario que cuenten con las herramientas suficientes para hacer efectivo este principio sin importar el volumen de trabajo al que se encuentren sometidos, por ende, finalmente, el artículo 95 que regula en estricto sentido la materia que a este trabajo atañe, es decir, las tecnologías al servicio de la administración de justicia, se expone textualmente:

> *El Consejo Superior de la Judicatura debe propender por la incorporación de tecnología de avanzada al servicio de la administración de justicia. Esta acción se enfocará principalmente a mejorar la práctica de las pruebas, la formación, conservación y reproducción de los expedientes, la comunicación entre los despachos y a garantizar el funcionamiento razonable del sistema de información.*
>
> *Los juzgados, tribunales y corporaciones judiciales podrán utilizar cualesquier medios técnicos, electrónicos, informáticos y telemáticos, para el cumplimiento de sus funciones.*
>
> *Los documentos emitidos por los citados medios, cualquiera que sea su soporte, gozarán de la validez y eficacia de un documento original siempre que quede garantizada su autenticidad, integridad y el cumplimiento de los requisitos exigidos por las leyes procesales.*
>
> *Los procesos que se tramiten con soporte informático garantizarán la identificación y el ejercicio de la función jurisdiccional por el órgano que la ejerce, así como la confidencialidad, privacidad, y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley.*

En el entendido del anterior artículo queda clara la obligación del estado al adoptar las tecnologías que se encuentran actualmente a su disposición para la efectividad del servicio

público a la administración de justicia, encargado directo de la protección de los bienes, honra, vida, derechos y libertades de los asociados.

Por otro lado, en el año 2011 es promulgada la ley 1437 por medio de la cual se crea el Código de procedimiento administrativo y de lo contencioso administrativo (CPACA), esta ley llega al ordenamiento jurídico con la intención de buscar un funcionamiento célere y eficaz de la función administrativo, debido a ello, comienza por establecer una serie de procedimientos sostenidos en el uso de las herramientas tecnológicas al alcance el Estado para alcanzar dichos fines.

En el artículo 53 del CPACA se establece que los trámites administrativos se pueden llevar a cabo usando los medios electrónicos, claro está, sin limitar le a las personas los otros mecanismos con los que cuente para acceder a la justicia y siempre que las entidades tengan las herramientas necesarias para garantizar el acceso de gratuidad a estos mecanismos electrónicos y tecnológicos. El articulo 56 contempla la notificación electrónica cuando el ciudadano lo ha aceptado de manera previa y, finalmente, el artículo 59 de la misma ley regula la materia del expediente electrónico, entendiéndose por este los documentos y diligencias de un litigio o proceso administrativo que se encuentre foliado con la correspondiente firma digital de la correspondiente autoridad.

Finalmente, frente a la regulación legislativa de carácter ordinario, se encuentra el Código General del Proceso, ley 1564 del año 2012 que en la sección segunda, titulo 1, capitulo 1, articulo 103, reglamenta el uso de las tecnologías de la información y las comunicaciones, estableciendo el camino para el correcto funcionamiento del sistema judicial, manda a que en todas las actuaciones judiciales debe procurarse el uso de las tecnologías de la información y las comunicaciones, con el fin de agilizar y facilitar el acceso a la justicia, así como ampliar la cobertura actual del sistema.

Para ello, conviene que las actuaciones judiciales se podrán realizar a través de mensajes de datos. La autoridad judicial deberá contar con mecanismos para permitir generar, archivar y comunicar mensajes de datos.

Por otro lado, atribuye a la sala administrativa del consejo superior de la judicatura la función de adoptar las medidas necesarias para una vez entre en vigencia la ley se garanticen las condiciones técnicas a los funcionarios para el cumplimiento de la aplicación de las TIC en el ejercicio de sus funciones.

Por último, al hacer referencia al ***plan de justicia digital*** dispone que estará integrado por todos los procesos y herramientas de gestión de la actividad jurisdiccional por medio de las tecnologías de la información y las comunicaciones, que permitan formar y gestionar expedientes digitales y el litigio en línea. El plan dispondrá el uso obligatorio de dichas tecnologías de manera gradual, por despachos judiciales o zonas geográficas del país, de acuerdo con la disponibilidad de condiciones técnicas para ello. Dejando de esta manera solidas las bases normativas para el desarrollo de este tema.

Normatividad	Articulado
Constitución política de 1991	Preámbulo, Art 2, Literal b Art 152, Art 229.
Ley 270 de 1996 "Estatutaria de Justicia"	Art 4, Art 7, Art 95.
Ley 1437 de 2011 "Código de procedimiento administrativo y de lo contencioso administrativo"	Art 53, Art 56, Art 59.
Ley 1564 de 2012 "Código general del proceso"	Art 103

Fuente: Creación propia del autor.

De la administración de justicia

En razón de ser un tema coyuntural y trasversal de la presente investigación, se hace imperativo desglosar todo lo referente a él, por ende, se traen a colación, el concepto y los principios que rigen la administración de justicia en el marco normativo colombiano. Para así poder establecer como se vulneran las garantías establecidas por la normatividad al no aplicarse de manera correcta las TIC:

Definición

El artículo 1 de la ley 270 del año 1996, estatutaria de justicia, establece que la administración de justicia:

> *"Es la parte de la función pública que cumple el Estado encargada por la Constitución Política y la ley de hacer efectivos los derechos, obligaciones, garantías y libertades consagrados en ellas, con el fin de realizar la convivencia social y lograr y mantener la concordia nacional."*

La definición que esta ley consagra, hace énfasis en el importante rol que le tiene la función pública de administrar justicia, que pasa por hacer cumplir las obligaciones y garantizar los derechos de todas las personas naturales y jurídicas, tanto de derecho público como privado, para, garantizar la paz y el orden dentro el grupo social al cual está llamada a aplicarse. Así mismo, el derecho a la administración de justicia ha sido definido por la jurisprudencia constitucional, en la sentencia T-283/13 Como:

> "*la posibilidad reconocida a todas las personas residentes en Colombia de poder acudir en condiciones de igualdad ante los jueces y tribunales de justicia, para propugnar por la integridad del orden jurídico y por la debida protección o el restablecimiento de sus derechos e intereses legítimos, con estricta sujeción a los procedimientos previamente establecidos y con plena observancia de las garantías sustanciales y procedimentales previstas en las leyes. Aquella prerrogativa de la que gozan las personas, naturales o jurídicas, de exigir justicia, impone a las autoridades públicas, como titulares del poder coercitivo del Estado y garantes de todos los derechos*

ciudadanos, distintas obligaciones para que dicho servicio público y derecho sea real y efectivo."

Este concepto que establece la Corte constitucional sirve para explicar detalladamente y de manera más completa unificar criterios sobre que es el derecho a la administración de justicia y la responsabilidad que adquiere el Estado en relación a los administrados de prestar un eficiente y eficaz servicio público de justicia, de la misma manera, establece que la obligación del estado en relación a sus habitantes:

"*puede dividirse en tres categorías, a saber: las obligaciones de respetar, de proteger y de realizar los derechos humanos. Con base en esta clasificación, a continuación, se determinará el contenido del derecho fundamental a la administración de justicia. En primer lugar, la obligación de respetar el derecho a la administración de justicia implica el compromiso del Estado de abstenerse de adoptar medidas que tengan por resultado impedir o dificultar el acceso a la justicia o su realización. Asimismo, conlleva el deber de inhibirse de tomar medidas discriminatorias, basadas en criterios tales como el género, la nacionalidad y la casta. En segundo lugar, la obligación de proteger requiere que el Estado adopte medidas para impedir que terceros interfieran u obstaculicen el acceso a la administración de justicia del titular del derecho. En tercer lugar, la obligación de realizar implica el deber del Estado de (i) facilitar las condiciones para el disfrute del derecho y, (ii) hacer efectivo el goce del derecho. Facilitar el derecho a la administración de justicia conlleva la adopción de normas y medidas que garanticen que todas las personas, sin distinción, tengan la posibilidad de ser parte en un proceso y de utilizar los instrumentos que la normativa proporciona para formular sus pretensiones."*

Ahora bien, la Corte hace el ejercicio de explicar de manera minuciosa cada una de las obligaciones del Estado, donde cabe rescatar que, además de evitar la obstrucción por parte de terceros y la aplicación de medidas que limiten este derecho, insta, al estado a adoptar medidas y normas que faciliten el disfrute de este derecho por parte de los habitantes, valga aclarar que en el entendido de esta investigación, las normas que regulan esta materia ya existen, afirmación que se sustenta en el marco normativo del presente trabajo, por ello, el paso a seguir del estado es materializar todos los preceptos contemplados en la normatividad.

El artículo 4 de la ley establece el principio de celeridad en la función de justicia, planteando:

"La administración de justicia debe ser pronta, cumplida y eficaz en la solución de fondo de los asuntos que se sometan a su conocimiento. Los términos procesales serán perentorios y de estricto cumplimiento por parte de los funcionarios judiciales. Su violación injustificada constituye causal de mala conducta, sin perjuicio de las sanciones penales a que haya lugar"

En el caso concreto se puede afirmar que el problema central radica en la congestión de procesos en manos de la rama judicial, que, a pesar de contar con este volumen tan alto de trabajo, no cuenta con las herramientas necesarias para realizarlo de la mejor manera, por

dicha razón, se hace evidente que la aplicación de las TIC entra a jugar un papel importante en la protección de estos principios.

Ahora, el artículo 6 de la ley 270, consagra la cláusula de gratuidad en la administración de justicia, contempla así que: *"La administración de justicia será gratuita y su funcionamiento estará a cargo del Estado, sin perjuicio de las agencias en derecho, costas, expensas y aranceles judiciales que se fijen de conformidad con la ley"* Deja de esta manera claro que todos los costos en relación a la aplicación de los medios electrónicos corren a cargo del estado, por ser este el directamente el obligado a garantizar la efectiva prestación de este servicio, fundada esta afirmación en la teoría que ubica la razón de existencia del Estado en la efectiva prestación de servicios públicos, como la justicia.

Finalmente, el artículo 7 de la ley establece el principio de eficiencia, fundando que:

> *"La administración de justicia debe ser eficiente. Los funcionarios y empleados judiciales deben ser diligentes en la sustanciación de los asuntos a su cargo, sin perjuicio de la calidad de los fallos que deban proferir conforme a la competencia que les fije la ley."*

Bajo lo que postula este principio se hace de suma importancia la capacitación de los funcionarios y empleados judiciales en el correcto uso de las TIC, en razón de que, de nada ayudaría a la eficiencia del sistema implementar un sofisticado sistema tecnológico, cuando no cuenta con unos funcionarios capaces de hacer buen uso y sacar todo el provecho del potencial del mismo.

Estado actual y desafíos de la implementación de las Tic en Villavicencio

El Distrito Judicial de Villavicencio está formado por un Tribunal Administrativo (Derecho Contenciosos Administrativo) un Tribunal Superior (Derecho Penal, Laboral, Civil, Agrario, Familia), que a su vez se despliega en despachos judiciales de Juzgados de Circuito, Especiales, Descongestión y Municipales. En los cuales se hace evidente un claro déficit en relación a la aplicación de tecnologías, aun, entendiendo que por mandato legal y constitucional se les insta a tomar esas medidas en pro de garantizar la célere, eficaz, eficiente y universal administración de justicia a los habitantes del territorio. Esta dificultad en materia de aplicación se puede dar por variados aspectos:

-El desconocimiento de jueces y magistrados en el uso de estos medios electrónicos, por lo que resulta necesario en primer lugar que el Estado, a través de la autoridad correspondiente el Consejo Superior de la Judicatura, promueva y fortalezca la cualificación en razón de hacer viable este avance que se hace necesario.
-La inoperancia o falta de iniciativa de las autoridades designadas para materializar estos procesos.
Ahora bien, en algunos tribunales del país se ha realizado ya este avance de manera satisfactoria. Referente importante resulta el Tribunal Administrativo del Departamento del Magdalena dirigido por la magistrada María Victoria Quiñones Triana, claro ejemplo del esfuerzo por implementar estas medidas por medio del grupo "Victoria en línea" que sustentándose en la plataforma GDATA implementa de manera progresiva toda suerte

de herramientas electrónicas y tecnológicas que resultan muy didácticas y de fácil acceso a los interesados en acceder a los servicios del tribunal.

Entre los cuales se encuentra la posibilidad de: Acceder a expedientes digitales a los cuales solo tienen acceso las partes, los abogados y el ministerio público, observar los procesos en línea, subir memorial, observar videos de audiencias, tener presente el calendario de audiencias, estados electrónicos, traslados, correspondencia diaria, registro de proyectos de sentencia y de autos, relación de procesos a despacho y consulta de procesos en TYBA.

También brinda el acceso a una variada colección de jurisprudencia, a la ley 1437 interactiva, a sentencias de unificación, control ciudadano, conferencias virtuales, noticias, difusión de jurisprudencias vía WhatsApp y finalmente listas de chequeo que resultan de gran ayuda para los abogados al momento de evitar la inadmisión de las demandas.

Gracias a toda esta serie de esfuerzos antes mencionados de parte del grupo de trabajo de este tribunal, se puede romper ese paradigma de la lejanía del derecho y las tecnologías, esa cultura de las bodegas llenas de papel impreso. Por este merito el grupo Victoria en línea fue premiado por el Consejo de Estado en el concurso "la jurisdicción tiene talento para las TIC" que se realizó en el XVIII encuentro de la Jurisdicción de lo Contencioso Administrativo en la ciudad de Neiva en el año 2012.

No obstante, esta experiencia en el norte del país, requiere de una difusión e implementación en recursos que anualmente se destinan, para la infraestructura y soporte que garantice no únicamente en el acceso a la justicia sino una celeridad y eficiencia; los recursos tecnológicos que el gobierno nacional ha iniciado a implementar en la última década responden a la vanguardia, pero requiere de una mayor articulación con la rama judicial, las magistraturas y los despachos.

Se requiere de una concientización en la optimización de recursos que permitan, que las herramientas tecnológicas que están disponibles en aras de una eficiente administración de justicia, puedan implementarse, esto partiendo de la mentalidad del funcionario judicial en cada despacho y también en la práctica legal de los abogados litigantes.

Conclusión

Primero, se puede afirmar que en materia normativa existe ya bastante legislación en relación a la necesaria utilización de las TIC en la administración de justicia, ya son 22 años desde que se empiezan a realizar planteamientos concretos en este campo, como los vistos en la ley 270 del 96, por otro lado, con el pasar de los años han surgido nuevas herramientas jurídicas afines a los avances tecnológicos más recientes, no obstante, se hace evidente un gran estancamiento no solo a nivel regional si no nacional, cuando se trata de materializar lo establecido por la regulación, se nota una falta de iniciativa tanto de las entidades encargadas del tema como de los empleados y funcionarios judiciales que se muestran reacios al cambio.

Claro está que no se hace posible generalizar, cuando hay precedentes tan importantes en el uso y los beneficios de las TIC como el Tribunal del Magdalena, que sirve de ejemplo hoy en

día, de cuál es la manera correcta en que la rama judicial debe afrontar los cambios que se le vienen en pleno siglo XXI, de como con capacitaciones, trabajo y disposición se puede llegar a un alto nivel de calidad en el servicio, garantizando de esa manera celeridad y eficiencia en el desarrollo de los procesos, per se, generando esa confianza que han ido perdiendo con el paso de los años los ciudadanos de a pie en el sistema judicial gracias a su obsoletísimo, atraso e ineficacia, que como ya se ha dicho en el desarrollo del trabajo se debe a la falta de herramientas tecnológicas del sistema judicial.

Citaciones Bibliográficas

Constitución Política de Colombia, Asamblea Nacional Constituyente, 1991.
Ley 270 de 1996, Congreso de la República de Colombia, 1996
Ley 1437 de 2011, Congreso de la República de Colombia, 2011
Ley 1564 de 2012, Congreso de la República de Colombia, 2011
Tribunal administrativo de Magdalena,
https://www.d1tribunaladministrativodelmagdalena.com/

IMPLEMENTACION DEL NOTARIADO ELECTRÓNICO EN LA REPÚBLICA DE COSTA RICA A LA LUZ DE LA LEY DE CERTIFICADOS, FIRMAS DIGITALES Y DOCUMENTOS ELECTRÓNICOS.

Por: ***Rafael Montenegro P.***
Costa Rica

En Costa Rica, desde el año 2005, se ha vivido una revolución jurídica en relación con las nuevas tecnologías. Es a partir de dicho año que se podría marcar el inicio del reconocimiento jurídico de los documentos electrónicos, de los certificados electrónicos y más aún, el reconocimiento de la firma electrónica.

Gradualmente, para el legislador costarricense, el reconocimiento de la firma electrónica dentro del sistema jurídico nacional ha sido un hito, lo cual ha permito que posterior a ello, se genere normativa especial para las telecomunicaciones, reconocimiento jurídico del derecho a la autodeterminación informativa, y especialmente, implementación de un registro mercantil electrónico y próximamente el ejercicio de la función notarial de forma electrónica.

Es con esto último que surge para el sistema jurídico costarricense el mayor reto, ya que las nuevas tecnologías han permitido el ejercicio de la función notarial de forma más expedita, sencilla y ha brindado a dicha labor seguridad jurídica años atrás debatible. En este sentido, cabe resaltar las sabias palabras de uno de los padres del derecho informático (HO, 2010), cuando manifestó que "Hoy día la sociedad actual se avoca a abandonar el uso de documentos en papel y migra al documento electrónico, en cualquier uso y ámbito. Dentro de poco, la propia realidad exigirá un cambio en las funciones notariales, en el manejo de las escrituras públicas y en la forma de dar fe pública; por ende, también en la forma de registrar documentos públicos".

Con este contexto, es menester conocer un poco del marco normativo que ha afectado al Notario Público en Costa Rica desde el punto de vista de las nuevas tecnologías, el cual a su vez, ha abierto el camino a que la función notarial pueda ir especializándose y más aun actualizándose.

Contexto Normativo Costarricense.

El mayor antecedente electrónico para el Notariado en Costa Rica, se puede encontrar en la Ley de Certificados, Firmas Digitales y Documentos Electrónicos (Ley 8454) del 30 de agosto de 2005 (En adelante identificada como la "Ley de Firma Digital"). Esta normativa, faculta al individuo en general para aplicar la firma electrónica en todo tipo de transacciones de índole privado o de índole público. Esto aplicará entonces para actos gubernamentales como actos de derecho privado, por ello la norma en cita (Investigaciones Jurídicas S.A., 2006) desde su artículo primero expresa:

> "Esta Ley Aplicará a toda clase de transacciones y actos jurídicos, públicos o privados, salvo disposición legal en contrario, o que la naturaleza o los requisitos particulares del acto o negocio concretos resulten incompatibles.
>
> El Estado y todas las entidades públicas quedan expresamente facultados para utilizar los certificados, las firmas digitales y los documentos electrónicos, dentro de sus respectivos ámbitos de competencia"

De esta forma y si se trae a colación lo dispuesto en el artículo primero del Código Notarial de la República de Costa Rica (Ley 7764) del 22 de abril de 1998, el Notariado público según (SANCHEZ SANCHEZ, 2008) "es la función pública ejercida privadamente. Por medio de ella, el funcionario habilitado asesora a las personas sobre la correcta formación legal de su voluntad en los actos o contratos jurídicos y da fe de la existencia de los hechos que ocurran ante él", siendo así las cosas, la Ley de Firma Digital por su naturaleza es de aplicación directa por parte del Notario, entendiendo a este como un funcionario público que ejerce su función de forma privada.

Con solo este primer acercamiento, el Notario costarricense ha tenido un contacto directo con aquellos principios básicos del derecho informático tales como el principio de equivalencia funcional y el principio de neutralidad tecnológica. Aquí, es importante traer a colación lo dispuesto por la Ley Modelo de Firma Electrónica desarrollada por la UNCITRAL, que en lo que respecta al principio de neutralidad tecnológica (Comisión de las Naciones Unidas para el Derecho Comercial Internacional, 2002) ha manifestado que "… no debe haber diferencias de tratamiento entre los mensajes firmados electrónicamente y los documentos de papel con firmas manuscrita, ni entre diversos tipos de mensajes firmados electrónicamente…", de tal forma que "CNUDMI" continua aclaran que "…El principio fundamental de la no discriminación se ha concebido con la finalidad de tener una aplicación general. Sin embargo, cabe señalar que este principio no tiene que afectar la autonomía de la voluntad contractual de las partes…"; adicionalmente, frente al principio de la equivalencia funcional la UNCITRAL, a través de la Ley Modelo de Comercio Electrónico, ha establecido ciertos parámetros que son de basta vigencia y aplicación en la función notarial, de tal forma que (Comision de las Naciones Unidas para el Derecho Comercial Internacional, 1999), expresa que:

> "Así pues, la Ley Modelo sigue un nuevo criterio, denominado a veces "criterio del equivalente funcional", basado en un análisis de los objetivos y funciones del requisito tradicional de la presentación de un escrito consignado sobre papel con miras a determinar la manera de satisfacer sus objetivos y funciones con técnicas del llamado comercio electrónico. Por ejemplo, ese documento de papel cumple funciones como las siguientes: proporcionar un documento legible para todos; asegurar la inalterabilidad de un documento a lo largo del tiempo; permitir la reproducción de un documento a fin de que cada una de las partes disponga de un ejemplar del mismo escrito; permitir la autenticación de los datos consignados suscribiéndolos con una firma; y proporcionar una forma aceptable para la presentación de un escrito ante las autoridades públicas y los tribunales. Cabe señalar que, respecto de todas esas funciones, la documentación consignada por medios electrónicos puede ofrecer un grado de seguridad equivalente al del

> papel y, en la mayoría de los casos, mucha mayor fiabilidad y rapidez, especialmente respecto de la determinación del origen y del contenido de los datos, con tal que se observen ciertos requisitos técnicos y jurídicos"

Al tener claro estos dos grandes preceptos, la Ley de Firma Digital en Costa Rica, desde su artículos dos y durante el desarrollo del texto legislativo, brinda al operador jurídico la opción de aplicar estos principios con el uso de firma electrónica, por ello, el artículo 2 de la Ley de Firma Digital, reconoce en su inciso a) el principio de "Regulación legal mínima" como criterio o base del principio de neutralidad tecnológica y por otra parte en su inciso d) el principio de "Igualdad de tratamiento", con el cual existirá igual de tratamiento legislativo para las tecnologías de generación, proceso y almacenamiento involucradas.

Entrando a profundidad en el texto de la Ley de Firma Digital, se logra encontrar el contenido del artículo 3 y el artículo 9 de la norma en cita, los cuales, para lo que interesa, reconocen la equivalencia funcional de documento y de firmas en la República de Costa Rica y tan certera es la norma que en su redacción realiza una reforma tácita al resto del ordenamiento ya que expresa al final de su redacción que "En cualquier norma del ordenamiento jurídico en la que se haga referencia a un documento o comunicación electrónicos, se entenderán de igual manera tanto los electrónicos como los físicos", esto en el caso de la equivalencia funcional de documentos, pero en relación con la equivalencia funcional de firmas, la misma norma cita en su artículo nueve que "En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita". De esta forma, viendo el contexto de la norma en cita y ubicándonos históricamente hablando, se puede entonces resaltar aquellas palaras de (WORTMAN, 2010), cuando expresó que "Desde el punto de vista de las obligaciones, las nuevas medios informáticos altera el soporte material en el cual se expresa actualmente la voluntad (a veces en parte, a veces en su totalidad) y al hacerlo provoca la necesidad de crear nuevos mecanismos que cumplan la misma finalidad que el soporte de papel".

Más a profundidad, la Ley de Firma Digital, en su artículo 5 es donde prácticamente reconoce la posibilidad de implementar en Costa Rica el Notariado Electrónico. Este artículo, dentro de los actos en que el legislador permite la utilización de documentos, certificados y firmas electrónicas cita de relevancia los siguientes:

- La emisión de certificaciones, constancias y otros documentos.
- La presentación, tramitación e inscripción de documentos en el Registro Nacional.
- La gestión, conservación y utilización, en general, de protocolos notariales, incluso la manifestación del consentimiento y la firma de las partes.

Véase entonces, como expresamente y bajo un principio de legalidad, se habilita al notario público y por ende a la función notarial para que se emitan certificaciones y documentos notariales electrónicos, se presentes y tramites documentos de relevancia registral de forma electrónica y finalmente, se autoriza la gestión, conservación y utilización de protocolos notariales. De estos tres elementos, es importante señalar que:

a) En relación con la habilitación que ha recibido el Notario Público en Costa Rica para emitir certificaciones, constancias y otros documentos, es menester tener claro que

la misma, tiene su fundamento en el artículo 110 del Código Notarial de la República de Costa Rica, en la cual, al Notario se le reconoce la facultad de extender bajo su responsabilidad, certificaciones relativas a inscripciones, expedientes, resoluciones, o documentos existentes ya sea en registros u oficinas públicas, así como de libros, documentos o piezas privadas en poder de particulares. Este tipo de certificaciones podrán realizarse en lo literal, en lo conducente o en relación con. Ahora, si bien es cierto se reconoce desde el año 2005 la potestad certificadora de forma digital al Notario Público, no es hasta el año 2013 que se genera regulación expresa por la Dirección Nacional de Notariado (órgano máximo contralor y fiscalizador de la Función Notarial en Costa Rica), en el cual mediante los Lineamientos Para el Ejercicio y Control del Servicio Notarial, (Acuerdo 2013-006-004 del 13 de marzo de 2013 del Consejo Superior Notarial), en adelante identificados como los "Lineamientos Notariales", se manifestó en su artículo 13 que en relación a las certificaciones:

> "La autorización del notario para extender certificaciones se constriñe al ámbito documental o asientos informáticos, por lo que no es posible la certificación de manifestaciones verbales o acontecimientos observados, pues para ello, la legislación ha reservado el acta notarial.".

Más adelante, los lineamientos en cita (DIRECCIÓN NACIONAL DE NOTARIADO, 2013), mediante su artículo 17, aclaran respecto a las certificaciones de medios electrónicos que:

> "…La impresión de un documento electrónico es admisible como medio mecánico para la expedición de certificaciones. Si el texto de la certificación proviene directamente de una base de datos de un Registro Público y la transcripción del asiento es literal, se permite el uso de guarismos y abreviaciones. En estos casos, la hora y la fecha de expedición deberá coincidir con las de la consulta que sustenta la certificación"

De esta forma, el Notario entra en contacto con los nuevos paradigmas informáticos de los actos legalmente relevantes en la internet, y aquí es donde aplica lo dicho por (WORTMAN, 2010), en cuanto expresó (parafraseando) que los Notarios ante todos estos eventos tecnológicos deben estar involucrados y participar junto con otras disciplinas del quehacer profesional, con el fin de encontrar las soluciones tecnológicas más apropiadas, pudiendo ser estas, las videoconferencias, los chats, los correos electrónicos, plataformas digitales, redes cerradas, redes sociales, bases de datos entre otros, las cuales podrán habilitar al notario para las instrumentalizaciones pertinentes.

Ahora bien, ante semejante avance en la función notarial, como en todo, no hay dicha completa, pues, aunque en el papel y el texto de la Ley, los Notario Públicos en Costa Rica pueden emitir certificaciones electrónicas, según los Lineamientos Notariales, estas certificaciones que en principio son digitales, deberán imprimirse o expedirse en papel de seguridad asignado al Notario Público, satisfacer las especies fiscales y llevar sello blanco y firma del Notario. Ante lo cual, pareciera redundante el hecho que por una parte se permite la emisión de certificaciones electrónicas y por otra parte se exige la materialización de los documentos, pero, como se citó líneas atrás, es aquí

donde aplica el principio de equivalencia funcional y este tipo de documentos serán válidos tanto física como digitalmente.

b) En relación con la presentación, tramitación e inscripción de documentos en el Registro Nacional, la función notarial en Costa Rica ha tenido un avance vertiginoso los últimos cinco años. Hoy en día, el Notario costarricense puede presentar, tramitar e inscribir matrimonios de forma electrónica, puede inscribir sociedades mercantiles (Sociedad Anónima y Sociedad de Responsabilidad Limitada) de forma electrónica y puede legalizar libros societarios de forma electrónica.

c) En relación con la posibilidad de registrar sociedades anónimas o de responsabilidad limitada en formato electrónico, se debe resaltar que actualmente es de aplicación el Reglamento para el Funcionamiento y la Utilización del Portal "Crear Empresa" (Decreto Ejecutivo Número 37593-JP- MINAE-MAG-MEIC-S, del 12 de febrero de 2013), dicho cuerpo normativo en Costa Rica (PODER EJECUTIVO DE LA REPÚBLICA DE COSTA RICA, 2013), a partir de su artículo 14, establece que "Es obligación de los notarios inscribir toda nueva sociedad anónima y de responsabilidad limitada mediante la plataforma CrearEmpresa, siempre y cuando su capital sea pagado en dinero en efectivo o títulos valores", de esta misma forma, el Reglamento en cita hace referencia al formulario electrónico de inscripción, el cual contiene los requisitos de fondo necesarios para el registro adecuado de una sociedad mercantil. A esto, debe agregarse la obligación que tiene el Notario Público a partir del 9 de enero de 2017, en el cual además del formulario de inscripción de una sociedad mercantil, debe incluirse los estatutos en formato PDF y como requisito indispensable, es que dichos estatutos deben estar firmados electrónicamente, con un mecanismo de forma electrónica avanzada bajo plataforma PKI, con el cual, se certifique y se tenga certeza que el documento está firmado electrónicamente por el Notario Público y dicho documento, quedará inscrito o registrado en las bases de datos públicas del Registro Nacional, sección de personas jurídicas.

   Todo este proceso, años atrás, se puede indicar que tardaba alrededor de 2 o 3 semanas, hoy en día, por disposición reglamentaria, el trámite tardará por lo mucho 2 días en realizarse, esto en razón que el Reglamento en cita expresa y directamente manifiesta en su artículo 18 que "Cuando a criterio del registrador, el formulario electrónico cumple a satisfacción los requerimientos establecidos, procederá dentro del plazo máximo de dos días establecido para efectuar la calificación registral, a la inscripción de la nueva sociedad, generándose de forma automática un mensaje a CrearEmpresa con los datos de la nueva entidad.".

d) En relación con el tercer aspecto importante relacionado con la gestión, conservación y utilización, en general, de protocolos notariales, incluso la manifestación del consentimiento y la firma de las partes, es uno de los aspectos de mayor impacto a nivel de la Función Notarial en Costa Rica, esto ya que se deben tener en cuenta lo siguientes elementos:
   1) En relación con la gestión, conservación y utilización de protocolos notariales en formato electrónico, es importante aclarar que la legislación costarricense

reconoce que el Notario debe mantener tres tipos de protocolos dentro del ejercicio de sus funciones:

- **Protocolo propiamente dicho**: Conforme lo dispuesto en el Código Notarial, este protocolo se identifica como el conjunto de libros o volúmenes ordenados de forma numérica y cronológica, en los cuales el notario debe asentar los instrumentos públicos que contengan respectivamente los actos, contratos y hechos jurídicos sometidos a su autorización. Para un mayor entender, el artículo 44 del Código Notarial costarricense expresa que "Todos los notarios, incluidos quienes ejerzan el notariado como funcionarios consulares y los de la Notaría del Estado, usarán un tipo único de protocolo. Los tomos se formarán con doscientas hojas removibles de papel sellado, de treinta líneas cada una. Los folios deberán llevar impresas la palabra protocolo, la serie y la numeración corrida, según la cantidad de hojas; asimismo, serán identificadas con el nombre del Notario, mediante el uso del sello autorizado para tal efecto…". Doctrinalmente hablando, esto es así ya que tal como lo expresa (PEREZ FERNANDEZ DEL CASTILLO, 2001), "Es evidente y notorio que las escrituras públicas y los demás documentos incorporados en registros y archivos de escribanos y notarios tienen doble valor, a saber: el de documentos destinados a conservar la prueba fehaciente de contratos y actos, generalmente de interés material, y el de documentos históricos, elevados a esta categoría casi siempre por efecto del tiempo…", siendo entonces de vital importancia contar con este tipo de protocolos, pero, trayendo a colación lo dispuesto en la Ley de Firma Digital costarricense, pareciera que entonces el legislador, dejó previsto que el Notario pudiese implementar y usar estos protocolos ya no solo de forma material o análoga sino también de forma electrónica.
- **Protocolo o archivo de referencias**: En relación con este tipo de protocolo o archivo, la norma notarial costarricense, en su artículo 47 establece que todos los notarios deberán llevar un archivo de referencias con los documentos y comprobantes referidos en las escritura matrices y que, conforme a la ley, deben quedar en su poder. Estos documentos o comprobantes serán enumerados con foliatura corrida. Obviamente, conforme a la redacción de dicho artículo pareciera que el archivo al que hace referencia, debería de ser en formato material, físico o análogo. No obstante, con la entrada en vigencia de los Lineamientos Notariales, mediante su artículo 21 expresamente autoriza al notario público a mantener su archivo de referencias de forma física o digital. No obstante, en caso que el notario desee tener el archivo en cuestión en formato digital, deberá cumplirse con normativa especial que dicte el Consejo Superior Notarial en Costa Rica. Adicionalmente y como punto de relevancia, los Lineamientos Notariales dejan claro que la conservación, custodia y forma de llevar dicho archivo es responsabilidad exclusiva del notario y como punto relevante relacionado al derecho al olvido, se deja la salvedad que el plazo mínimo de los documentos de referencia deberán mantenerse en custodia por un plazo de diez años contados a partir de la fecha del documento notarial.

- **Copia de instrumentos públicos autorizados**: Este tipo de archivos o protocolos, hacen referencia a la copia de los instrumentos públicos autorizados

por el notario público en Costa Rica. Para tal efecto la norma notarial establece que todo notario deberá conservar en sus archivos una forma firmada por él, de todos los instrumentos públicos que ha autorizado, además, se establece la obligación de hacer constar el número de folios correspondiente a los documentos o comprobantes en el archivos de referencias, si existieren. Ante lo anterior, por lo dispuesto en el artículo 5 de la Ley de Firma Digital, pareciera que en este punto, cuando el legislador hace referencia a la conservación y firma de este protocolo, la misma podría ser de forma electrónica, más aún esto factible cuando se considera lo dispuesto en el artículo 21 antes citado de los Lineamientos Notariales, cuando en lo que interesa cita "Los archivos de referencias y copia de instrumentos públicos podrán ser compilados por el notario, en forma física o digital". Esto abre entonces la posibilidad que estas copias puedan mantener en formato digital y cuando la norma notarial hace referencia al término "firma", podríamos entonces entender que se refiere tanto a firma análoga como a firma electrónica, esto en concordancia con el artículo 9 de la Ley de Firma Digital.

De todo lo expuesto, sale a relucir un concepto notarial relevante, y este es que, el uso de protocolos busca proyectar cronológica e históricamente un documento notarial determinado. Pareciera que esto es un elemento de forma que ha sido garantizado por el formato físico del protocolo notarial, pero, acudiendo al texto de la Ley de Firma Digital costarricense, ésta en su artículo 6 viene a establecer los principios básicos de la seguridad información, los cuales, vendrían a dar seguridad jurídica a los protocolos notariales en su forma digital, ya que garantizarían tres grandes elementos, la inalterabilidad del documento, su accesibilidad futura y su preservación histórica. Para ello la norma en cita expresa:

"Cuando legalmente se requiera que un documento sea conservado para futura referencia, se podrá optar por hacerlo en soporte electrónico, siempre que se apliquen las medidas de seguridad necesarias para garantizar su inalterabilidad, se posibilite su acceso o consulta posterior y se preserve, además, la información relativa a su origen y otras características básicas…"

De lo expuesto, técnicamente hablando, se garantizaría de esta forma que el protocolo digital cumpla las mismas funciones del protocolo análogo, de hecho, este se convierte en el mejor ejemplo de aplicación del principio de equivalencia funcional. En este punto, la doctrina notarial ha sido clara en el tanto el maestro (PEREZ FERNANDEZ DEL CASTILLO, 2001) ha dejado claro que:

"…se estima que el notario debe abocarse, con amplios signos de apertura, a las nuevas exigencias sociales, técnicas y económicas del mundo contemporáneo, reconsiderando su trascendencia en el ámbito del derecho, en sus múltiples manifestaciones, particularmente en el campo del derecho comparado, internacional privado, administrativo y fiscal. Al servicio de esta idea recomienda a los notarios adheridos promover permanentemente los servicios de información que mantengan a sus integrantes actualizados respecto de todos lo

relacionado con su actividad, utilizando para ellos los medios técnicos más modernos…"

Por su parte, es importante señalar la posición de (NICOLAS GATTARI, 2011), en la cual concluye después de una exquisita disertación sobre el documento electrónico y el documento protocolar que "la grafía electrónica puede cumplir suficientemente los requisitos de visibilidad, expresividad y recognoscibilidad del texto y de su autor, incluso en el momento de destinatario. La corporalidad del documento electrónico se halla perfectamente cumplida en su soporte y en su grafía con su característica común electrónica que significa un avance en la comunicación y, por ende, en el derecho y en la sociedad".

2) En relación con la manifestación del consentimiento y la firma de las partes, es donde tal vez técnicamente hablando puede darse mayor inconveniente. Para ello deben analizarse algunos de los siguientes aspectos:

- Para los efectos del notario costarricense, las firmas, según el Código Notarial, deberán consignarse en forma seguida, sin ningún espacio entre el fin de la escritura y el inicio de las firmas. La norma aclara en su artículo 93 que primero serán las firmas de los comparecientes, luego la de los testigos, en su caso, y al final se pondrá la firma del notario autorizante. Para el legislador y el sistema legal notarial de Costa Rica, la firma de las partes es un elemento fundamental del acto notarial, en este sentido los tribunales costarricenses en tal sentido han expresado que "Según la doctrina, la firma, es la representación gráfica del nombre y apellido de una persona, hecha de su puño y letra, del modo que acostumbra y normalmente al pie del instrumento; acredita la prestación del consentimiento. Con ella el notario acredita la veracidad del texto, la legalidad del instrumento, responsabilizándose por cumplir requisitos normativos, además de asegurar la calificación de los actos y legitimar intervenciones…"
- [1], teniendo claro, esto, la jurisprudencia también ha considerado que la firma debe realizase en un mismo acto según el principio de unidad del acto y debe existir inmediación o presencia del Notario autorizante al momento de la firma, esto ya que la autorización del notario deberá contener el lugar, la hora el día, el mes y año en que se autoriza la escritura y además deberá contener las firmas de quienes intervienen en ella, siendo que primero firman los comparecientes, luego los testigos y por último el notario autorizante[2].
- Con base a lo expuesto, pareciera entonces que el elemento presencial es un elemento fundamental para el ejercicio de la función notarial, pues esto, es lo que permite al notario dar fe de los otorgantes y firmantes y es lo que configura de forma expresa y eficaz la manifestación de voluntad de las partes. Empero, para efectos de tecnificar este elemento de la función notarial, se puede traer a colación lo dispuesto en el artículo 8 y 9 de la Ley de Firma Digital costarricense en el sentido que:

[1] Tribunal de Notariado, voto número 148 de las 10:50 horas del 14 de agosto de 2003.
[2] Tribunal de Notariado, voto número 69 de las 9:45 horas del 23 de marzo de 2006. Tribunal de Notariado, voto número 240 de las 9:30 horas del 20 de octubre de 2006.

"**Artículo 8.- Alcance del concepto.** Entiéndase por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar de forma univoca y vincular jurídicamente al autor con el documento electrónico.

Una firma digital se considerará certificada cuando es emitida al amparo de un certificado digital vigente, expedido por un certificador registrado."

"**Articulo 9.- Valor equivalente**. Los documentos y las comunicaciones suscritos mediante firma digital, tendrán el mismo valor y eficacia probatoria que su equivalente firmado en manuscrito. En cualquier norma jurídica que se exija la presencia de una firma, se reconocerá de igual manera tanto la digital como la manuscrita.

Los documentos públicos electrónicos deberán llevar la firma digital certificada".

Siendo entonces que la Ley de Firma Digital costarricense es una norma especial y de fecha posterior al Código Notarial costarricense, pareciera que es posible entender que cuando el Código Notarial habla de las firmas de las partes en los instrumentos públicos, se hace referencia a la firma manuscrita y a la firma electrónica, que para los efectos de los documentos públicos (como en efecto lo es un documento protocolar), la firma electrónica deberá ser certificada. Siguiendo este análisis, en el caso que se implementara el protocolo electrónico notarial, las partes podrían firmar el documento usando firma electrónica avanzada certificada por un agente certificador inscrito en la República de Costa Rica y se podría aplicar el mismo principio antes citado para las certificaciones de documentos electrónicos, en el sentido que la hora y fecha de firma de las partes deberá coincidir con la fecha y hora del otorgamiento. Además, técnicamente hablando, para este escenario, sí sería necesario que el Notario en Costa Rica, cuente con una plataforma electrónica en la cual las partes puedan acceder y el sistema mediante el mecanismo PKI pueda certificar la presencia de las partes y así el notario cumple con los parámetros de inmediación y unidad del acto, ya que tal y como lo cita (MOLES PLAZA, 2004) "Así para que la red otorga el don de la ubicuidad: el administrado puede estar a la vez en el espacio <<real>> y en uno o varios espacios de Internet. Esto significa que un sujeto puede disponer al mismo tiempo, de una identidad en el espacio real y de varias identidades distintas en internet…".

3) Finalmente, pero no menos importante, el legislador, al brindar la posibilidad de otorgar y autorizar documentos públicos por medios electrónicos, se enfrenta a ciertas formalidades establecidas por otros cuerpos normativos de vieja data. Situación que debe actualizar y estandarizar conforme a los nuevos parámetros. Verbigracia de ello, se encuentra los actos relativos a las disposiciones de última voluntad. Este tipo de actos, de conformidad con el artículo 5 de la Ley de Firma Digital, no pueden ser otorgados mediante documentos electrónicos, mayoritariamente por un tema formal del artículo 583 del Código Civil, el cual establece que el testamento puede otorgarse ante un cartulario, mediante escritura pública. Lo que exige la materialización de esta manifestación de última voluntad. Sin embargo, volviendo al acápite anterior, si se logra generar una plataforma

electrónica, se usa una firma electrónica certificada y se logra cumplir los parámetros de ciberseguridad antes citados, técnicamente no existiría inconveniente en otorgar un testamento mediante escritura pública electrónica. No obstante, este un tema técnico económico que a futuro habrá que trabajarse.

Aunado a lo anterior y para reforzar la idea del otorgamiento de escrituras públicas por medios electrónicos, es importante tener en mente lo dispuesto en el artículo 10 de la Ley de Firma Digital, en el cual se establece la presunción de autoría de los documentos electrónicos firmamos electrónicamente, o en otras palabras se establece el principio de no repudio en el envío, pues dicho artículo expresamente manifiesta que:

> "Todo documento, mensaje electrónico o archivo digital asociado a una firma digital certificada se presumirá, salvo prueba en contrario, de la autoría y responsabilidad del titular del correspondiente certificado digital, vigente en el momento de su emisión.
>
> No obstante, esta presunción no dispensa el cumplimiento de las formalidades adicionales de autenticación, certificación o registro que, desde el punto de vista jurídico, exija la ley para un acto o negocio determinado."

Adicionalmente, (NICOLAS GATTARI, 2011), ha manifestado en relación con el concepto y aplicación de la firma análoga y la firma digital que las seis pautas de la firma análoga que son equiparables a la firma electrónica son:

> "a) la firma manual convierte en documento al proyecto de escrito; b) ese documento tiene contenido íntegro; c) se atribuye a un sujeto como tal y la certeza de ser tal sujeto; d) como hacedor del documento, aunque bien pudo prepararlo otro; e) el firmante asume su contenido, aprueba el negocio y las expresiones formales; f) la firma es manuscrita, esto es, corporal, índice de ciertos caracteres de un sujeto en las letras que se puede estudiar por medio de la grafología. Estas ideas también se aplican, sobre todo, a la firma digital porque ella documento el proyecto electrónico, prueba su integridad, autoría individualización, imputación y caracteres identificantes, más la inalterabilidad o no repudio y otros que se verán luego, es decir, supera las pautas de la firma cartácea…"

Teniendo claros y conocidos los alcances y efectos de la Ley 8454 dentro de la función notarial en Costa Rica, es importante indicar que actualmente, en corriente de la Asamblea Legislativa de la República de Costa Rica, existe un proyecto de Ley, cuyo objeto es actualizar la función notarial e incluir el uso de protocolos electrónicos y firmas electrónicas en los actos de relevancia jurídica y notarial del país. Proyecto de Ley que cabe analizar a groso modo a continuación.

Proyecto de Ley de Reforma al Código Notarial de la República de Costa Rica.

En corriente legislativa, se encuentra en estudio el proyecto de ley número 20,079 denominado "Reforma Integral a la Ley No. 7764 de 22 de mayo de 1998. Código Notarial", en adelante identificado como el "Proyecto de Ley". Este proyecto consigo trae elementos innovadores y relacionados con lo ya dispuesto por la Ley de Firma Digital en la República de Costa Rica. A continuación se presentarán algunos aspectos relevantes del proyecto, sin

embargo, cabe aclarar que el estudio del mismo podría abarcar todo un artículo académico posterior.

Dentro de los elementos que se incorporan con el Proyecto de Ley, se logran resaltar los siguientes:

1) Se reconoce el principio de progresividad tecnológica dentro de la función notarial: El artículo 3 del Proyecto de Ley viene aclarando que además de la obligatoria aplicación de la Ley de Firma Digital, todos los entes y órganos del Estado, encargados de regular, resguardar, proteger y sancionar la actividad notarial, estarán bajo la obligación de adoptar, adaptar y promocionar todos los medios tecnológicos que faciliten la función notarial, esto con el fin de que el sistema aproveche los avances tecnológicos y los medios o formatos para la gestión de la actividad notarial.
2) Se incluye una nueva definición de protocolo, de tal forma que el artículo 46 del Proyecto de Ley lo define como protocolo físico o protocolo digital, pudiendo el notario únicamente tener uno de estos autorizado. El texto del proyecto es:

   > "Protocolo físico es el conjunto de libros o volúmenes ordenados en forma numérica y cronológica, en los cuales el notario debe asentar los instrumentos públicos que contengan respectivamente los actos, contratos y hechos jurídicos sometidos a su autorización. Tendrá el número de folios y el tamaño de papel que determine el Consejo Superior Notarial.
   >
   > El protocolo digital es repositorio electrónico del Estado, utilizando a través de un Sistema Notarial Digital que permite a los notarios, mediante el uso de mecanismos de autenticación seguros como por ejemplo la firma digital certificada, llevar el respectivo registro de los instrumentos públicos que contengan los actos, contratos, hechos jurídicos sometidos a su autorización, así como el consentimiento y firma de las partes.
   >
   > El notario podrá optar únicamente por uno de los dos sistemas, no está permitido el uso del protocolo digital y físico de forma simultánea. Sin embargo, la notaria y el notario pueden solicitar el traslado de uno u otro sistema, previa solicitud a la Dirección Nacional de Notariado, quien reglamentará la forma de realizar el cambio.".

3) En relación con los tipos de protocolo autorizados para los notarios, se establece el notario físico que tendrá 200 hojas removibles y como parte novedosa, se incluye el protocolo en formato digital, el cual según el artículo 47 del Proyecto de Ley, "es único y se utiliza mediante la plataforma digital denominada Sistema Notarial Digital, ofrecida a los notarios mediante productos o servicios que serán definidos, regulados y autorizados por la Dirección Nacional de Notariado y se inicia con la autorización extendida por este mismo órgano."
4) Se establece la creación de los Sistema Notariales Digitales. Estos sistemas, de conformidad con el artículo 48 del Proyecto de Ley, serán plataformas electrónicas de uso exclusivo para notarios públicos mediante el cual podrán gestionar los actos, contratos y hechos jurídicos sometidos a la autorización en el protocolo digital del Estado.
5) En relación con los archivos de referencias y las copias de instrumentos públicos, el Proyecto de Ley ya establece la posibilidad que estos sean llevados, custodiados y almacenados en formato electrónico.

6) Conforme al artículo 84 del Proyecto de Ley, los protocolos digitales podrán ser firmados por las partes con el uso de firma digital certificada o podrán usar mecanismos biométricos de autenticación y firma seguros que sean previamente aprobados por el Consejo Superior Notarial.
7) En relación con la potestad certificadora del Notario Público, éste podrá certificar documentos por medios electrónicos, y deberá contar con la fecha del mismo momento de la consulta cuya información se está certificando. Además, podrá certificarse documentos de bases de datos de registros, universidades o instituciones de otros países siempre y cuando surta efectos en Costa Rica.
8) El notario en su potestad autenticadora podrá autenticar firmas, huellas dactilares u otros mecanismos biométricos autorizados por la Dirección Nacional de Notariado, siempre que hayan sido impresas en su presencia, para ello, deberá hacer constar que son auténticas.
9) De los procesos no contenciosos de conocimiento en sede notarial, no se hace referencia a la posibilidad que el Notario pueda gestionar, almacenar y mantener expedientes en formato digital.

Con esto, se logra observar que en Costa Rica, se está trabajando en la actualización de la función notarial con fundamento en las nuevas tecnologías, lo que se tiene hasta ahora es la vigencia de la Ley 8454, pero ya se encuentra en camino una reforma al Código Notarial, para efectos de contar con mayor tecnología a favor del servicio de la función notarial en Costa Rica. Ahora más que nunca, es necesario que el Notario en Costa Rica, se actualice, esté presto y atento a las nuevas tecnologías y de la mano del derecho informático, la informática jurídica documental y de gestión, se dé el paso que permita contar con un notariado electrónico en Costa Rica y más aún se abra la brecha para el notariado electrónico en la región centroamericana.

CONCLUSIONES.

De conformidad con lo identificado, se logra concluir que:

1. Con la entrada en vigencia y aplicación de la Ley 8454 en la República de Costa Rica, se ha dado apertura a la implementación de documentos electrónicos, certificados electrónicos, firmas electrónicas y protocolos electrónicos dentro de la función notarial.

2. El Notario, con el paso del tiempo, ha visto la necesidad de actualizar y homologar sus conocimientos de conformidad con la sociedad de la información.

3. Normativamente hablando, Costa Rica cuenta con el amparo legislativo para proceder a implementar y generalizar el uso de protocolos electrónicos y uso de firma electrónica avanzada como mecanismo de manifestación de voluntad en sede notarial.

4. En Costa Rica, el proyecto de Ley 20079 es una referencia precisa de cómo y bajo qué condiciones podrá implementarse las nuevas tecnologías dentro de la función notarial en la República de Costa Rica.

5. El permitir y reconocer el uso de nuevas tecnologías dentro de la función notarial en Costa Rica, puede agilizar, brindar mayor seguridad jurídica y facilitar el acceso de la población civil y del Notario Público a servicios más eficaces y a la prestación de la función pública del notariado de forma más expedita.

BIBLIOGRAFÍA.

- **ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA.** Reforma Integral a la Ley 7764 de 22 de mayo de 1998, Código Notarial. Proyecto de Ley 20079. *Asamblea Legislativa de la República de Costa Rica.* [En línea] http://www.asamblea.go.cr/Centro_de_Informacion/Consultas_SIL/Pginas/Detalle%20Proyectos%20de%20Ley.aspx?Numero_Proyecto=20079.

- **Comision de las Naciones Unidas para el Derecho Comercial Internacional. 1999.** CNUDMI. *Ley Modelo de la CNUDMI sobre comercio electrónico con la guía para su incorporación al derecho interno 1996.* . [En línea] 1999. [Citado el: 25 de Julio de 2018.] https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf.

- **Comisión de las Naciones Unidas para el Derecho Comercial Internacional. 2002.** Ley Modelo de la CNUDMI sobre firmas electrónicas con la guía para su incorporación al derecho interno. *CNUDMI.* [En línea] 2002. [Citado el: 18 de Julio de 2018.] http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf.

- **DIRECCIÓN NACIONAL DE NOTARIADO. 2013.** DIRECCIÓN NACIONAL DE NOTARIADO. *DIRECCIÓN NACIONAL DE NOTARIADO.* [En línea] 13 de Marzo de 2013. [Citado el: 26 de Julio de 2018.] http://www.dnn.go.cr/normativa/lineamientos/001-Lineamientos.pdf.

- **HO, Augusto. 2010.** Notariado electrónico en Panamá; Una necesidad inminente. [aut. libro] Federación Iberoamericana de Asociaciones de Derecho Informático. *Memoras XIV Congreso Iberoamericano de Derecho e Informática.* Monterrey : s.n., 2010, pág. 350.

- **Investigaciones Jurídicas S.A. 2006.** *Ley de certificados, firmas digitales y documentos electrónicos, y su reglamento.* Segunda Edición. . San José : Editorial Investigaciones Jurídicas S.A., 2006.

- **MOLES PLAZA, Ramon . 2004.** *Derecho y Control en Internet.* Primera Edición. Barcelona : Ariel Derecho, 2004.

- **NICOLAS GATTARI, Carlos. 2011.** *Manual de Derecho Notarial.* Segunda Edición. Buenos Aires : AbeledoPerrot, 2011.

- **PEREZ FERNANDEZ DEL CASTILLO, Bernardo. 2001.** *Doctrina Notarial Internacional.* Segunda Edición. . México : Editorial Porrúa. Av. República Argentina, 15, 2001.

- **PODER EJECUTIVO DE LA REPÚBLICA DE COSTA RICA. 2013.** CREAREMPRESA.GO.CR. *CREAREMPRESA.GO.CR.* [En línea] 12 de Febrero de 2013. [Citado el: 2018 de Julio de 27.] https://crearempresa.go.cr/cfmx/plantillas/gobDigital/Reglamento%20CrearEmpresa.pdf.

- **SANCHEZ SANCHEZ, Rafael. 2008.** *Código Notarial con legislación conexa.* [ed.] Editorial Juritexto S.A. Segunda Edición. . San José : Editorial Juritexto S.A., 2008.

- **WORTMAN, Javier. 2010.** Función Notarial. En el Ciberespacio ¿Seguridad jurídica vs. Seguridad informática? [aut. libro] Federación Iberoamericana de Asociaciones de Derecho Informático. *Memorias XIV Congreso Iberoamericano de Derecho e Informática.* Monterrey : FIADI, 2010.

"DERECHO DE LOS CONSUMIDORES, FRENTE AL COMERCIO ELECTRÓNICO"

Por: ***Silvina Vergara Aranda***
Uruguay

[1]Existen áreas de la contratación electrónica respecto del consumidor que, debido al ambiente tecnológico en que la relación se desenvuelve, plantean una problemática y requieren un tratamiento especial. Entre esas áreas encontramos la publicidad, cuestiones propias de la contratación electrónica (régimen jurídico que gobierna el contrato, fijación del momento y lugar de celebración del contrato, determinación de la expresión del consentimiento del consumidor, legislación aplicable), cuestiones de privacidad, autenticación y seguridad, educación del consumidor, sistemas seguros de pago, transparencia de términos y condiciones contractuales.

Cuando el usuario de Internet decide adquirir bienes o servicios a través de la red se encuentra en una situación de desequilibrio en relación con la empresa proveedora de los bienes o servicios que los ofrece mediante su sitio web. La contratación es totalmente despersonalizada, corre riesgos de ser una potencial víctima de abusos de la oferta, del marketing y de las condiciones contractuales. EL ciberconsumidor es la parte más vulnerable y la que debe ser tutelada, como tal en la relación de consumo. Esta protección se verifica a través de normas de orden público, que limitan la autonomía de la voluntad y por tanto no pueden ser modificadas por las partes, en este caso proveedor o consumidor. Este tipo de tutela responde a una realidad fáctica que ubica al consumidor en la parte más débil de la relación económica. Ésta defensa del consumidor plasma el principio del favor debilii, correspondiente a la parte más débil del contrato. Este consumidor inserto en una plataforma virtual que lo transforma en un consumidor tecnológico, mayormente vulnerable que en las transacciones tradicionales.

¿De dónde deben provenir las medidas aplicables a la protección de los consumidores?

Podemos identificar tres mecanismos:

1- Los hemisféricos
2- Los regionales
3- Las legislaciones nacionales

Puntos importantes a la hora de legislar en relación a los consumidores y al Comercio Electrónico:

- Legalidad y formalidad de las transacciones realizadas. Estandarización en temas como contratos electrónicos y telemáticos, formalidades mínimas para garantizar la validez de una transacción.

[1]*ASPIS, Analía,* Comercio Electrónico "Régimen Contractual", Errepar, Bs As Argentina.

- Jurisdicción y Legislación. EL consumidor en internet se topa con una multiplicidad de normas y leyes que los desestimulan. Se debe tender una legislación uniforme con estándares mínimos que aseguren una visión armónica a al menos uniforme a nivel internacional, que aliente al consumidor a hacer uso del Comercio Electrónico, independientemente de su ubicación geográfica o jurisdiccional.
- Solución de controversias. Se debe realizar un trabajo de consenso entre Gobierno, proveedores y consumidores, para asegurar que la resolución de conflictos funcione de modo efectivo. Se requiere incentivar un marco de solución de controversias internacional que permita aplicar normas básicas universalmente reconocidas, de modo práctico. La practicidad requiere que no resulte más complejo o costoso el trámite administrativo del reclamo o proceso de mediación que el objeto del mismo.
- En protección al consumidor, se debe dejar a la autorregulación, de preferencia los aspectos de competencia, entre proveedores a fin de estimularlos.
- Promover sistemas de identificación inequívoca de personas y empresas en medios electrónicos. Es decir, trabajar en sistemas de Certificación Electrónica de sitios y usuarios.

Diversas respuestas jurídicas de protección

Ley de Relaciones de Consumo 17250 11/08/2000, Uruguay. Defensa de los Consumidores. Contratación Electrónica.

a- Contratos celebrados fuera de los locales comerciales: Artículo 16 “La oferta de productos o servicios que se realice fuera del local empresarial, por medio postal, telefónico, televisivo, informático o similar da derecho al consumidor que la aceptó a rescindir o resolver “ipso jure” el contrato. El consumidor podrá ejercer tal derecho dentro de los 5 días hábiles contados desde la formalización del contrato o de la entrega del producto, a su sola opción sin responsabilidad alguna de su parte”.

b- Cláusulas abusivas en los contratos de adhesión: Artículo 31 “ Son consideradas cláusulas abusivas, sin perjuicio de otras, las siguientes –a Las que exoneren o limiten la responsabilidad del proveedor. –b Las que impliquen renuncias del derecho del consumidor. c- Cláusula resolutoria pactada exclusivamente en favor del proveedor. –d Las cláusulas que impliquen renuncias al consumidor a ser resarcido o reembolsado. –e Las cláusulas que establezcan que el silencio del consumidor implica aceptación.

c- Información sobre los productos y servicios, importancia de la contratación a distancia. Es uno de los aspectos esenciales en las relaciones de consumo, el deber de informar, como también actuar de buena fe, siendo una obligación esencial del proveedor del producto o servicio: Artículo 6 “ La información suficiente, clara, veraz, en idioma español. La protección contra la publicidad engañosa, los métodos coercitivos o desleales en el suministro de productos o de servicios y las cláusulas abusivas en los contratos de adhesión.”

Artículo 12: “La oferta dirigida a consumidores determinados e indeterminados, trasmitida por cualquier medio de comunicación y que contenga información suficiente precisa en relación a los productos o servicios vincula a quien la emite y a aquel que la utiliza.”

Artículo 13: La oferta de productos deberá brindar información clara y fácilmente legible sobre sus características."
Artículo 20: "En la oferta de servicios el proveedor deberá informar….".

d- Garantías de los productos y servicios: Artículo 23" El proveedor de productos o servicios deberá ofrecerla por escrito, estandarizada cuando sea para productos idénticos. Ella deberá ser fácilmente comprensible y legible y deberá informar al consumidor sobre el alcance de sus aspectos más significativos."
e- Responsabilidad civil: Artículo 32 "La violación por parte del proveedor de la obligación de actuar de buena fe o la transgresión del deber de informar en la etapa precontractual de perfeccionamiento o de ejecución del contrato, da derecho al consumidor a optar por la reparación, la resolución o el cumplimiento del contrato, en todos los casos más los daños y perjuicios que correspondan."
Artículo 34" Si el vicio o riesgo de la cosa o de las prestación del servicio resulta un daño al consumidor, será responsable el proveedor de conformidad con el régimen previsto en el Código Civil".
f- Aspectos generales:

¿Cómo alcanzar un equilibrio entre los derechos de los consumidores y las operaciones comerciales electrónicas?

Por un lado los consumidores aspiran a recibir sus productos libres de defectos, de calidad satisfactoria de acuerdo al precio, durables y que no representen un peligro usados normalmente. En cuanto a servicios respecta, se puede esperar que sea prestado con los debidos cuidados y diligencia, dentro de un tiempo razonable y a un precio también razonable. Estos aspectos pueden ser regulados en la protección a las ventas a distancia, protección contra abusos en el uso de los datos, o contra malos usos de los sistemas informáticos. Es imprescindible que las legislaciones regulatorias tengan en cuenta el aspecto transfronterizo de estas relaciones, y que la aplicación de dichas soluciones sea similar. El problema se acentúa debido a la incompatibilidad de enfoques regulatorios de los EEUU y la Unión Europea, siendo estos los actores principales en el tema, de referencia para los restantes países.

[2]El sistema autorregulatorio de EEUU

El gobierno de los Estados Unidos ha mantenido en reiteradas oportunidades que los gobiernos deben evitar restricciones innecesarias al comercio electrónico, que cuando la intervención del gobierno es necesaria, su objetivo debe ser una intervención mínima, para generar el ambiente necesario. Las empresas deben establecer reglas y mecanismos necesarios, ocupando así la regulación legal y estatal. Esto mirando siempre las características de internet y de un comercio electrónico a escala global, siendo el consumidor el que debe proteger sus propios intereses. En una primera instancia parecería que el consumidor se vería desprotegido desde este punto de vista, pero por el contrario la autorregulación sería la forma de lograr la armonía en el comercio electrónico y los consumidores.

[2] Manual de Derecho de Consumo. Madrid. REUS 2016.

La Unión Europea y la uniformidad legislativa

El objetivo de la Unión Europea es la armonía legislativa y no la uniformidad en la protección de los derechos de los consumidores, lo que significa que en ciertos estados los consumidores gozan de una protección más grande y profunda que en otros. El modelo legislativo armonizador tiene su origen en los principios básicos establecidos en el Tratado de Roma, que hacen referencia a la protección de los consumidores y a la libre circulación de los factores. Esto último se explica en la creencia, reafirmada por la Corte Europea de Justicia, que distintos niveles de protección a los consumidores en distintos estados miembros atentaría contra la libre circulación de bienes y servicios entre los miembros de la Unión. Esta postura sigue siendo sostenida por las autoridades de la Unión, que últimamente han tomado ciertas medidas tendientes a aumentar los niveles de protección a los consumidores y la cooperación en la administración de tales de tales derechos. Uno de los problemas en los que diferencias en el nivel de protección acarrearía discriminación a negocios electrónicos de otros estados miembros.

[3]Nuevo Reglamento de Protección de Datos de la Unión Europea 25/05/2018

En general, el RGPD no recoge una nueva reorganización de la política de protección de datos ya conocidos. Sino que los ya conocidos seguirán vigentes. Estos son:

- Prohibición salvo autorización: este principio significa que a priori se prohíbe cualquier procesamiento de datos personales a no ser que esté permitido. Aplicándose a cualquier dato personal.
- Limitación de la finalidad: las empresas solo podrán recopilar y editar datos con fines específicos. Para ello deben formularse los objetivos y documentarse el uso futuro de los datos. Ej. una empresa recaba datos con fines laborales no puede utilizarlos con fines publicitarios.
- Minimización de datos: exige que las empresas recopilen la menor cantidad de datos posibles, "lo menos posible y tanto como sea necesario".
- Transparencia: el tratamiento de los datos debe ser comprensible para los interesados. Esto por un lado requiere avisos de privacidad claros y por otro significa mayores derechos para los usuarios.
- Confidencialidad: Las empresas tienen la obligación de proteger los datos personales de sus clientes de forma técnica y organizativa ya sea del tratamiento o modificación no autorizados, del robo o la destrucción de dichos datos, es necesario aplicar medidas técnicas de protección.

Nueva normativa a la que se tienen que atener las empresas, sobre todo las que forman parte del comercio online.

[3] " Nuevo Reglamento de Protección de Datos de la Unión Europea" 25/05/2018 Digital Guide 1&1 web www.1and1.es

Seguridad general de los datos en la empresa

- Evaluación del impacto de la protección de los datos: Las empresas tienen la obligación de llevar a cabo evaluaciones de riesgos y también de definir las medidas de protección adoptadas para minimizarlos.
- Datos de los trabajadores: Como las empresas procesan los datos de los trabajadores.
- Delegados de protección de datos: estos delegados supervisan la estrategia de protección de datos elaborada y el cumplimiento del RGPD, dado que una empresa con más de 10 trabajadores dedicados al procesamiento de datos personales debe recurrir a un delegado de protección de datos.
- Obligaciones de notificación: Cuando se tenga en cuenta incidentes de seguridad, estos deben notificarse en un plazo de 72 horas a los interesados y a las autoridades responsables.

Seguridad de los datos personales

- Obligaciones de documentación
- Privacy by design: Las empresas deben tener en cuenta la privacidad desde el diseño técnico de sus empresas comerciales. La regla es el menor tratamiento de datos posible.
- Privacy by default (privacidad por defecto: que debe predefinirse técnicamente la variante que mejor garantice la protección de datos, lo que evita que los consumidores lidien con ajustes técnicos complejos para conseguir limitaciones en el procesamiento de datos.

El derecho a la portabilidad de los datos; Es un nuevo derecho que permite al interesado obtener los datos que haya facilitado a un responsable de tratamiento y concernientes a su persona, en un formato estructurado, de uso común, de lectura mecánica e interoperable. También permite transmitirlos a un nuevo responsable de tratamiento sin que el anterior responsable se pueda oponer.

<u>El deber de informar, alcance en la Ley de Relaciones de Consumo</u>

[4]La ley de Relaciones de Consumo tiene un fin protector, por lo que la inclusión del deber de informar es a los efectos de proteger a los consumidores. ¿Cuál es la información que se debe suministrar? Implica por parte del proveedor de servicio o producto poner en conocimiento del consumidor no cualquier cantidad de tipo de datos, sino aquellos suficientes y adecuados para evitarle un daño. De allí que constituye una manifestación específica del deber de informar, que tiene carácter instrumental respecto de la obligación de seguridad. La obligación del proveedor de advertir al consumidor no está limitada a los supuestos de comercialización de cosas o servicios riesgosos, es exigible con independencia de cuál sea la naturaleza o cualidades del producto o servicio prestado, es decir, aunque se trate de cosas y servicios que puedan catalogarse como no riesgosos en sí mismos. No se agota con la

[4] *TEVEZ N.* Alejandra "El deber de advertencia en las Relaciones de Consumo" LA LEY Año LXXIXX N° 81 Buenos Aires, Argentina.

comercialización del producto, sino que subsiste después. Entiendo que para el proveedor, cualquier vicio en el producto o servicio tiene un costo económico, por lo que va a buscar minimizar el costo en la producción económica. Teniendo en cuenta además que el proveedor, es el único conocedor del proceso y estado en cual se encuentra el producto y servicio, esto lo pone en un lugar de desigualdad frente al consumidor. Cuando la ley establece [5]"información clara y suficiente" impone al proveedor un hacer objetivo y determinado jurídicamente, por lo que hace que el proveedor ante la falta de cumplimiento de esta obligación responda por una responsabilidad objetiva. Además la ley prevé que dicha información no sea engañosa, que induzca al consumidor a error. Como consecuencia de ello el proveedor estaría limitando la libertad del consumidor de elegir libremente entre otros productos o servicios.

Conclusión

El derecho de los consumidores, en especial en el ciberespacio, se suma a la complejidad que representan las Relaciones de Consumo. Teniendo en cuenta los diferentes puntos analizados en el comportamiento de los proveedores, desde el deber de informar en forma clara y veraz, así como la especial atención a las operaciones electrónicas. El nuevo Reglamento Europeo de Protección de Datos muestra avances en la temática, confirmando la necesidad de nuevas formas de protección en el uso de datos personales, la solicitud y la administración de los mismos en los diferentes sitios Web, así como un régimen de administradores de los diferentes sitios que son utilizados por empresas, entidades que manejan datos personales. Esto parte del diseño previo y planificado en la obtención de los mismos.

Por otro lado encontramos leyes que regulan las relaciones de consumo, siendo extensible a las operaciones electrónicas, pero sigue habiendo un debe por parte del Estado, en cuanto a una justicia accesible y expedita para los consumidores. En Uruguay existe la ley de las pequeñas causas de Relaciones de Consumo con un monto reclamable, que tiene un tope de poca cuantía, la misma en la práctica es poco operativa, por ejemplo, su utilización no se ha diversificado en términos reales a todo el país, sí lo ha hecho en términos formales con la distribución de competencia judicial, muchos operadores judiciales encuentran confusa su aplicación y desconocen la instrumentación de la misma. Por ello el consumidor, se ve envuelto en procesos judiciales, cuando todo ello podría haberse evitado con un comportamiento adecuando por parte de los proveedores. Todo ello cuando pensamos en el territorio nacional. Por lo que sabemos en el ciberespacio no tenemos tiempo ni lugar, por lo que las operaciones electrónicas necesitan consideradas desde otro ámbito, para tutelar los intereses de las partes. Por lo que entiendo fundamental el compromiso por parte de los Estados de aunar criterios y establecer pautas y reglamentos comunes, así como lo es el Reglamento de Protección de Datos Personales de la Unión Europea así como también la solución de EEUU, a través de un régimen autorregulatorio. Y por último y no menos importante, encontrar el derecho a la paz en las diferentes relaciones de consumo en el ciberespacio, permitiendo el desarrollo de los pueblos y la solidaridad entre los mismos.

[5] Ley de Relaciones de Consumo 17250, Año 2000, Uruguay.

Anexos

Comentario de Sentencia Definitiva Nro. 49/2017 Juzgado de Paz Departamental, Atlántida, Uruguay.

En la referida sentencia, la actora suscribió con la demandada contrato de arrendamiento de cabaña para vacacionar. La oferta de se realizó a través de la página web de la misma. Allí aparecían e individualizaban los artículos y muebles con que contaba la cabaña. Al llegar a la misma se constata que no había horno, solo un calentador precario, lo que ocasionó que tuviera que tirar parte de los alimentos que llevó para consumo en esos días, ya que uno de los integrantes de la familia tiene una afección de salud que le impide el consumo de algunos alimentos. Ante ello la actora pidió la devolución del monto pagado y le fue negado. El lugar presentaba deterioro importante en paredes y mobiliario, además de no contar con mesa y sillas para el número de personas que ofrecía la cabaña en su página Web. El incumplimiento por parte de la demanda generó el no disfrute de las vacaciones de la familia. La actora sostuvo que una violación al deber de informar al brindar información falsa sobre lo ofrecido por la cabaña, información con la que de haber contado habría determinado por no alquilar la cabaña. Por lo que pidió se condene a la demandada a la devolución total del dinero pagado aparándose en la ley de relaciones de consumo, 17250.

La propia demandada en su declaración de parte, admitió que la página web no estaba actualizada, aclarando que hace poco adquirió dicho emprendimiento, por lo que la información allí ofrecida no resulta totalmente fidedigna.

Respecto del estado general de la cabaña, se constató en la documental agregada que el mismo no es bueno, excediendo los desperfectos constatados –roturas, filtraciones de agua desde el techo y falta de mantenimiento, lo mínimamente aceptable del consumidor medio, máxime teniendo en cuenta que las estadías contratadas en este tipo de vivienda, están destinadas a vacacionar, por lo que es exigible a efectos de garantizar una estancia adecuada, un mínimo de confort.

Cabe señalar, que existe responsabilidad de la propietaria en mantener la página Web en las que se ofertan las cabañas en forma actualizada, debiendo coincidir lo ofrecido con lo disponible en la realidad. Dicha página reviste gran importancia, en estos casos, pues determina para el usuario nada más ni nada menos que la contratación de la estadía ofrecida. Asiste razón a la actora, al citar doctrina que entiende que la información que posee el oferente es parte sustancial de las relaciones de consumo, poniendo en una situación de desigualdad al consumidor. Lo que hace una obligación principal del proveedor de brindar información veraz del producto o servicio.
Por lo analizado precedentemente, corresponde condenar a la demandada al monto que abonó la actora por concepto de arrendamiento.

Bibliografía

1- ASPIS, Analía "Comercio Electrónico, Régimen Contractual" Errepar, Bs. As. Argentina.
2- Manual de Defensa del Consumidor en Uruguay web www.consumidor.mef.gub.uy
3- Manual de Derecho de Consumo. Madrid, REUS, 2016.
4- Nuevo Reglamento de Protección de Datos de la Unión Europea. 25/05/2018 Digital Guide 1&1 web www.1and1.es
5- Tevez N. Alejandra "El Deber de Advertencia en la Relaciones de Consumo" La Ley Año LXXIXX N° 81 Buenos Aires, Argentina.
6- Ley de Relaciones de Consumo N° 17250 del año 2000.

INTELIGENCIA ARTIFICIAL Y SU APLICACIÓN EN EL ÁMBITO JURISDICCIONAL: PROBLEMAS, AVANCES, PERSPECTIVAS Y RETOS, ANÁLISIS DEL CASO NACIONAL

Por: ***Willmar José Gallegos Sotomayor***
Perú

"LOS ROBOTS VAN A QUITAR EL TRABAJO, A TODOS AQUELLOS QUE TRABAJEN COMO ROBOTS…"

INTRODUCCION

El presente trabajo hablara sobre la posibilidad de aplicar la inteligencia artificial en el ámbito jurisdiccional y en la administración pública , de manera más precisa en la toma de decisiones Judiciales y de la administración Publica, hará un breve repaso de los proyectos e intentos realizados hasta el momento y cuanto se ha avanzado en la materia, tanto internacional como nacional, pero al final aterrizara en el campo de estudio específico , que es el sector Publico de Perú, al final se llegaran a conclusiones, si es posible o no la aplicación en el sector.

Se hará un pequeño resumen de conceptos preliminares, en la que intervienen ambas materias , tanto derecho e Informática y el campo de la Inteligencia artificial, no abordará temas tales como son La regulación en Tecnología ; las normas que tiene el derecho en el campo de la informática, sino que hablará sobre la informática y la Inteligencia artificial aplicadas al derecho en la administración de Justicia y la Administración Pública y a los diversos sistemas qué funcionan en un sistema de Gobierno electrónico, por lo tanto se trata de un trabajo de investigación donde se pretende llegar a conclusiones prácticas y reales; donde se pretende abordar el tema de manera realista, tomando en cuenta los avances hasta el momento y a la vez poner en manifiesto las deficiencias que ha tenido el sistema peruano en gobierno electrónico, alrededor de estos años ya que lleva un retraso en comparación a otros países.

En la segunda parte se hará, una breve explicación, de cómo se aplicó y se puede aplicar LA INTELIGENCIA ARTIFICIAL Y LOS SISTEMAS EXPERTOS en la toma de decisiones judiciales administrativas y de otra índole, porque se puede y hasta dónde se puede llegar a utilizar dichos Sistemas De Expertos, en la toma de decisiones y se analizará porque no se puede confiar del todo en la Informática.
En la tercera parte se hará un breve resumen de lo avanzado hasta el momento en el sistema de peruano y se mencionara proyectos tales como el Expediente Judicial Electrónico y la emisión de la Ley De Firmas Y Certificados Digitales y su implicancia, entre otros.

En el cuarto punto se mencionaran las conclusiones, recomendaciones a futuro y campos de aplicación siempre enfocándose a la realidad peruana.

1.- CONCEPTOS PRELIMINARES DE INTELIGENCIA ARTIFICIAL, CONCEPTOS BÁSICOS, TEORIA BÁSICA, SISTEMAS INFORMÁTICOS Y SISTEMAS EXPERTOS

Antes de empezar con la presente ponencia y la exposición de la idea central es necesario hacer un repaso, y una introducción de los principales términos y elementos, que se tratarán en este estudio siendo que muchos de los que leen, no son informáticos no conocen, no tiene una idea aproximada de algunos términos que se tratarán en este trabajo:

ALGORITMO:

Un algoritmo es un conjunto de instrucciones o reglas que previamente han sido escritas y definidas y ordenadas que pueden ser finitas y las cuales nos indican, cómo realizar determinada actividad mediante la indicación de pasos es así que Mediante los algoritmos que parten de un estado inicial y una entrada y mediante la realización de pasos sucesivos se llega al final de éste y se obtiene una solución para el presente estudio, los algoritmos representan la base de los sistemas expertos y los sistemas informáticos en general y representan la base de la programación.

Es así que para llegar también a una solución o una conclusión mediante instrucciones en el campo judicial o de normas , se utiliza Algoritmos, en la actualidad muchas veces ni siquiera nos damos cuenta de ello, ya que los aplicamos de manera directa e inconsciente los cuales, no son graficados, sino que simplemente son indicados es el caso que cuando aplicamos, un procedimiento sea en la vía Civil Penal o Administrativa y estamos siguiendo etapas y fases estamos, utilizando algoritmos también cuando aplicamos normas leyes con determinadas condiciones y con determinadas sentencias indicaciones, también estamos aplicando algoritmos

APRENDIZAJE AUTOMÁTICO

El aprendizaje automático es la capacidad de las computadoras de aprender e intentar imitar el razonamiento humano, esto puede incluir el desarrollo de su aprendizaje en forma autónoma a lo largo del tiempo, proporcionándoles datos como interacciones del mundo real y otro tipo de observaciones. Pero dado que el pensamiento y razonamiento humano es tan variado y complejo, se hace difícil llegar a querer igualarlo.

AUTONOMÍA

Se habla de autonomía cuando los dispositivos con IA no necesitan ayuda de las personas; esa autonomía se clasifica en diferentes niveles. Un ejemplo de ello son los coches autónomos Los coches autónomos, por ejemplo, que alcanzan un nivel 4 de autonomía cuando no necesitan una persona para funcionar a plena capacidad y por tanto no tienen volante ni pedales.

PROCESAMIENTO NATURAL DEL LENGUAJE

El procesamiento natural del lenguaje, es analizar y comprender la estructura del lenguaje humano para convertirlo en instrucciones, solamente una red neuronal avanzada es capaz de analizar y comprender la estructura del lenguaje humano; esta interpretación y su procesamiento resultan indispensable para servicios de traducción, chatbots o asistentes de IA como Alexa o Siri.

En el caso de procesos judiciales aún no se ha llegado al grado tal de que un software escuché los alegatos y los fundamentos de las partes y pueda procesarlos y pueda obtener un resultado, pero esto no sería nada extraño que se diera en un futuro no muy lejano

RED NEURONAL

Con un diseño similar al sistema nervioso y al cerebro humano, una red neuronal organiza las etapas de aprendizaje para dar a la IA la capacidad de resolver problemas complejos dividiéndolos en niveles de datos. Las redes neuronales aplican la táctica de la división en conjuntos de datos más pequeños para ir superando cada capa de su aprendizaje.

SISTEMA EXPERTO

Un sistema experto (también llamado un sistema basado en conocimiento) captura en forma efectiva y usa el «conocimiento de un experto» para resolver un problema particular experimentado en una organización.
A diferencia del DSS, que deja la decisión final al tomador de decisiones, un sistema experto selecciona la mejor solución a un problema o a una clase específica de problemas.
Se dice que los sistemas expertos traten de imitar el comportamiento humano utilizando la información el usuario les proporciona o con la información que son alimentadas, un caso típico de sistema experto es aquel al que le haces preguntas hasta que puede edificar un objeto o encontrar lo que sobre lo que se estaba preguntando

Raymond Kurzweil(1) señala que los sistemas expertos tienen tres componentes primarios:

a) Una base de conocimiento estructurada con bases de datos relacionados con los conceptos propios del dominio;

b) Reglas de decisión que describen los métodos para tomar decisiones en un campo especializado, y [1]

c) Máquina de inferencia, que también recibe el nombre de motor de inferencia, sistema que aplica las reglas de base de conocimientos a la toma de decisiones y es capaz de conducir el razonamiento para resolver un problema específico.

LA METODOLOGÍA PARA LA ELABORACIÓN DE UN SISTEMA EXPERTO

También debe tomarse en cuenta que un sistema experto es como sistema de información o software qué contiene los mismos elementos y también ha pasado por distintas fases y etapas en su desarrollo y elaboración.

[1] Raymond Kurzweil, *La era de las máquinas inteligentes*, México, CONACYT/Equipo Sirius Mexicana, 1994, p. 504.

La utilización de sistemas expertos trae diversos ventajas tales como la gran capacidad de almacenamiento de información, que difícilmente podrá tener una persona común y el tiempo en que perdura, es entre otras características, las cuales son según ***Goretty Carolina Martínez Bahena***[2] son:

A continuación se señalan algunas características de un sistema inteligente:

a) Es un programa de computo que puede estar ligado a otros elementos de transferencia y conversión de información;

b) Dispone de una gran cantidad de conocimiento sobre un problema fruto de la experiencia y realiza un razonamiento similar al que haría un humano frente a un problema;

c) Puede operar con datos cuantitativos y con datos cualitativos;

d) Puede emitir conclusiones a partir de datos vagos o incompletos;

e) Puede interrumpir una línea de razonamiento para ocuparse de otra y ser capaz de volver a su línea anterior y,

f) Puede tener interfaces externas, o consultar una base de datos, esto es, ser capaz de comunicarse con otros y tener la posibilidad de operar en ambientes distintos.

MODELOS DE SISTEMAS EXPERTOS

Brevemente mencionamos dos:

a) **Modelo De Procesamiento Simbólico**, el cual es un sistema experto basado en conocimiento.

b) **Modelo Conexionista Y De Redes Neuronales,** que es un modelo que trata de resolver problemas no algorítmicos, a partir de la experiencia almacenada como conocimiento trata de emular el cerebro humano y su comportamiento realmente las redes neuronales son bastante utilizada en diversos campos de la ciencia como la medicina, la programación, la informática, entre otros

SOBRE LOS SISTEMAS EXPERTOS JURÍDICOS

Un sistema experto jurídico es un sistema que puede plantear posibles soluciones algunos asuntos jurídicos aplicando el conocimiento mismo de normas y leyes en la materia el sistema experto jurídico puede estar compuesto por:

a) Conocimiento

b) Motor de Inferencia

c) La Interfase con el Usuario

[2] ***Goretty Carolina Martínez Bahena,*** La inteligencia artificial y su aplicación al campo del Derecho **alegatos**, núm. 82, México, septiembre/diciembre de 2012

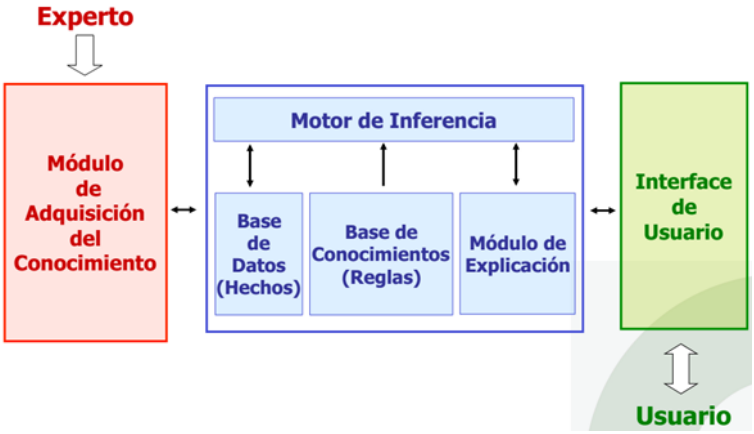


Figura 1. Arquitectura de un Sistema Experto Basado en Reglas. (Díez, 2010)

TIPOS DE SISTEMAS EXPERTOS JURÍDICOS

Se han dado ciertos tipos de sistemas expertos jurídicos, entre ellos mencionaremos a sistemas QUE se basa en la literalidad del texto normativo O QUE por el contrario, se basan en tareas propias del procesamiento cognitivo. Ent3e ellas tenemos:

a) Sistemas basados en reglas de producción

b) Modelo positivista explícito subyacente

c) Modelo constructivista

d) Modelo de razonamiento legal basado en casos.

Y algunos ejemplos de Sistemas expertos jurídicos son:

Expertius	Sistema experto basado en el modelo constructivista y redes neuronales
Split-up	Sistema experto basado en reglas y redes neuronales expertos
SIES	Sistema experto de sentencias

SIES: SISTEMA EXPERTO DE SENTENCIAS

Sobre este sistema experto nos vamos a centrar un poco, ya que fue inicialmente ideado para apoyar a los jueces emitir sentencias, en juicios de Divorcio en México fue creado por la doctora **María de Socorro Téllez** e incluía un prototipo de Sentencia cuya base del conocimiento estaba integrada por los requisitos de forma y fondo de una sentencia de derecho familiar. En el sistema tenían que estar incluidas bases de datos del procedimiento judicial en familia así como los datos de la demanda contestación y análisis de las pruebas documental confesional testimonial y otros.

Pero en este sistema experto no sólo se utilizaba la lógica; ya que si bien es cierto se tenía que conocer el proceso jurídico a fondo, era necesario conocer y dominar Cómo aplica la

lógica en el campo del derecho con todas sus variantes ya que se trataba de un problema de Lógica de Razonamiento Jurídico.

Esta fue una de las primeros intentos por elaborar un sistema experto de sentencias, el cual tuvo buena acogida por parte de los usuarios que son los trabajadores del mismo Juzgado, en México pero se toparon con variedad de dificultades y retos a realizar; como principal conclusión que podemos sacar de esto es que un sistema experto no puede hacer el trabajo de manera integral; sino que representa una herramienta y un apoyo en la labor jurisdiccional.

INFORMÁTICA JURÍDICA DECISIONAL

Es una rama de la informática jurídica qué consiste en la utilización de la informática como instrumento para ayudar en la toma decisiones, tal es el caso de los jueces ante la sentencia está basada en Inteligencia Artificial, su objetivo más ambicioso es que la máquina resuelva los mismos problemas jurídicos

SISTEMAS INFORMÁTICOS DE GESTIÓN, SISTEMAS DE ESTUDIOS DE ABOGADOS

En el campo de los sistemas expertos sistemas informáticos e Inteligencia artificial también encontramos del otro lado la utilización de estos; por parte de los usuarios qué son los Abogados, Usuarios, Entidades, Fiscalías, Comisarías y todos los que forman parte de este sistema cada uno de ellos utiliza las herramientas tecnológicas de la manera que mejor le es posible, existiendo en la actualidad infinidad de herramientas e innovaciones que mejorarán y optimizarán el trabajo que se realiza tales como Sistemas De Información, Sistemas De Análisis De Datos, Sistemas The Big Data, Sistemas De Inteligencia Artificial Aplicada A Estudios Jurídicos, Archivos Y Documentos Electrónicos, Firma Digital, Chatbots para Asesoría, Automatización De Procesos Y Trámites Legales, etc.

La ventaja que tienen algunos organismos y empresas del sector jurídico; es que no se encuentran limitadas las órdenes del Gobierno Central y es que ellos pueden aplicar las tecnologías que prefieran de manera libre y como mejor les parezca pero al encontrarse con una institución, con la cual tienen que interactuar como es el Poder Judicial, en el caso peruano se dan contra un muro, que los frena tal es el caso por ejemplo de la firma digital la cual ya se utilizaba desde los años noventa, pero que recién en nuestro país se está implementando de pocos en el Sector Público.

2.- POSIBLE APLICACIÓN O NO APLICACIÓN, DE LA INTELIGENCIA ARTIFICIAL EN EL CAMPO DE LAS DECICIONES JUDICIALES Y ADMINISTRATIVAS.

2.1 JURIMETRIA

Para el presente trabajo, daremos un breve concepto de lo que es Jurimetría, actualmente el mundo globalizado y competitivo en que nos encontramos conocer la probabilidad de éxito, de un proceso o de un recurso planteado ante los tribunales, conocido como "escrito" (cómo se llama en Perú) se hace muy importante, Asimismo determinar cuánto puede demorar en

resolverse o en procesar determinado acto es muy es información valiosa para los que interactúan con el sistema de justicia.

Para definir el término Jurimetría y para hacer una correcta definición de este se analizará desde dos enfoques un enfoque tradicional y un enfoque actualizado

Así que se tiene que en el año 1949, Loevinger da a conocer su artículo JURIMETRICS THE NEXT STEP FORWARD en la revista Minnesota Law Review en el cual acuña el término de *Jurimetría como el conjunto de investigaciones, tanto lógico matemáticas como estadísticas, dirigidas a los distintos tipos de análisis de la información jurídica y a su tratamiento mecánico mediante computadoras, con la finalidad de documentar de forma automática dicha información, racionalizarla, enseñarla, administrarla y preservarla dentro de la esfera del Derecho*.

Según este concepto la J**urimetría,** son todas aquellas herramientas actualizadas, que se utilizan para medir "la información jurídica" de todo tipo, es por ello que se le da más importancia a la Estadística y a al Análisis de Datos

Actualmente el término se ha dado y utilizado con mayor intensidad y muchas veces él utiliza de manera incorrecta; actualmente el enfoque va más orientado y se acerca a la Inteligencia Artificial es así que si es cierto si bien es cierto se utilizan herramientas como la Estadística El Análisis de Datos, inclusive Big Data entre otros en el campo de la información, que se genere dentro del sistema jurídico a esto se le agrega la utilización de Inteligencia Artificial ,la cual se aplicaría en diversos sistemas y para esto se uniría con los datos recopilados es así que se utiliza una fuente de información y bases de datos para lograr a través de los sistemas expertos predecir ciertos resultados y procesar toda esta información, existen diversidad ejemplos en la actualidad estudios de abogados internacionales qué utilizan estas herramientas de análisis de información para sus casos y saber qué probabilidades y posibilidades de éxito tendrán

En Perú esta práctica aún no es muy difundida y es limitada a algunas empresas; pero en el campo de la Justicia; no se aplica, por los costes que implica y la información; qué es restringida, no habiendo una política de datos abiertos concreta en el país.

2.2 SISTEMAS EXPERTOS EN LA TOMA DE DECICIONES JURÍDICAS Y RESOLUCIÓN DE SENTENCIAS, DESDE EL PUNTO DE VISTA DEL DERECHO

Ya hemos desarrollado el marco preliminar, pero ahora vayamos a la parte central y más importante de nuestra ponencia, ¿si es posible aplicar los sistemas expertos y los sistemas de Inteligencia artificial en un proceso o procedimiento judicial de tal manera que tengamos una suerte de jueces reemplazados por un software o programa o reemplazados por un robot, es esto posible?

Cómo se tienen idea, en una decisión judicial llámese Sentencia, entran diversos factores a tallar para la emisión final de ésta, no sólo es la el razonamiento y el silogismo puro qué se aplica de manera mecánica y lógica, si bien es cierto se aplica la ley de manera estricta en

una sentencia, existen diversas variantes que hacen que la decisión final, tenga diversos matices.

Analizaremos algunas de estas variantes:

A.-Interpretación de la Norma

Para aplicar tal o cual Norma los Resolutores o Jueces utilizan un criterio llamado "Interpretación de la Norma" existiendo diversos tipos tales como Interpretación literal, interpretación teleológica, interpretación histórica entre otros, lo cual si está permitido y aceptado, utilizando y aceptándose esta forma de aplicar la Norma por la razón de que no todas las normas son perfectas y se encuentran vacíos o encuentran deficiencias, este análisis, no podría ser hecho por un Sistema Experto ya que no conoce los criterios necesarios para realizar esta interpretación y aunque los conociera y fueron ingresados a su Base de Conocimientos, no podría aplicarlo como una persona lo haría.

B.-Sobre atenuantes agravantes eximentes y otras variantes de la norma

Cuándo se aplica una sanción o infracción los Resolutores, toman en cuenta diversos factores en la en la realización de la misma; tales como los hechos adicionales que motivaron o que formaron parte de realizar dicha acción, tales como los agravantes , qué hacen que una sanción sea más drástica, o las atenuantes que hacen que se reduzca la sanción o pena, sería muy fácil para un sistema experto aplicar estos atenuantes o agravantes, dándoles una valorización sea positiva o negativa, pero la diferencia sustancial con una persona está en la clasificación de estas conductas, ya que existen algunas que no sé enmarcan en ninguna formas de ser agravante o atenuante, expresamente mencionada, por la norma, por lo cual el resolutor, tendría que aplicar criterios especifico o hacer una comparación jurisprudencial para aplicar correctamente dichas variaciones.

C.-Conocimiento del sistema y la jurisprudencia

Cuando se presenta una Resolución Final, entran diversos aspectos que se deben tomar en cuenta y que sólo una persona con conocimiento amplio y total de la Realidad Jurídica Legal, puede aplicar o puede hacer valer, si bien es cierto los personas no son infalibles y son susceptibles de errores también es cierto que la experiencia de una persona no se compara la experiencia de un sistema de información o software.

Por lo cual no se puede, comparar y aplicar de la misma manera la utilización de sistemas expertos en la administración de Justicia y cómo se Aplicaría en el ámbito Empresarial donde los resultados son más exactos y "fríos", ya que en el ámbito empresarial no entra a tallar ese factor humano subjetivo, como si lo hace y le es permitido al derecho.

La conclusión más importante hasta este momento, es que en el derecho el razonamiento no va a ser como las matemáticas no hay una conexión exclusiva y excluyente entre sus proposiciones, ya que las diferentes proposiciones normas y reglas que se utilizan el derecho no se aplican de manera silogística.

El producto jurídico sentencias resoluciones es más como una obra de arte, Conformada por diversos factores y variables, que no son solo la aplicación de la Norma en solitario y no es el resultado de un proceso mecánico de extracción de información, también hay que tomar en cuenta, la acción creativa del juez o resolutor y todos los factores que tomó en cuenta para realizar dicha sentencia.

SOBRE SENTENCIAS Y FALLOS CONTRADICTORIOS.

Al analizar de qué manera se aplica las normas y qué manera piensa un juez o resolutor, nos vamos con la idea de que esta pequeña variación que pueden aplicar cada uno de ellos puede hacer que la sentencia o resolución, cambie o no hay uniformidad al respecto y podemos pensar que la solución para esto sería aplicar un software o un sistema experto, pero hay que tomar en cuenta, que un sistema experto está alimentado por una base de conocimientos, la cual está entrenada por la misma información que se le ingresa, al ingresársele información de manera contradictoria, el sistema experto no garantizara un resultado uniforme

Para solucionar el problema de fallos contradictorios o diferentes entre ellos, la norma ha establecido soluciones tales como Los Plenos Casatorios, Los Precedentes Vinculantes, La Jurisprudencia Vinculante, etc. la cual es aplicada por los jueces en sus sentencias, pero usando el juicio y evaluación respectiva aplicada al caso concreto, análisis y discernimiento que sería difícil de hacer por un Sistema Experto.

2.3 POSTURAS A FAVOR Y EN CONTRA

Hasta el momento ya hemos analizado desde el lado del Derecho, cuáles serían las dificultades aplicar un Sistema Experto; en la resolución y emisión de decisiones judiciales o resoluciones administrativas; el siguiente punto a tratar, es sobre cuáles serían sus puntos en contra y sus beneficios:

2.3.1 Puntos en contra:

Fallas.
Una de las principales objeciones que se le hace a los sistemas expertos, es la falibilidad, ya que estos no son perfectos, esto no resultaría ser ningún problema si se tratase de experimentos, ensayos , simulaciones que hace en el ámbito académico, pero si estamos hablando de aplicarlo a la vida real a situaciones tales como decidir sobre darle pena de muerte a una persona , o condenar a cadena perpetua a un acusado , ya la cosa cambia, ya que no se puede dejar tamaño responsabilidad a un software.

Limitaciones.
Un Sistema Experto pese a tener grandes bases de conocimiento y bases de datos, horas de entrenamiento, tiende a ser limitado con respecto al conocimiento, que se debería aplicar en la emisión de una sentencia o cuando se habla de analizar, ya que como dijimos anteriormente analiza el problema con una visión limitada y no holística o más amplia y mucho menos humana

Ingrediente subjetivo.
Parece irónico decir qué en una Ciencia Jurídica debe aplicarse resultados de manera o con ingredientes subjetivos, pero en el campo del Derecho sucede así y más aún en el campo de las decisiones y sentencias, acciones que no puede realizar un software o Sistema Experto

Responsabilidad.
Un punto muy interesante es el de la responsabilidad; si utilizamos un Sistema Experto para condenar a una persona y luego resulta que esta es inocente, quién ASUME la "Responsabilidad Funcional"(Cómo se le llama en Perú)es acaso el programador?, tal vez sea el equipo de programadores del proyecto, es acaso el operador del sistema, quienes asumen esa responsabilidad ?

2.3.2 Puntos a favor.

Ahora veremos los puntos que se deben tomar en cuenta para aplicar un Sistema Experto y llevarlos a la práctica y tomarnos en serio, en este punto de la actualidad en que nos encontramos:

BASE DE CONOCIMIENTOS EXPONENCIAL
Los sistemas expertos poseen una base de conocimientos y una base de datos y pueden procesar una cantidad de información que para el Humano común sería imposible procesar en muy poco tiempo y es esa ventaja la que se puede aprovechar en la actualidad, en dónde se puede revisar gran número de normas y diversas materias en muy poco tiempo siendo esta una gran herramienta para el juez y los operadores de y también en la administración pública

PROCESAMIENTO DE INFORMACION Y RAPIDEZ
La información que se puede recopilar y utilizar, ya sea en Jurisprudencia, como Normas, como en Doctrina, como todo tipo de información es muy superior a la que puede hacer una persona o trabajador común, Pero lo importante es el tiempo en que está se procesa ya que los actuales sistemas son cada vez más rápidos y precisos en los resultados logrados.

REVISION DE FALLOS
Como ya se dijo anteriormente se puede aprovechar todo esta capacidad, de los Sistemas Expertos, no sólo para generar resultados, sino para revisar resultados de Operadores De Justicia, Resolutores y Jueces lo cual haría qué el producto final y la decisión final sea la óptima, siendo un filtro más en la emisión de resoluciones y sentencias, lo que haría es optimizar y mejorar los resultados, la producción y la eficacia de estos.

TIEMPO
Y es a mi parecer el factor más importante de todos; al utilizar herramientas de software y tecnología en la administración en el sistema de Justicia: el tiempo, y ya que en Perú el sistema resulta ser bastante lento e ineficiente, siendo esto un perjuicio para la población y para la misma justicia que buscan todos los que acuden al Poder Judicial, y la principal

crítica de ellos hacia este organismo, es el tiempo; con el uso de Sistemas Expertos, **se reducirían significativamente los tiempos que actualmente se están haciendo** y si a esto se suma el uso de tecnología por parte de los demás usuarios del sistema de Justicia , tales como Abogados, Estudios Jurídicos, Policía, Ministerio Público ,Entidades Del Estado, se lograrían resultados ideales, para la población, lo cual también mejoraría el dinamismo y la Economía del país.

Figura 2, https://elperuano.pe/fotografia/thumbnail/2018/05/07/000043090M.jpg

2.4 CONCLUSIONES PARCIALES SOBRE ESTA SECCIÓN.

Los sistemas expertos no van a reemplazar la actividad de un JUEZ O RESOLUTOR , y no van a reemplazar todo el SISTEMA JUDICIAL , son una herramienta y un medio más el cual debe ser utilizado y aprovechado, por lo que, lo que van a hacer es mejorar y potencializar las capacidades y la producción de los jueces y resolutores, es una excelente herramienta en la medida que se le aplique, lo mejor posible , ya que es imposible aplicársele de manera total con una responsabilidad absoluta; sino que forman parte y deben formar parte del Sistema; y ya nos damos cuenta que se aplica , parcialmente, mediante algunos sistemas informáticos; pero aún hay mucho camino que recorrer y queda por cumplir muchas iniciativas e igualar la aplicación que se está haciendo en otros países.

3.-APLICACIÓNES E INICIATIVAS EN LA REALIDAD PERUANA CAMPO DE APLICACIÓN: SISTEMA PERUANO DE JUSTICIA Y LA ADMINISTRACION PÚBLICA.

En esta sección hablaremos un poco de lo que es la aplicación de toda esta tecnología dentro de la realidad peruana; poniendo énfasis o centrándonos en el sistema peruano de justicia y la administración pública en el Perú se han implementado hace poco normas, sobre la simplificación administrativa en éstas se busca incidir más sobre la aplicación de la tecnología en los servicios que brindan atención al público por parte de las entidades.

Es también de importancia mencionar algunas iniciativas, de algunos organismos tales como la SGDI (Secretaria De Gobierno Digital) que se esfuerzan por lograr un servicio al ciudadano más tecnológico en todo el Estado, pero que en comparación con países como Colombia, Brasil, Uruguay en Latinoamérica y alejándonos un pocos más en Europa, recién se encuentra en una etapa inicial.

Algunas iniciativas tales como la masificación del DNI ELECTRÓNICO y la aplicación de la Ley De Firmas de Certificados Digitales, sientan las bases para tener un Estado más tecnológico, pero resultan insuficientes ya que los avances en informática son muy rápidos y dejan, a lo que podría ser la tecnología de hoy ya obsoleta el día de mañana. Por lo cual es recomendable tomar ejemplos y modelos de éxito de otros países como referencia, más no igualarlos ni en intentar copiarlo al pie de la letra, ya que la realidad de cada país y cada región es diferente y no se lograrían los mismos resultados.

En lo que respecta al Poder Judicial, la principal iniciativa reciente es la implementación del EXPEDIENTE JUDICIAL ELECTRÓNICO (EJE)en algunas Cortes y Juzgados del país lo cual representará y masificación en el uso de medios digitales en la Administración De Justicia.

Pero en lo que se refiere a Inteligencia artificial en la administración pública y en el Sistema Judicial, ésta se encuentra aún muy lejos de aplicarse en el Estado Peruano, debido justamente a qué se encuentran en una etapa en la que no ha tomado en cuenta estas aplicaciones y posibles usos y sus beneficios, siendo también el principal problema la falta de presupuesto para incentivar, estas iniciativas.

Figura 3. http://eje.pe/wps/wcm/connect/EJE/s_eje/as_inicio/

5.-CONCLUSIONES

Los sistemas expertos como tales, no se pueden aplicar en el campo de las decisiones judiciales de manera íntegra , por el momento , y menos en la realidad peruana, pero si se deben aplicar en otras áreas de gestión y se debe aplicar la tecnología, optimizando varios procesos en la gestión y administración en los campos administrativo y judicial.

Los sistemas de información y los sistemas expertos y representen excelentes herramientas en la gestión, en la Administración de Justicia y En La Gestión Pública y éstas deben utilizarse de la mejor manera posible, ya que representan una ayuda invalorable en el trabajo cotidiano, pero nunca van a reemplazar, en todo el trabajo de una persona con conocimiento y experiencia sobre el tema sino que son una herramienta más, a tomarse en cuenta.

Los Sistemas Expertos y la Inteligencia Artificial, tienen posibilidades aplicación increíbles , dentro del sector público y más aun dentro del el campo Empresarial y el sector Privado más aun, ya que gozan de muchos facilidades, para que puedan aplicársele, tales como la libertad que tienen para utilizar las herramientas tecnológicas, cosa que no ocurre cuando lo aplicas en el estado peruano ya que te encuentras limitado a la tecnología que ahí se utiliza,

otro punto limitante es el presupuesto que se requiere para implementar ese tipo de proyectos en cualquier empresa o entidad

Existen en Estados Unidos y en otros países, ya muchas iniciativas sobre la aplicación de sistemas de Inteligencia artificial en el campo de las Decisiones Judiciales, pero estás aún no han sido tomadas en cuenta en el sistema peruano y en las oficinas de TIC de muchas entidades.

La tecnología suele alcanzar muchas veces y sobrepasar las predicciones que se tenían sobre ella y no sería bueno qué innovaciones tales como el blockchain y los Smart Contract, tomen por sorpresa y sobrepasen cualquier regulación que se pueda tener , sobre ellas es así por ejemplo que ya existe en el mundo, en diversos países iniciativas legales para limitar el uso de Bitcoin, pero no se logra porque, como una vez más repito, *la tecnología va muchos pasos más adelante que el derecho,* por lo cual es el derecho el que debe adaptarse a la realidad y no al revés, pero siempre respetando los principios básicos constitucionales establecidos por cada Nación.

Como último punto, quiero tratar, sobre la aplicación de los sistemas y la tecnología y la afectación al empleo de las personas; ya que si bien es cierto que muchas veces la tecnología ha reemplazado acciones repetitivas y tediosas que realizaba una persona, con lo cual se tiene la idea , *que una máquina va reemplazar y dejar sin trabajo a las personas,* lo cual hace que muchos trabajadores, tengan la idea equivocada de que al implementar más tecnología en sus puestos de trabajo sus empleos corran riesgo, lo cual no debería ser un motivo para oponerse al uso de la tecnología, sino un motivo más para capacitarse especializarse y adaptarse a las nuevas tendencias; ya que si bien es cierto se dejará de lado muchas acciones que se realizaban, se crearán otras actividades en las cuales trabajar, tales como la programación el diseño la gestión y el manejo de software.

BIBLIOGRAFIA

René Acosta Ramírez , Yadirka Verdecia Díaz , Yarina Amoroso Fernández, Jurimetría : Una opción para la sociedad. Serie Científica de la Universidad de las Ciencias Informáticas, Vol. 9, No. 4, Abril, 2016

DEFINICION DE INFORMATICA JURIDICA: La Informática jurídica de en Prezi. [en línea], [sin fecha]. [Consulta: 14 marzo 2016]. Disponible en: https://prezi.com/_kosqhnmjjzd/definicion-de-informatica-juridica-la-informatica-juridica/.

Goretty Carolina Martínez Bahena, La inteligencia artificial y su aplicación al campo del Derecho alegatos, núm. 82, México, septiembre/diciembre de 2012

Bourcier, Daniéle. *Inteligencia artificial y derecho*. Barcelona [España], UOC, 2003.

Guastini, Ricardo. *Estudios sobre la interpretación jurídica*. 4ª ed. México, Universidad Nacional Autónoma de México/Porrúa, 2002.

Hartnell, Tim. *Inteligencia artificial conceptos y programas*. Cambridge, MSX, 2007.

Huerta Anguiano, Julio Alberto. *Diagramación de argumentos dialógicos y derrotantes en el sistema inteligente Expertius*. Tesis para obtener el grado de Licenciado en Derecho, México, UNAM, 2009.

Lin, Fuhua Oscar. *Designing distributed learning environments with intelligent software agents*. Estados Unidos, Information Science Publishing, 2005.
Nikolaev, Nikolai Y. *Adaptive learning of polynomial networks*. Nueva York [EU], Springer Verlag, 2006.

Cáceres Nieto, Enrique. "Las teorías jurídicas como realidades hermenéuticas". *Boletín Mexicano de Derecho Comparado*. UNAM. Nueva Serie. Año XXXV, núm. 103, México, ene-abr., 2002. Disponible en:

Huerta Anguiano, Julio Alberto. *Diagramación de argumentos dialógicos y derrotantes en el sistema inteligente Expertius*. Tesis para obtener el grado de Licenciado en Derecho, México, UNAM, 2009.

Websites:

-https://tallerdederechos.com/

- http://elderechoinformatico.com/wordpress/

- https://derechoytecnologiaperu.wordpress.com/

- http://julionunezderechoinformatico.blogspot.com/

- **http://fiadi.org/**

LA LEGITIMIDAD PROCESAL EN EL DERECHO AL OLVIDO.

Por: ***Dra. Rebeca Karina Aparicio Aldana***[1]

Controversias sobre la legitimidad pasiva de *Google Spain* en el TS Español, en virtud de lo resuelto por TJUE, y su aplicación en el ordenamiento jurídico peruano – *Google* Perú S.R.L

I. Legitimidad para obrar pasiva – concepto y alcances

La legitimidad para obrar es fundamentalmente un concepto lógico de relación, cuyo entendimiento se basa en los conceptos de relación jurídica sustantiva - entendida esta como el conflicto intersubjetivo o incertidumbre de relevancia jurídica que se presenta en la realidad - y relación jurídica procesal, aquella que surge cuando alguna de las partes en conflictos decide solucionar el problema acudiendo a los tribunales, como demandante, iniciando un proceso en donde el juez hará partícipe del mismo a la contraparte, como demandado, y a todas aquellas personas que puedan coadyuvar a la solución del conflicto. Así, en un proceso hay legitimidad para obrar cuando las partes materiales en conflicto, es decir, las conformantes de una relación jurídica sustantiva, son también las partes en la relación jurídica procesal: demandante y demandado[2].

La legitimidad para obrar consiste, entonces, en la posición habilitante para formular la pretensión o para que contra alguien se formule, por ello, necesariamente radica en la afirmación de la titularidad del derecho subjetivo material (legitimidad para obrar activa) o en la imputación de la obligación (legitimidad para obrar pasiva)[3], de tal forma que, dentro de un proceso particular, la legitimación procesal no es otra cosa que la consideración legal en virtud de la cual se exige, para que la pretensión de fondo pueda ser examinada, que los sujetos en conflicto en razón de un determinado objeto litigioso sean las mismas que actúen como parte en el proceso[4].

En este orden de ideas, la legitimidad para obrar consiste, respecto al demandante, en ser la persona que conforme con la ley sustancial está legitimada para que por sentencia de fondo y mérito se resuelva si existe o no el derecho o la relación jurídica sustancial pretendida en

---

[1] Doctora (*Suma Cum laude*) en Derecho y Máster en Derecho del Trabajo y la Seguridad Social de la Universidad Rey Juan Carlos (Madrid-España); Máster en Derecho, con mención en Derecho Constitucional, y Abogada por la Universidad de Piura (Perú); Licenciada en Derecho por la Universidad de Alcalá (España). Analista Legal de la Dirección de Protección de Datos Personales del Ministerio de Justicia (Perú) y Profesora de Derecho del Trabajo y Nuevas Tecnologías en la Escuela Jurídica y de Negocios (ESJUR).

[2] MONROY GÁLVEZ, Juan. Las excepciones en el Código Procesal Civil Peruano, *Themis*, N° 27-28, 1994, Perú, p. 124.

[3] En el mismo sentido, MONTERO AROCA, Juan. "La legitimación en el Código Procesal Civil del Perú", *Ius et Praxis. Revista de la Facultad de Derecho de la Universidad de Lima*, N° 24, 1993, Perú, p. 14.

[4] MATURANA MIQUEL, Cristian, "El procedimiento, la legitimación para obrar y el control de admisibilidad en el requerimiento de inaplicabilidad e inconstitucionalidad", *Revista de Derecho Público*, N° 72, 2010, Chile, p. 413.

la demanda, y respecto al demandado en ser la persona que conforme a ley sustancial está legitimada para discutir u oponerse a dicha pretensión del demandante.

Así, la legitimación para obrar pasiva o del demandado, se puede definir como aquella en la cual este debe ser la persona a quien, conforme a ley, le corresponde contradecir la pretensión del demandante o frente al cual permite la ley que se declare la relación sustancial objeto de la demanda o la pretensión[5].

Atendiendo a esta definición tanto Google *Spain* como Google Perú S.R.L. señalan no tener legitimidad para obrar pasiva, pues afirman que se constituyen en una persona jurídica distinta de Google Inc. o Google LLC, por lo que no se encuentran en posibilidad de atender a la solicitud de los reclamantes que alegan el ejercicio de su derecho al olvido, ello debido a que su actividad no se encarga de la administración de los servicios de las plataformas de búsqueda, que se encuentran a cargo de Google LLC o Google Inc.

La plataforma Google *Search*, señalan Google *Spain* y Google Perú, pertenece a los productos brindados por Google LLC o Google Inc. y es a través de este servicio que se realiza la indexación de las búsquedas. Google Perú S.R.L o Google *Spain* constituyen simplemente meros gestores de publicidad, por lo que tanto Google Perú S.R.L o Google *Spain* no tienen control alguno sobre el referido motor de búsqueda, y, por ende, no se le puede pretender atribuirle la capacidad para efectuar tratamiento de datos personales de ningún tipo.

Siendo esto así, no existiría de acuerdo a lo alegado por Google *Spain* y Google Perú legitimidad para obrar pasiva, en primer lugar, porque ambas personas jurídicas realizarían actividades ajenas a las propias del tratamiento de datos personales, pues su actividad principal es la de gestores de publicidad, actividad que no implica tener control sobre el motor de búsqueda que es Google *Search* y, segundo, porque esta plataforma de indagación o indexación no se encuentra a su cargo sino que es parte de los productos o servicios de una persona jurídica distinta que es Google LLC o Google Inc.

II. Estado de la cuestión – España:

1. A favor de la no responsabilidad de *Google Spain*.

Sentencias del Tribunal Supremo Sala de lo Contencioso Administrativo, 13 de junio de 2016[6] y 14 de marzo de 2016[7]: interpretación en sentido restringido de responsable de tratamiento.

1.1. Hechos:

La Agencia Española de Protección de datos resuelve que *Google Spain* y *Google Inc.* son corresponsables en el tratamiento de datos personales.

[5] DEVIS ECHANDÍA, Hernando. "Teoría General del Proceso", Tomo I, Universal, 1984, Argentina, pp. 297 y 298.
[6] STS Contencioso administrativo, de 14 de marzo de 2016 (Rec. 1380/2015)
[7] STS Contencioso administrativo, de 13 de junio de 2016 (Rec. 810/2015)

Por este motivo, *Google Spain* impugna judicialmente esta resolución ante la Sala Contencioso Administrativa de la Audiencia Nacional quien coincide con lo resuelto por la autoridad administrativa.

Visto lo anterior, *Google Spain* interpone un recurso de casación ante el Tribunal Supremo - Sala de lo Contencioso alegando falta de legitimidad pasiva en el procedimiento administrativo ya que no desarrolla ninguna actividad de tratamiento de datos, no interviene en ningún motor del buscador de *Google*, limitándose a una actividad de promoción de la contratación de servicios, esencialmente publicitarios, por lo que no puede considerarse responsable del tratamiento de los datos del interesado.

1.2. Núcleo de la cuestión debatida:

Para el Tribunal Supremo, el núcleo de la cuestión debatida es la determinación del responsable del tratamiento de datos objeto de litigio y, concretamente, se pregunta si *Google Spain* ¿Es corresponsable del tratamiento de los datos que gestiona *Google Inc*. a través de su motor de búsqueda en internet?

1.3.Normativa aplicable:

- Artículo 2.d de la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995:

Define al responsable del tratamiento como: "la persona física, jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales…".

- Artículo 3.d. de la Ley Orgánica 15/1999, de Protección de Datos Personales.

Conceptualiza como responsable del tratamiento a aquella: "persona física o jurídica, de naturaleza pública o privada, u órgano administrativo que decida sobre la finalidad, contenido y uso del tratamiento".

1.4. Argumentos de las resoluciones

Para ambas resoluciones el eje central para delimitar la cuestión sobre la legitimidad pasiva de *Google Spain* pasa por establecer los elementos esenciales para definir al responsable del tratamiento que son:

- La determinación de los fines y los medios del tratamiento de los datos personales.
- La delimitación de la concreta responsabilidad en el cumplimiento de las obligaciones impuestas por las normas de protección de datos.

Así, atendiendo a lo resuelto por Tribunal de Justicia de la Unión Europea, en su sentencia de 13 de mayo de 2014[8], que «desbloqueó numerosos procedimientos jurídicos en toda Europa»[9], el Tribunal Supremo español resuelve:

[8] STJUE, de 13 de mayo del 2014, asunto C-131/12. Un desarrollo doctrinal sobre lo resuelto en esta sentencia en: COTINO HUESO, Lorenzo. "La STJUE del caso Google vs. AGPD de 2014. Algunos olvidos y otras tendencias negativas respecto a las libertades informativas en internet", Valencia, España, 2014, en documentos *on line*: http://www.uv.es/seminaridret/sesiones2014/google/ponenciacotino.pdf (última revisión 9 de julio de 2018).

[9] MARTÍNEZ OTERO, Juan María. "La aplicación del derecho al olvido en España tras la STJEU Google contra AEPD y Mario Costeja", *Revista Boliviana de Derecho*, N° 23, Bolivia, 2017, p. 132.

- El gestor del motor de búsqueda de *Google Inc*., realiza la siguientes actividades: hallar información publicada o puesta en internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas, según un orden de preferencia, por ende, al ser Google Inc. quien gestiona el motor de búsqueda *Google Search*, es responsable del tratamiento de datos al determinar los fines, las condiciones y los medios del tratamiento de datos personales.
- Al ser *Google Inc*. quien gestiona el motor de búsqueda también asume las responsabilidades del tratamiento de datos, con las obligaciones que de ello se derivan, en orden al efectivo cumplimiento de la normativa tanto europea como nacional reguladora del tratamiento de los datos personales, sin que esa responsabilidad pueda trasladarse también a otro sujeto o sujetos que, sin intervenir en esa gestión del motor de búsqueda, realiza actividades conexas o vinculadas, como las que realiza *Google Spain* cuyas actividades se abocan a la promoción publicitaria como soporte económico del motor de búsqueda.
- El Tribunal Supremo deja en claro que ninguna de las actividades que atribuyen responsabilidad sobre el tratamiento de los datos es realizada por *Google Spain*, tales como:
  a. Hallar información publicada o puesta en internet por terceros.
  b. Indexarla de manera automática.
  c. Almacenarla temporalmente.
  d. Ponerla a disposición de los internautas, según un orden de preferencia determinado.

  Lo que se ha probado es que es Google Inc. es quien gestiona técnica y administrativamente a *Google Search*, no existe prueba de que *Google Spain* realice en España una actividad directamente vinculada a la indexación o almacenamiento de información o de datos en los sitios de internet de terceros, dado que *Google Spain* se limita a la promoción y venta en España de espacios publicitarios del motor de búsqueda y, en ese sentido, constituye una actividad conexa o vinculada económicamente a su matriz, pero sus actividades son de distinta naturaleza a la determinación de los fines y medios del tratamiento.

  No debe por tanto identificarse, ni confundirse la determinación de los fines y medios del tratamiento, que caracteriza la consideración de responsable, con la actividad de colaboración en la consecución de objetivos. De ahí que sólo Google Inc. es la responsable del tratamiento, pues a ella corresponde en exclusiva la determinación de los fines, las condiciones y los medios de tratamiento de datos personales.

En este orden de ideas, si *Google Spain* no realiza ninguna de las actividades que atribuyen responsabilidad sobre el tratamiento de los datos, difícilmente puede considerarse responsable o corresponsable del tratamiento de datos controvertido, pues no consta participación alguna en la gestión del motor de búsqueda y determinación de fines y medios de dicho tratamiento y, por ello, no existe asunción o atribución a la misma de responsabilidad en el cumplimiento de alguna de las obligaciones que la norma impone al responsable del tratamiento. En este orden de ideas, sólo *Google Inc*. es el responsable del concreto tratamiento de los datos.

Cabe aclarar que según el Tribunal Supremo esta afirmación no supone un desconocimiento de la Sentencia del Tribunal de Justicia de la Unión Europea, porque:

- El Tribunal de Justicia de la Unión Europea trae a colación la vinculación económica de *Google Spain* con Google Inc., no en razón de atribuirle a *Google Spain* la calidad de responsable del tratamiento de datos personales, sino con la finalidad de poder aplicarle la norma nacional española y comunitaria a *Google Inc*. (domiciliada en EEUU).

Así concluye:
No es que se trata de ampliar el concepto de responsable del tratamiento, sino en dejar en claro que la norma de conexión territorial para poder aplicarle a *Google Inc.* la normativa española y comunitaria es la contenida en el artículo 4.1.a de la Directiva 95/46 que bajo el rótulo de "Derecho nacional aplicable" dispone que:

1. *Los estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando:*
   a. *El tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro…*

La misma directiva en su considerando 19 señala que: "El establecimiento en el territorio del Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable" y "que la forma jurídica de dicho establecimiento, sea una simple sucursal, una empresa filial con personalidad jurídica, no es un factor determinante".

Por ende, no puede discutirse que *Google Spain* se dedica al ejercicio efectivo y real de una actividad mediante una instalación estable en España. Además, está dotada de personalidad jurídica propia, encontrándose su actividad, en tanto parte del Grupo *Google*, económicamente vinculada a la de *Google Inc.*, pues permite la promoción y venta en España de los espacios publicitarios del motor de búsqueda, lo que sirve para rentabilizar el servicio propuesto por el motor, con lo cual se puede afirmar que ambas actividades: las del motor de búsqueda (*Google Inc.*) y las de quien realiza las actividades publicitarias (*Google Spain*) se encuentran íntimamente relacionadas y, por ende, *Google Spain*, es un establecimiento de *Google Inc*. pues, en el marco de sus actividades, es posible que *Google Inc*. sea económicamente rentable[10].

En este orden de ideas, de acuerdo al Tribunal de Justicia de la Unión Europea se establece un ámbito de aplicación territorial particularmente extenso que incluye responsables del tratamiento no domiciliados dentro de la Unión Europea cuando este tenga efectivamente un establecimiento de este responsable en alguno de los estados miembros, aun cuando este "establecimiento" no se dedique al tratamiento efectivo de los datos. De esta forma, el Tribunal de Justicia de la Unión Europea trata de evitar la elusión del cumplimiento de la normativa europea de protección de datos en base a que el responsable del tratamiento no tiene su sede social en el territorio europeo.

Sin embargo, esto no significa atribuirle corresponsabilidad a *Google Spain* en el tratamiento de los datos personales, sino que la consideración por parte del Tribunal de Justicia de la Unión Europea de *Google Spain* S.L. como establecimiento en España de *Google Inc*. se

[10] Importante desarrollo sobre el ámbito de aplicación territorial de la legislación española de Google en: *Vid.* SIMÓN CASTELLANO, Pere. *El régimen constitucional del derecho al olvido digital,* Tirant lo Blanch, Valencia, España, 2012, pp. 194 y ss.

realiza a los efectos de atraer la aplicación de la normativa europea y, por derivación, la española de protección de datos personales, al tratamiento gestionado por la segunda, a través de su motor de búsqueda *Google Search*, no obstante tratarse de una empresa ubicada fuera de la Unión.

En estricto seguimiento de esta argumentación, el responsable del tratamiento era *Google Inc.* y no *Google Spain,* por lo que esta última no se encontraba legitimada pasivamente dentro del proceso administrativo iniciado ante la Agencia Española de Protección de Datos; pese a ello esta entidad emitió pronunciamientos contra esta empresa frente a la cual no tenía habilitación legal para ejercitar las facultades de control, ni, en consecuencia, seguir un procedimiento eficaz al respecto, lo que determina la nulidad de pleno derecho de las resoluciones que le atribuían responsabilidad.
La apreciación de este vicio de la resolución impugnada no puede eludirse por la simple referencia a la condición de *Google Spain* de representante de la compañía estadounidense, pues:

- No se acredita de forma alguna la realidad de esta representación, ni con carácter general ni específica para este procedimiento, habiendo *Google Spain* negado esta condición.
- La intervención de un representante no altera la titularidad del derecho o condición de obligado, ni traslada la responsabilidad del representado al representante.

De manera que, aun en el supuesto de actuación por representante, que no es el caso, subsiste la condición de responsable del tratamiento y su legitimación pasiva, por lo que el procedimiento y la declaración de obligado al cumplimiento y realización del derecho a la tutela que se demanda por el reclamante ha de dirigirse frente al responsable del tratamiento controvertido, que en este caso el *Google Inc*.

En resumen, la identificación de *Google Inc.* como responsable del tratamiento al que debe dirigirse el titular de los datos personales en el ejercicio de su derecho se justifica ampliamente en:

a. La clara definición legal de la condición de responsable del tratamiento en la norma nacional española y en la norma comunitaria.
b. La interpretación que al respecto sostiene el Tribunal de Justicia de la Unión Europea que al resolver declara expresamente que:
    - El tratamiento de datos consiste en: hallar información publicada o puesta en internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas.
    - El gestor de un motor de búsqueda debe considerarse responsable de dicho tratamiento. En el caso concreto, nadie cuestiona que el "gestor" es *Google Inc*. y no *Google Spain*.
    - La percepción de dicha interpretación objetivamente puede sostenerse por los distintos tribunales que han de aplicar la norma comunitaria.
    - La naturaleza de la obligación cuyo cumplimiento exige el interesado, obligación de hacer o no hacer impuesta por la ley (acceso, cancelación, rectificación, oposición) requiere de la efectiva participación del responsable del tratamiento de datos objeto de impugnación, participación que delimita el alcance de su responsabilidad y la exigencia de la correspondiente reparación, adoptando las medidas precisas al efecto.

- La asunción como propia de tal condición por parte de la entidad Google Inc. que a raíz de la sentencia del Tribunal de Justicia de la Unión Europea ha adoptado medidas tendentes a facilitar el ejercicio del denominado "derecho al olvido".

Ello impide considerar como responsable a *Google Spain* que ninguna participación tiene en la gestión del motor de búsqueda y en la determinación de los fines y medios del tratamiento, circunstancia que en ningún momento se cuestiona.

1.5. Sobre el proceso trilateral de tutela

La sentencia del 13 de junio de 2016 deja en claro que es consciente que el procedimiento de tutela de los derechos de acceso, rectificación, cancelación y oposición tiene como requisito la comunicación o reclamación al responsable del tratamiento, frente a cuya respuesta negativa, no satisfactoria o ausencia de respuesta, el interesado puede formular reclamaciones ante la Agencia Española de Protección de Datos contra la cual puede interponerse recurso contencioso administrativo.

Por ello, aunque reconoce que en el ámbito jurisdiccional, la identificación de *Google Inc*. como responsable del tratamiento al que debe dirigirse el titular de los datos personales en el ejercicio de su derecho, genera *a priori* el problema de que *Google Inc*. tiene su domicilio legal en California (EEUU); este inconveniente en realidad no es tal, porque no supone para este una dificultad o carga añadida, en ninguna fase del procedimiento dado que puede ejercer tales derechos a través de cualquiera de los servicios de atención al público, con lo cual puede formularse electrónicamente de manera sencilla, gratuita y directa por los servicios implementados por *Google Inc*. que ofrece a los interesados información completa sobre el ejercicio de sus derechos, facilita los correspondientes formularios y proporciona instrucciones precisas para cumplimentarlo.

Tampoco, el hecho de que *Google Inc*. tenga su domicilio en el extranjero, significa una carga para Agencia Española de Protección de Datos porque basta para la iniciación del procedimiento la presentación de la correspondiente reclamación ante la Agencia Española de Protección de Datos, sin que las comunicaciones con el responsable del tratamiento en el ámbito del procedimiento abierto presenten mayores exigencias que las llevadas a cabo directamente por el interesado, máxime teniendo en cuenta la implicación de los intervinientes en el desarrollo de la llamada sociedad de la información y la constante evolución normativa hacia la tramitación de los procedimientos a través de medios electrónicos.

2. A favor de responsabilidad de *Google Spain*.

Sentencia del Tribunal Supremo Sala de lo Civil, de 5 de marzo de 2016[11]: Interpretación en sentido amplio del responsable del tratamiento.

2.1. Argumentos que sostienen la postura:

Los hechos de la sentencia son los siguientes:

La demanda que da origen a esta sentencia, aunque encuentra sus antecedentes en procedimientos trilaterales de tutela, no tiene origen en una acción contenciosa administrativa

[11] STS Civil, de 5 de abril de 2016 (Rec. 3869/2014).

contra una resolución de 2010 la cual estimaban la reclamación formulada y el derecho de oposición ejercido contra *Google Spain* e instaba a esta entidad para adoptar las medidas necesarias para retirar los datos de su índice e imposibilitar el acceso futuro a los mismos.

La demanda es una acción iniciada en 2011 contra Google *Spain*, con fecha posterior a esta resolución administrativa, en donde se solicita la tutela de los derechos al honor, a la intimidad, a la propia imagen y a la protección de datos personales, exigiendo:

- Que se declare que *Google Spain* había cometido una intromisión en sus derechos a la intimidad personal, familiar, a la imagen y al honor.
- Que se les ordenara retirar la información personal de las indexaciones, pues pese a las resoluciones administrativas esta información continuaba en la web.
- Que esa intromisión ilegítima les había causado daños morales y económicos.

La audiencia nacional resolvió que *Google*, a partir de la decisión de Agencia Española de Protección de Datos que estimó la reclamación contra *Google Spain* y que instó a que esta entidad tomara medidas necesarias para retirar los datos de su índice e imposibilitar el acceso en el futuro, debía conocer la Antijuricidad de su conducta y, sin embargo, continuó presentando el enlace en la página web.

Ahora considera que *Google* sólo es responsable de los daños patrimoniales con fecha posterior a la resolución de Agencia Española de Protección de Datos de 2010, sin embargo, si lo considera responsable de daño moral, dado que la divulgación de la información de internet sí afectaba sus derechos al honor, intimidad.

Google Spain recurre esta sentencia alegando lo siguiente:

- No tener legitimación pasiva porque no es la responsable del buscador donde se indexa la información litigiosa, siendo el único responsable del tratamiento Google Inc[12].

Al respecto el Tribunal Supremo resuelve:
Que la razón por la que el Tribunal de Justicia de la Unión Europea considera aplicable la normativa comunitaria europea sobre protección de datos fue que *Google Spain* podía ser considerado responsable del tratamiento, entendiendo este concepto en sentido amplio, acorde con la finalidad de la Directiva.

Para justificar esta conclusión analiza con detalle la Sentencia del Tribunal de Justicia de la Unión Europea, de 13 de mayo de 2014 señalando lo siguiente:

- El Grupo *Google* utiliza una empresa filial: *Google Spain*, como agente promotor de ventas de los espacios publicitarios que se generan en el sitio de internet de *Google*. *Google Spain* tiene personalidad jurídica propia y domicilio en España y dirige su actividad fundamentalmente a las empresas radicadas en España, actuando como agente comercial del grupo, en dicho Estado miembro. Tiene como objeto social promocionar, facilitar y procurar la venta de productos y servicios de publicidad *on line* a través de internet para terceros, sin embargo, la actividad de promoción y venta de espacios

[12] Sobre los argumentos de Google *Spain* para rechazar la aplicación de la ley española: *Vid.* RALLO LOMBARTE, Artemi. *El derecho al olvido en internet*, Centro de Estudios Constitucionales, Madrid, España, 2014, pp. 137 y ss.

publicitarios, de la que *Google Spain* es responsable para España, constituye la parte esencial de la actividad comercial del Grupo *Google* y puede considerarse que está estrechamente vinculada a *Google Search*[13].

- Partiendo de esa premisa, el Tribunal de Justicia de la Unión Europea aclara que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable y que la forma jurídica del establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante.
- *Google Spain* se dedica al ejercicio efectivo y real de una actividad mediante una instalación estable en España. Además, al estar dotada de personalidad jurídica propia es de este modo filial de *Google* Inc. en el territorio español y, por lo tanto, es un establecimiento.
- Por ello frente a la alegación de que únicamente *Google Inc*. es el único responsable del tratamiento el Tribunal Supremo resuelve señalando que el Tribunal de Justicia de la Unión Europea no exige, para que sea aplicable el derecho nacional, que el tratamiento de datos personales controvertido sea efectuado por el propio establecimiento en cuestión, sino que se realice en el marco de las actividades de este.
- Además, como se trata de la defensa y protección de derechos fundamentales, no cabe interpretaciones restrictivas.
- Atendiendo a la interpretación extensiva de este concepto debe entenderse en el sentido de que se lleva a cabo un tratamiento de datos personales en el marco de las actividades de un establecimiento responsable de dicho tratamiento en el territorio de un Estado miembro. Entonces, habrá tratamiento cuando el gestor de un motor de búsqueda crea en el Estado miembro una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de ese Estado miembro.

El Tribunal Supremo – Civil afirma que la Sentencia del Tribunal de Justicia de la Unión Europea:

- No tenía como objeto determinar el concepto de responsable del tratamiento, sino si el tratamiento de datos personales se lleva a cabo en el marco de las actividades de un establecimiento del responsable de dicho tratamiento en el territorio de un Estado miembro cuando el gestor de un motor de búsqueda crea, en el estado miembro, una sucursal o una filial destinada a garantizar la promoción y la venta de espacios publicitarios propuestos por el mencionado motor y cuya actividad se dirige a los habitantes de este Estado miembro, a efectos de determinar el ámbito territorial de aplicación de la legislación europea.
- Sin embargo, esta sentencia si hace referencia a cuestiones importantes para resolver el tema motivo del recurso, siendo estos los siguientes:
    1. El amplio concepto de responsable del tratamiento: como persona, autoridad, servicio u organismo que sólo o conjuntamente con otros determina los fines y

[13] Por otro lado, también la actividad del buscador, aunque realice una actividad comercial, tiene importantes efectos en lo que respecta al ejercicio de derechos fundamentales, como, el ejercicio del derecho a la libertad de información, pues ordena el contenido de internet y permite a los internautas acceder a todo tipo de fuente. Al respecto: *Vid.* MARTÍNEZ OTERO, Juan María. "El derecho al olvido en internet: debates cerrados y cuestiones abiertas tras STJUE Google vs. AEPDP y Mario Costeja", *Revista de Derecho Político*, N° 93, España, 2015, pp. 123 y ss.

los medios del tratamiento de datos personales, pues el objetivo de protección eficaz y completa de los derechos fundamentales afectados por el tratamiento de los datos personales impide una interpretación restrictiva.

2. Las actividades de *Google Inc*. y *Google Spain* están indisociablemente ligadas, pues la primera no sería posible sin la segunda que le aporta los resultados económicos. Además, la presentación de resultados de la búsqueda, consecuencia del tratamiento automatizado de los datos personales, viene acompañada de la presentación de publicidad vinculada a los términos de búsqueda introducidos por los internautas, cuya contratación es promovida por *Google Spain*.
3. El tratamiento de datos que supone el funcionamiento del buscador Google en las búsquedas realizadas desde España se realiza en el marco de las actividades de *Google Spain*, filial de *Google Inc*, que ha de ser considerado como el establecimiento en España de dicha compañía, a efectos de la aplicación de la normativa sobre protección de datos, no siendo un factor determinante la forma jurídica de *Google Inc* haya decidido que adopten sus establecimientos en Estados distintos de aquel en que está situado actualmente el domicilio social, los EEUU.

En este contexto cobra pleno sentido:

a. Que, *Google Inc*. haya designado a *Google Spain* como responsable del tratamiento en España de dos ficheros inscritos por *Google Inc.* ante la Agencia Española de Protección de Datos.
b. Que, cuando la Agencia Española de Protección de Datos ha requerido a *Google Spain* para que cancele el tratamiento de datos de una determinada persona, dicho tratamiento haya resultado cancelado, aunque lo haya sido con meses de retraso.
c. Que *Google Spain* haya aceptado su legitimación pasiva en anteriores litigios seguidos en relación con los efectos en España del funcionamiento del motor de búsqueda de *Google*, porque dicho tratamiento de datos se realiza en el ámbito de actividad conjunta de la matriz y la filial española.

Sentado lo anterior, aunque no se puede negar que *Google Inc.* es el encargado del gestor de búsqueda de *Google Search* y, por ende, responsable del tratamiento de datos, lo cierto es que *Google Spain* también puede ser considerada, en sentido amplio, como responsable del tratamiento de los datos que realiza el buscador de *Google Search* en su versión española conjuntamente con su matriz *Google Inc.* y, por tanto, está legitimada pasivamente para ser parte demandada en los litigios seguidos en España en que los afectados ejerciten en un proceso civil sus derechos de acceso, rectificación, cancelación y oposición; y, exijan responsabilidad por la ilicitud del tratamiento de los datos personales realizados por el buscador de *Google* en su versión española.

Una interpretación en contrario significaría frustrar en la práctica el objetivo de garantizar una protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.
Una interpretación restrictiva supondría en la práctica, un serio obstáculo, cuando no un impedimento para la efectividad de los derechos fundamentales que el ordenamiento jurídico protege frente al tratamiento automatizado de datos de carácter ilícito.

Los sujetos protegidos por la normativa sobre protección de datos son las personas físicas. El efecto útil de la normativa comunitaria se debilitaría enormemente si los afectados hubieran de averiguar, dentro del grupo empresarial titular de un motor de búsqueda, cuál es la función concreta de cada una de las sociedades que lo componen, lo que en ocasiones, constituye incluso un secreto empresarial y, en todo caso, no es un dato accesible al público en general.

También se debilitaría el efecto útil de la normativa europea si se diera trascendencia a la personificación jurídica que el responsable del tratamiento de los datos diera a sus establecimientos en distintos Estados miembros, obligando de este modo a los afectados a litigar contra sociedades situadas en un país extranjero.

Incluso en el caso de litigar en España, la inmensa mayoría de las personas tendría dificultades para interponer la demanda de protección de sus derechos fundamentales contra una sociedad domiciliada en EEUU y obtener la tutela judicial efectiva de sus derechos en un plazo razonable, tanto por el elevado coste que supone la traducción en inglés de la demanda y la documentación que le acompaña, como la dilación que implicaría la inevitable tardanza en el emplazamiento de dicha sociedad al tener que acudir a los instrumentos de auxilio judicial internacional, con lo que se prolongaría la situación de vulneración de los derechos fundamentales. Y, sobre todo, en caso de tener una sentencia condenatoria, si la demandada no le diera cumplimiento voluntariamente, el ciudadano afectado debería solicitar el reconocimiento y la ejecución de la sentencia en los EEUU, con el coste y las dificultades, tanto de orden teórico como práctico.

Por otra parte, dadas las características del servicio que prestan estos motores de búsqueda, la sociedad más directamente relaciona con la determinación de los fines y medios del tratamiento de datos personales podría ser ubicada en otro Estado con el que no existieran relaciones que permitieran el emplazamiento de la sociedad y el posterior reconocimiento y ejecución de la resolución que se dictara.
En definitiva, aceptar la tesis de que sólo *Google Inc.* es responsable del tratamiento significaría abocar a los interesados a unos procesos que dificultan el ejercicio de sus derechos haciendo en la práctica, casi imposible, su protección, pues habría que interponerse contra empresas radicadas en EEUU con los elevados gastos y dilaciones que ello trae consigo.

2.2. En relación a las sentencias de lo contencioso

Para el Tribunal Supremo – Sala de lo Civil, las sentencias de lo contencioso no son condicionante para resolver como se ha hecho en el presente caso por las siguientes razones:

- En las sentencias de lo contencioso se está resolviendo con relación a resoluciones dictadas en un procedimiento administrativo seguido ante la Agencia Española de Protección de Datos, mientras que esta sentencia se dicta en un proceso civil que tiene por objeto la protección de los derechos fundamentales del demandante, en concreto, los derechos al honor, a la intimidad y a la protección frente al tratamiento automatizado de datos de carácter personal.
- La vulneración de los derechos fundamentales del demandante no proviene de que Google *Spain* haya incumplido con la resolución administrativa, sino que no canceló el

tratamiento de los datos personales cuando fue requerida para ello por el demandante a la vista de las circunstancias concurrentes:

- Naturaleza de la información asociada a los datos personales (indulto de una pena).
- Periodo transcurrido desde que sucedieron los hechos relevantes.

2.3. Nuevo Reglamento General de Protección de Datos Personales y su impacto en lo que respecta al ámbito territorial de aplicación en España.

El Reglamento General de Protección de Datos europeo supone el mayor hito legislativo en materia de privacidad y protección de datos personales en Europa en los últimos veinte años, viniendo a sustituir a la Directiva 95/46/CE. El nuevo RGPD entró en vigor en mayo de 2016 y es de aplicable cumplimiento en España a partir del 25 de mayo de 2018.

En lo que se refiere al ámbito territorial de aplicación se han producido una aclaración y un cambio importante de paradigma:

1. Aclaración: De acuerdo a lo establecido en la Directiva 95/46/CE el tratamientos debía lleve a cabo en el contexto de las actividades de un establecimiento dentro de la UE. El Reglamento General de Protección de Datos, por su parte dispone que se aplicará al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado de la Unión, aclarando que esta aplicación se producirá independientemente de que el tratamiento tenga lugar o no en la Unión, es decir, será de aplicación a aquellas empresas fuera de la UE que realicen actividades dentro de la UE que impliquen el tratamiento de datos personales, incluso si dicho tratamiento no tienen ningún tipo de presencia física en el territorio de la Unión.

En este orden de ideas, si existe un establecimiento de una empresa dentro de la UE que realiza tratamiento de datos fuera de la Unión de residentes europeos, le sería aplicable el reglamento. Este sería uno de los criterios para considerar que a Google Inc. le es aplicable la legislación de la Unión Europea.

2. Cambio de paradigma: Según la Directiva 95/46/CE el ámbito de la aplicación fuera de la unión es el criterio de medios, si los medios utilizados para tratar datos por parte de la empresa extranjera son de la unión, se consideraba aplicable la normativa nacional. El reglamento reemplaza el criterio de medios por el de a quien se dirigen los servicios, con algunas características especiales:
   - Cuando el tratamiento se refiera a datos de residentes de la UE.
   - Debe tener por objeto la oferta de bienes o servicios o el control del comportamiento o de la conducta cuando este se lleve dentro de la UE.

Lo que supondría incluir como responsable a Google *Spain* dentro del ámbito de aplicación del Reglamento General de Protección de Datos personales.

Cabe aclarar que esta delimitación del ámbito de aplicación en ningún caso supone reconocer como responsables del tratamiento a ambas personas jurídicas, sólo deja en claro que ya sea por uno o por otro motivo tanto Google *Spain* como Google Inc. son pasibles de aplicación de la legislación de protección de datos de la Unión.

III. Aplicación de la normativa peruana de protección de datos a Google LLC y Google Perú S.R.L.:

3.1. Ámbito de aplicación: en razón del establecimiento.

Dado que Google LLC, responsable del tratamiento, es gestionado por una empresa que tiene su domicilio social en Estados Unidos, territorio distinto al del Estado peruano, habría que aclarar si la normativa nacional peruana le es aplicable.

El artículo 5 del Decreto Supremo 003-2013-JUS del Reglamento de la Ley 29733, de Protección de Datos Personales establece que las disposiciones de la Ley de Protección de Datos y de su Reglamento son de aplicación al tratamiento de datos personales cuando:

1. Sea efectuado en un establecimiento ubicado en el territorio peruano correspondiente al titular del banco de datos personales o de quien resulte responsable del tratamiento.

Este mismo artículo, en su penúltimo párrafo, aclara que: "(…) se entenderá como establecimiento (…) si se trata de personas jurídicas residentes en el extranjero (…) el local en el que se encuentre la administración principal del negocio en el territorio peruano, o en su defecto el que designe, o cualquier instalación estable que permita el ejercicio efectivo de una actividad.

En virtud de este inciso, a todo titular o responsable de banco de datos que tenga "un establecimiento" o instalación estable en territorio peruano debe de serle aplicada la normativa peruana de protección de datos, independientemente de que este establecimiento se dedique o no efectivamente al tratamiento de los mismos.

Lo que se debe determinar, entonces, es si Google Perú efectivamente puede considerarse o no como un establecimiento de Google LLC. Téngase en cuenta a este respecto que hasta antes de 2018, Google LLC no tenía sede en el Perú.

En primer lugar Google Perú se dedica al ejercicio efectivo y real de una actividad mediante una instalación estable en Perú.

Asimismo, está dotada de una personalidad jurídica propia con su propio objeto social: dedicarse a la publicidad del Grupo Google, por lo que las actividades que realiza Google Perú permiten el ejercicio efectivo de las actividades de Google LLC, pues están destinadas a la promoción y venta en el Estado peruano de los espacios publicitarios del motor de búsqueda de Google LLC, que sirven para rentabilizar el servicio propuesto por este motor.

Por ello, las actividades desarrolladas por Google LLC (gestor del motor de búsqueda) y Google Perú (publicidad del grupo Google) ubicado en el Estado peruano se encuentran indisociablemente ligadas dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable, siendo este motor el medio que al mismo tiempo permite realizar las actividades publicitarias.

Por ello, Google Perú puede ser considerado como una instalación estable que permite las actividades de Google LLC dentro el Estado peruano y, en consecuencia, puede aplicársele a esta empresa, radicada en Estados Unidos, la normativa peruana sobre protección de datos.

Ahora, es importante señalar que en el Perú aún no existe un pronunciamiento judicial respecto al tema de la legitimidad pasiva de Google Perú S.R.L.; sin embargo si existen resoluciones administrativas emitidas por la Autoridad de Protección de Datos.

A este respecto, la Autoridad de Protección de Datos peruana, afirma que «*si bien no ignora que Google, para efectos societarios o de otra índole tenga diversas denominaciones, reparticiones, sedes nacionales y competencias empresariales separadas y divididas o compartimentadas y su sede principal esté en Estados Unidos de América, (…) al mismo tiempo es claro que, para los efectos de definir la competencia que la ley le otorga para la efectiva protección de los datos personales de los peruanos, ha de atenerse a lo que la legislación peruana establece.*

En la misma línea de razonamiento, es un hecho que Google, por su propia decisión, cuenta con un establecimiento bajo la forma societaria legítima [Google Perú S.R.L.] *y de su conveniencia, que realiza actividad económica en el territorio peruano vinculada, entre otros, a la prestación de servicios de publicidad, anexos al servicio de búsqueda de información indexada que presta Google Search*»[14].

3.2. Ámbito de aplicación: En razón del medio utilizado.

El otro criterio para determinar el nexo competencial es, si los medios que utiliza la transnacional Google, están o no situados en territorio nacional.

De acuerdo a lo señalado por la Autoridad de Protección de Datos peruana son medios aquellos que desarrollan operaciones técnicas (automatizadas o no) que efectúa el responsable del tratamiento, ajenos al control del titular de los datos personales, y precisamente bajo el control de un responsable distinto al titular de los datos personales. Dentro de estos medios se encontrarían los motores de búsqueda, cuya base de datos es recogida por un programa llamado araña o motor que se dedica a buscar páginas en la red que organiza y cataloga automáticamente relacionando temas con palabras clave. Así, las arañas están programadas para recorrer las páginas web recopilando información sobre sus contenidos con independencia de la ubicación territorial del soporte informático de dicha información.

De esta forma, cuando un usuario indaga sobre una información concreta en el motor de búsqueda determinados programas de dicho buscador consultan las bases de datos y presentan resultados clasificados por su relevancia para esa búsqueda concreta.
Ahora, para ofrecer su servicio, Google utiliza el motor de búsqueda *Google Search* que rastrea servidores de páginas web ubicados en todo el mundo, es decir, con independencia de la ubicación territorial del soporte de la información y ciertamente con independencia de la ubicación territorial de su sede principal, de modo que, evidentemente, incluye información

[14] Resolución Directoral N° 045-2015-JUS/DGPDP, de 30 de diciembre de 2015, p. 10.

con soporte en territorio peruano e información de peruanos residentes en Perú, para extraer información que dará respuesta a las búsquedas de usuarios también peruanos, lo que sustenta, afirma la Autoridad de Protección de Datos Peruana, la venta de publicidad dirigida al público peruano.

Por ello, continúa, no cabe duda que *Google Search*, en el desarrollo de sus actividades comerciales:
- Rastrea información que contiene datos personales de ciudadanos peruanos con la finalidad de facilitar su posterior localización.
- Presenta información en función de la ubicación geográfica, pudiendo optarse por la información sólo extraída en sitios web propios del Perú.

En consecuencia, para brindar el servicio de búsqueda en internet al mercado peruano, Google realiza la operación técnica consistente en visitar las páginas webs ubicadas en servidores webs peruanos, registrar e indexar información extraída, por lo que resulta evidente que utiliza medios situados en territorio peruano, y en su caso para el tratamiento de los datos fuera del control de los titulares de los datos personales[15].

3.3. Solución dada por el Perú: Google Perú sí tiene legitimidad de obrar – Un problema: la no determinación del específico o específicos responsables.

Las resoluciones administrativas emitidas hasta el 2017 referidas a la cuestión materia de análisis en el Perú se decantan por la posición de considerar tanto a Google LLC como a Google Perú S.R.L como responsables del tratamiento pues sostiene, como lo hace España, que las actividades que realiza Google Perú S.R.L. en territorio peruano tiene como finalidad posicionar a Google LLC como marca y dinamizar la publicidad *on line* en el Perú, desempeñando dicho establecimiento (en el marco del ámbito de aplicación territorial de la LPDP y su reglamento) actividades vinculadas al tratamiento de datos personales derivados de las búsquedas efectuadas en el motor de búsqueda Google Search.

En consecuencia, se afirma que la actividad del motor de búsqueda de Google Search (Google LLC) y la actividad del establecimiento (Google Perú S.R.L) se encuentran indisolublemente ligados; toda vez que:
- La publicidad es el medio para hacer rentable al buscador.
- Los resultados de las búsquedas son acompañadas por la publicidad[16].

Por ello, no es ajena al tratamiento que resuelta inadecuado debido a la hipervisualización de información personal de ciudadanos peruanos sin consentimiento (…) al resultar, la gestión de Google Perú S.R.L. una parte inseparable en el proceso del negocio del buscador[17].

Por ello, bajo la personería jurídica local o transnacional se encuentra dentro del ámbito de aplicación de la LPDP y su reglamento, como responsable del tratamiento

[15] Resolución Directoral N° 045-2015-JUS/DGPDP, de 30 de diciembre de 2015, pp. 11 y 12.
[16] Resolución Directoral N° 045-2015-JUS/DGPDP, de 30 de diciembre de 2015, p. 16.
[17] Resolución Directoral N° 012-2016-JUS/DGPDP, de 11 de marzo de 2016, p. 22.

Sin embargo, la peculiaridad en Perú es que al momento de delimitar la responsabilidad no opta por una responsabilidad conjunta de Google Perú S.R.L y de Google LLC de forma subsidiaria, ya que la ley no establece una responsabilidad solidaria en estos casos, sino alternativa resolviendo declarar fundada las reclamaciones formuladas contra Google bajo la personería de Google Inc. o de Google Perú S.R.L.

Ello, obviamente, genera el inconveniente de no definir a la persona efectivamente responsable del tratamiento de los datos personales y cuál de las dos personas jurídicas debía realizar las acciones pertinentes que den cumplimiento a lo dispuesto por la Autoridad de Protección de Datos. Por ello "si bien los nombres de Google Inc. (entiéndase Google LLC) y Google Perú SRL parecen relacionarse, la [Autoridad de Protección de Datos Personales] del Perú debe diferenciar la personalidad jurídica que mantiene cada una de estas entidades, ya que sus fines societarios y comerciales son diferentes"[18].

3.4. Argumentos a favor de la primera postura – Falta de Legitimación pasiva de Google Perú S.R.L.

De acuerdo al ordenamiento jurídico peruano, el titular del banco de datos personales es la persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad (artículo 2.15 de la LPDP).

Asimismo, el artículo 2. 10 del RLPDP define como encargado del tratamiento a aquel que realiza el tratamiento de los datos personales, pudiendo ser el propio titular o el encargado del banco de datos personales u otra persona por encargo del titular del banco de datos personales, en virtud de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación. Incluye a quien realice tratamiento de datos personales por orden del responsable del tratamiento cuando este se realice sin la existencia de un banco de datos personales.

Por su parte, el artículo 2.14 del RLPD define al responsable del tratamiento como aquél que decide sobre el tratamiento de los datos personales, aun cuando no se encuentre en un banco de datos personales.
En conclusión, el titular del banco de datos personales puede identificarse plenamente con el responsable del tratamiento de datos personales cuando exista un banco de datos personales. También puede que el titular del banco de datos personales o el responsable de su tratamiento asuman plenamente el tratamiento de los datos, sin encargarle esa labor otra persona distinta. Sin embargo, cuando las labores tratamiento son encargadas a otra persona diferente del titular o responsable existirá un encargado del tratamiento.
La LPDP establece claramente que el titular y el encargado del tratamiento de datos personales son las personas obligadas a cumplir con un adecuado tratamiento de los datos personales (artículo 28 y s.s.) siendo, por ende, los responsables de su inadecuado uso o transmisión.

[18] CUENCA ESPINOZA, Alexander. "Protección de Datos personales y Derecho al olvido. Análisis del caso Perú vs. Google", *Foro,* N° 27, Ecuador, 2017, p. 137.

Entonces, si únicamente, de acuerdo a la legislación peruana, el titular, responsable o encargado del tratamiento son quienes deben de responder por los inadecuados usos o transferencias de datos personales, es importante determinar si efectivamente Google Perú, puede ser considerado o no titular, responsable o encargado del tratamiento de datos.

Para determinar si Google Perú es o no titular, responsable o encargado del tratamiento es necesario determinar la efectiva participación en la determinación de los fines y medios de tratamiento, es decir, su efectiva intervención en los concretos aspectos de fijación de fines y medios del tratamiento de datos.
El artículo 2.17 de la LPDP define el tratamiento de datos como cualquier operación o procedimiento técnico automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración, modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de datos personales.

De esto se puede deducir que es el gestor del motor de búsqueda quien determina los fines y los medios de esa actividad, de igual forma como sucede en el caso Español y, por lo tanto, el único titular del tratamiento es Google LLC.

En este orden de ideas, consideramos que el criterio a tener en cuenta es el de quien en sentido estricto, realiza el tratamiento, es decir, aquella persona jurídica a la cual efectivamente se le puede responsabilizar por realiza esta función, que no es otra que Google LLC.

Ahora, este argumento de responsabilidad del tratamiento de Google LLC actualmente contaría con el respaldo de venir acompañado del hecho de que esta persona jurídica cuenta con una sede o sucursal en el Perú, con lo cual no cabe duda alguna de la plena aplicación de la legislación nacional peruana a esta transnacional.

BIBLIOGRAFÍA

MONROY GÁLVEZ, Juan. Las excepciones en el Código Procesal Civil Peruano, *Themis,* N° 27-28, Perú, 1994.
MONTERO AROCA, Juan. "La legitimación en el Código Procesal Civil del Perú", *Ius et Praxis. Revista de la Facultad de Derecho de la Universidad de Lima*, N° 24, Perú, 1993.
MATURANA MIQUEL, Cristian, "El procedimiento, la legitimación para obrar y el control de admisibilidad en el requerimiento de inaplicabilidad e inconstitucionalidad", *Revista de Derecho Público*, N° 72, Chile, 2010.
DEVIS ECHANDÍA, Hernando. "Teoría General del Proceso", Tomo I, Universal, 1984, Argentina.
COTINO HUESO, Lorenzo. "La STJUE del caso Google vs. AGPD de 2014. Algunos olvidos y otras tendencias negativas respecto a las libertades informativas en internet", Valencia, 2014 España.
MARTÍNEZ OTERO, Juan María. "La aplicación del derecho al olvido en España tras la STJEU Google contra AEPD y Mario Costeja", *Revista Boliviana de Derecho*, N° 23, Bolivia, 2017.

SIMÓN CASTELLANO, Pere. *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, Valencia, España, 2012.
RALLO LOMBARTE, Artemi. *El derecho al olvido en internet*, Centro de Estudios Constitucionales, Madrid, España, 2014.
MARTÍNEZ OTERO, Juan María. "El derecho al olvido en internet: debates cerrados y cuestiones abiertas tras STJUE Google vs. AEPDP y Mario Costeja", *Revista de Derecho Político*, N° 93, España, 2015.
CUENCA ESPINOZA, Alexander. "Protección de Datos personales y Derecho al olvido. Análisis del caso Perú vs. Google", *Foro*, N° 27, Ecuador, 2017.

LAS CRIPTOMONEDAS Y SUS IMPLICACIONES TRIBUTARIAS

Por: ***José Francisco Vega S.***
Panamá

Introducción.

Nos hemos acostumbrado a escuchar casi a diario que la tecnología avanza a pasos agigantados en todos los aspectos de nuestras vidas. Y eso es totalmente cierto, sobre todo en el campo de la informática: primero llegaron enormes computadoras, más tarde los ordenadores personales, después el internet; le siguieron los multimedios, luego los dispositivos portátiles y, con el tiempo, estos se hicieron inteligentes. Más recientemente vino a escena el almacenamiento masivo de datos -también conocido como "Big Data"-, el internet de las cosas y por último la inteligencia artificial.

Muchos dirían que todos estos constituyen ejemplos clásicos, representativos de la evolución tecnológica. Sin embargo, antes de profundizar en los criptoactivos y su sistema, para una más ágil comprensión quizás sea oportuno establecer una línea que separe la concepción tradicional de la evolución dentro de la tecnología y la disrupción tecnológica.

Según la Real Academia Española, la disrupción se refiere a "la rotura o interrupción brusca de algo". Entonces, .que debe suceder para que se considere que ha ocurrido una disrupción de la tecnología? Podríamos decir que una tecnología disruptiva nace cuando se interrumpe abruptamente el proceso de evolución y surge una nueva modalidad tecnológica que no tiene antecedentes.

Cuando se habla de tecnología disruptiva se hace referencia a un proceso de intervalo dentro de la evolución tecnológica. Por ejemplo, en la actualidad, nos encontramos en la era digital web 3.0, donde los usuarios y los dispositivos electrónicos pueden interactuar a través de la red mediante un lenguaje natural interpretado por un software. Sin embargo, se espera que dentro de uno años se llegue a la etapa de web 4.0, en la que la inteligencia humana se sintonice con la artificial, para que los seres humanos y los dispositivos nos podamos comunicar en un solo lenguaje en la toma de decisiones rutinarias.

En ese sentido podemos citar a UBER como un ejemplo de proyectos de tecnología disruptiva, cuyos creadores detectaron las fallas principales en los sistemas de transporte. Los taxis y automóviles se crearon hace anos y han evolucionado con el paso del tiempo. Sin embargo, UBER interrumpe ese proceso evolutivo y crea una nueva tecnología a través de una plataforma centralizada, donde cada conductor esta indexado a la red y todo el proceso de selección del transporte es automatizado, incluyendo el pago. Dentro de sus activos fijos, la empresa no invierte en un solo vehículo; todos son de socios que se unen a la plataforma y trabajan conjuntamente.

Clasificación del dinero digital.

El Banco Central Europeo, en un informe de 1998, ofrece un concepto de dinero digital según el cual se trata de un "valor monetario almacenado electrónicamente en un dispositivo tecnológico que puede ser usado para realizar pagos a cualquier empresa distinta del emisor, sin necesidad de involucrar cuentas bancarias en la transacción, pero actúa como instrumento propagado al portador".

Este prepago radica en que el usuario puede anteponer, en dinero fiat, o sea, en dinero fiduciario, el monto que desea transformar en dinero electrónico, que puede venir representado en una tarjeta de débito, monedero virtual o almacenado directamente en una computadora o dispositivo móvil.

El Grupo de Acción Financiera, dentro de su informe de junio de 2014 titulado "Monedas Virtuales. Definiciones Claves y Riesgos Potenciales de LA/FT" establece que la moneda digital puede hacer referencia a una representación digital de cualquier moneda virtual (no dinero fiat) o de dinero electrónico (dinero fiat) y por este motivo, a menudo su uso es intercambiable con el término "moneda virtual".

El informe del GAFI también divide las monedas virtuales en convertibles y no convertibles. La moneda virtual no convertible pretende ser especifica de un dominio o mundo virtual particular, como los videojuegos de rol multijugador excepcionales en línea (MMORPG, por sus siglas en ingles), o Amazon.com, y en virtud de las normas que regulan su uso, no se puede cambiar por dinero real. Algunos ejemplos incluyen: Project Entropía Dollars, Q Coins, y World of Warcraft Gold.

Sin embargo, en el caso del videojuego World of Warcraft Gold surge el debate, sobre si su moneda virtual es convertible, debido a que el juego consiste en múltiples jugadores que se constituyen en el mundo virtual a través de su avatar combatiendo contra monstruos y otro jugador, al ganar la batallas, el jugador va acumulado "oro" que en teoría se usa para el comercio de bienes de consumo. Dentro del mundo virtual existe la posibilidad de que un jugador le venda su "oro" a otro jugador a cambio de dinero fiat, físico, de libre circulación, dando lugar así a un mercado negro de venta de "oro" virtual a otros jugadores, para enriquecer sus arcas y así disponer de más bienes dentro del juego a cambio de dólares físicos. Es en este punto, donde inicia el laberinto para las administraciones tributarias en cuanto al dinero virtual, debido a que es imposible gravar ese ingreso percibido por el jugador que vendió su "oro" a otro.

La moneda virtual convertible tiene un valor equivalente en moneda real y puede ser intercambiada una y otra vez por dinero real. Algunos ejemplos incluyen: Bitcoin, e-Gold (fuera de uso), Liberty Reserve (fuera de uso), Second Life Linden Dollars, y WebMoney10.

Monedas virtuales centralizadas vs descentralizadas.

Las monedas virtuales centralizadas dependen exclusivamente de una autoridad administrativa, es decir un intermediario que controla el sistema. El intermediario emite la moneda y establece los parámetros para poder utilizarla, mantiene un registro contable central

de pago y tiene potestad para cambiar la moneda, el administrador también puede fijar la tasa del cambio de la moneda virtual, o según el valor establecido en dinero real o su respaldo en cualquier reserva de valor del mundo real como el oro.

Las monedas virtuales descentralizadas (también conocidas como criptomonedas), son monedas virtuales de código abierto, fundamentadas matemáticamente, que funcionan en una red de pares distribuida, sin autoridad central administradora, de vigilancia o de supervisión. Son ejemplos de ellas el Bitcoin, LiteCoin y Ethereum. Estamos frente a una criptomoneda cuando nos encontramos ante una moneda digital que reúne las características de convertible y descentralizada. Podemos definir la criptomoneda como una moneda virtual cimentada sobre un algoritmo matemático que está protegida a través de la encriptación. De esta forma, los principios de la criptografía establecen un nuevo modelo económico de la información segura, descentralizada y compartida. Las criptomonedas se apoyan en las llaves públicas y privadas para traspasar valor de una persona a otra y deben contener una firma criptográfica cada vez que se realiza una transacción.

Bitcoin y Altcoin.

Es prácticamente imposible hablar de aspectos de las criptomonedas sin referirse al bitcoin, la más famosa de ellas en la actualidad. La historia de las criptodivisas lleva apenas un par de años; en 1998 un activista informático que se hace llamar Wei Dai público en la lista de correo electrónico Cypherpunks una propuesta sobre un sistema de intercambio de valor y ejecución de contratos basados en una moneda irrastreable a la que llamo B-money. En 2008, el registro del nombre de dominio www.bitcoin.com fue hecho a nombre de "Satochi Nakamoto" y aún no está claro si se trató de un sujeto o una entidad anónima.

Aunque muchas personas creen que el bitcoin fue lanzado en algún momento durante los últimos cinco o seis años, en realidad se comenzó a generar los primeros bitcoins a principios del 2009 y a partir de entonces fueron efectuadas las primeras transacciones.
Podemos decir que los bitcoins son monedas virtuales cuyas unidades de cuenta están compuestas por bits de ordenamiento alfanumérico exclusivas, y su valor está sujeto a la confianza entre los usuarios que están dispuesto a comprar bitcoins en el mercado. Una de las principales características de las criptomonedas, es su alto grado de comercialización bajo anonimato y que son convertibles en dinero fiat (dólares, euros, francos, yuan, etc.).

Los factores disruptivos del bitcoin y demás criptomonedas generan un dolor de cabeza a las administraciones tributarias, debido a que el usuario almacena las criptomonedas en una billetera electrónica que únicamente es identificada con un código; algo así como versiones virtuales de las cuentas bancarias cifradas que fueron tan populares en algunas jurisdicciones hasta finales de siglo pasado. Por este motivo, no se puede saber la verdadera identidad del usuario final.

Las demás criptomonedas descentralizadas y convertibles en dinero fiat son conocidas como "Altcoin" y tienen un fundamento matemático distinto al del bitcoin. Algunos de los ejemplos de Altcoin más dignos de mención son Litecoin, Monero, Ethereum, Zerocoin, Dogecoin. En la actualidad existen más de mil criptomonedas distintas.

El blockchain y la contabilidad de triple partida.

El blockchain es una tecnología que indiscutiblemente ha llegado para quedarse, y además sirve como base para los procesos del futuro. Gracias a ella, el actual internet de la información alcanzara un nuevo paso evolutivo, denominado el internet del valor.

Este registro contable público, denominado blockchain, está distribuido entre diferentes participantes, organizado matemáticamente en bloques de transacciones entre sí que están protegidos criptográficamente. En otras palabras, es una base de datos descentralizada que no puede ser alterada, ni vulnerada por ciberdelincuentes. A través del blockchain, aun las partes que no confían plenamente en otras pueden mantener un acuerdo sobre la existencia, el estado y evolución de una serie de información compartida. El consenso es la clave del blockchain, porque permite que todos los participantes puedan confiar en la información grabada en el sistema.

En términos contables el blockchain se asemeja a un diario donde se registran en orden cronológico las transacciones de compra y venta de criptomonedas. En cada bloque, que no puede ser mayor a 1 megabyte, caben aproximadamente dos mil transacciones, su lenguaje es el formato de texto (txt.) y cada transacción y contenido del bloque está protegido por un algoritmo criptográfico alfanumérico muy difícil de descifrar, denominado "hash".

Existe un debate histórico entre los estudiosos de la contabilidad, acerca de quién fue el inventor de la doble partida. Por un lado prevalece la teoría de que el primer inventor fue Benedetto Cotrugli; otros se la atribuyen a Fray Luca Pacioli. Sin duda este último es el más popular en los libros de historia de la contabilidad. La doble partida es un sistema para registrar las operaciones, de forma que cada partida asentada en el "debe" tenga su propia contrapartida en el "haber". Han pasado más de 500 años desde su origen y esta técnica contable aún se encuentra en uso.

Con la llegada del blockchain, el sistema contable de doble partida podría quedar obsoleto y pasar a un sistema de triple partida. En este entorno, los negocios actuales necesitan una manera diferente de obtener a la confianza y la liquidez de los proveedores que requieren para progresar.

Desde el segmento de la tecnología contable, una de las soluciones es la contabilidad de triple entrada, que inicio a finales de los 80 y se ha actualizado para hacer realidad un modelo contable en el que todas las anotaciones que involucran a terceras partes estén selladas criptográficamente y verificadas por una tercera entrada. De esta forma, cualquier transacción registrada, tanto una factura como un pedido, es una transacción real con una expectativa real de pago. Es pocas palabras, la contabilidad de triple partida quedaría compuesta de la siguiente forma: "debe", "haber" y el algoritmo criptográfico que tiene que ser validado por un grupo de usuarios llamados comúnmente "mineros", para acreditar la transacción y proteger la integridad de los valores sin que sean modificados o maquillados.

Los retos de las administraciones tributarias ante las criptomonedas.

Sin duda alguna, en la actualidad el tema de la economía digital en general y especialmente las criptomonedas, representa un problema para las administraciones tributarias de los diferentes países. Basta con imaginar que existan monedas virtuales cuyo único respaldo es la confianza de los usuarios, con un valor que fluctúa las 24 horas del día, que puedan ser convertidas en dinero fiat y que el poseedor de estas criptomonedas no pueda ser identificado, debido a que están almacenadas en una billetera electrónica acreditada mediante un código de usuario. La combinación de estas características convierte la recaudación de los tributos por parte del Estado en un complejo desafío.

A través de las herramientas de la economía digital y aceptando las criptomonedas como medio de pago, el contribuyente puede llegar a generar ingresos prácticamente ilimitados mediante la compra o venta de criptoactivos y aumentar así su patrimonio sin verse en necesidad de declararlo ante la administración tributaria.

Colateralmente, la emisión de criptomonedas puede generar otros problemas. Por ejemplo, en materia económica, tenemos la inflación, debido a que la susceptibilidad de la criptomoneda de ser convertible en dinero fiat, automáticamente se traduce en un incremento de flujo de efectivo en el mercado, creando una distorsión. En este sentido, criptomonedas como Ethereum, cuya emisión es ilimitada y su valor no tiene ningún respaldo, podrían representar un aumento en la especulación y el poder adquisitivo de sus usuarios.

La debilidad imperativa en cuanto a la declaración de las rentas obtenidas en criptomonedas parece haber tendido un espeso manto de complejidad sobre la tributación que le corresponde. La naturaleza del mercado, unida a su volatilidad, dificulta la creación de procedimientos claros en la presentación de declaraciones de tributos.

La Acción 1 de BEPS, los precios de transferencia y los criptoactivos

La implementación de las acciones del plan BEPS (Base Erotion and Profit Shifting, por sus siglas en inglés) es ya ampliamente conocida. Los países del G20 habían observado que gran parte de la elusión en materia de tributación internacional se consolido en la economía digital junto al comercio electrónico. Por medio de la acción del plan BEPS, esos países trataron de llenar las lagunas que dejan las diferentes actividades que realizan las empresas multinacionales (EMN) al momento de transferir costos y gastos por medio de la economía digital, a jurisdicciones con menor carga impositiva como método de erosión de su base imponible.

La principal recomendación de la acción 1 del plan BEPS, es la modificación del concepto de establecimiento permanente (EP). Podemos encontrar una definición precisa de establecimiento permanente dentro de la cláusula general de EP en el artículo 5.1 del Modelo de Convenio de Doble Imposición (MDCI) de la OCDE y que señala lo siguiente: (www.gerens.cl, 2010) *"Lugar fijo de negocios en que una empresa efectúa toda o parte de su actividad"* en ella también se encuentran recogidos los presupuestos fundamentales que deben contener la figura de

EP los cuales son: la existencia de un lugar de negocios, el lugar de negocios debe ser fijo y que se realice la actividad de la empresa a través de dicho negocio.

A simple vista se podría deducir que la principal característica del establecimiento permanente es que debe contar con un lugar fijo de negocios. Sin embargo, si lo tratamos de comprender en el contexto de las empresas que comercializan criptoactivos, podríamos enfrentar limitaciones para identificar su verdadero lugar de negocios, ya que casi ninguna tiene un establecimiento fijo, sino que efectúan la compra, venta, minería y almacenamiento de criptomonedas a través de facilidades que se ofrecen totalmente en línea, sin la necesidad de un establecimiento físico consolidado.

Un ejemplo de esto podría ser una empresa que ejecute una oferta inicial de monedas (ICO, por sus siglas en ingles) que no es más que un evento en el que un proyecto basado en blockchain vende una serie de tokens (criptoactivos generados mediante transacciones en línea) a los primeros usuarios, a cambio de otras criptomonedas.

Esto significa que un proyecto blockchain puede ofrecer a los inversores algunas unidades de una nueva criptomoneda o token a cambio de otras criptomonedas más conocidas, como pueden ser Bitcoin o Ethereum. En pocas palabras, a través de las ICO se puede colocar ofertas públicas de nuevas criptomonedas en el mercado, en forma semejante a lo que hacen las compañías que realizan ofertas públicas de adquisición (OPA) en el sector de valores.

En cuanto al reconocimiento del establecimiento permanente de las empresas que realicen operaciones comerciales a través de plataformas de comercio electrónico, economía digital y manejo de criptoactivos, se podría incluir una exigencia dentro de las modificaciones del concepto de EP sugerido por la acción 1 del Plan BEPS, que requiera acreditar la propiedad del nombre de dominio bajo el que llevan a cabo su actividad comercial digital en la Internet, mediante una constancia otorgada a través de un protocolo de consulta para consultar bases de datos de los titulares registrados de los nombres de dominio y de la correspondiente dirección IP, como el Whois de la Internet Corporation for Assigned Names and Numbers (ICANN, por sus siglas en ingles).

ICANN es la organización encargada del gobierno del internet y su principal función es asignar las direcciones de protocolo de internet (IP) e identificar y gestionar las funciones del sistema de nombres de dominio y la administración de servidores de raíz.

Otro reto significativo para las administraciones tributarias radica en el análisis de estudios de precios de transferencia cuando se trata de empresas que realizan el intercambio de criptomonedas con su parte relacionada en el extranjero. Como sabemos, los precios de transferencia están regidos por el principio de libre competencia y su definición la podemos encontrar en el artículo 764-A del Código Fiscal que establece lo siguiente:

> *"El principio de libre competencia. Las operaciones que realicen los contribuyentes con partes relacionadas deberán valorarse de acuerdo con el principio de libre competencia, es decir, los ingresos ordinarios y extraordinarios y los costos y deducciones necesarios para realizar esas operaciones, deberán determinarse considerando el precio o monto que*

habrían acordado partes independientes bajo circunstancias similares en condiciones de libre competencia. El valor así determinado, deberá reflejarse para fines fiscales en las declaraciones de rentas que presente el contribuyente, siguiendo para ello la metodología establecida en los artículos contenidos en este Capítulo."

Aplicar el precitado principio a un análisis de estudio de precios de transferencia cuando una empresa transfiere criptomonedas a su parte relacionada, es sumamente difícil, debido a que los criptoactivos, son una tecnología disruptiva y no tienen antecedentes, el valor de la criptomoneda está respaldado por la confianza de la gente y no tienen agencias que puedan calificar, por ejemplo, si el producto tiene grado de inversión. El mercado de las criptomonedas es sumamente volátil, su valor fluctúa a cada minuto y funciona las 24 horas del día, a diferencia del mercado de capitales. Por último, existen más de mil tipos de criptomonedas y ninguna es comprable con otra en su valor, por ende, se hace muy difícil aplicar los métodos de comparación establecidos en el artículo 762-F del Código Fiscal, ya sea por métodos relacionados a precios no controlados, método de costo adicionado, método de precio de reventa, método de partición de utilidades y método de margen neto de la transacción.

La OCDE y su preocupación sobre las criptomonedas.

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) no estaba ajena a las limitaciones y desafíos que suponen los criptoactivos en materia tributaria y este ano presento ante el G20 en la ciudad Buenos Aires, Argentina, un informe que pretende regularlos. El documento aborda el impacto de la digitalización en la política tributaria y la administración tributaria. Por un lado, afirma que el uso de las criptomonedas representa un alto riesgo para la trasparencia tributaria que se ha logrado alcanzar en los últimos anos y, por otra parte, aconseja a los Estados adscritos al G20 el uso de tecnologías basadas en blockchain, debido a que constituyen un método más seguro de registro contable. Sin embargo, al final de la reunión, los diferentes ministros de finanzas de los Estados miembros de esa organización concluyeron sin resoluciones definitivas.

CONCLUSIÓN

Una frase muy trillada, de Benjamín Franklin, conocida por estudiosos y profesionales de la tributación dice que "en este mundo solo hay dos cosas seguras: la muerte y pagar impuestos".

No importa el tipo de gobierno que se tenga, sea una república o una monarquía, una democracia o una dictadura, cuyo sistema sea capitalista o socialista, en principio, todo ciudadano está obligado a pagar impuestos, a excepción de los de Corea del Norte, debido a que a través del artículo 25 de su Constitución el Estado abolió los impuestos y se responsabilizó de asegurar a todos los trabajadores condiciones plenas para la alimentación, el vestido y la vivienda.

Aunque a los ciudadanos de muchos otros países les gustaría habitar en un mundo libre de impuestos y así poder acumular más capital, la recaudación tributaria se remonta a los

tiempos bíblicos; tanto así que, en la Santa Biblia, en el Nuevo Testamento, Lucas 15:1 relata lo siguiente:

> *"Mientras Jesús enseñaba, se le acercaron muchos de los que cobraban impuestos para el gobierno de Roma, y también otras personas a quienes los fariseos consideraban gente de mala fama."*

Es decir, los recaudadores de impuestos, a través de los siglos han cobrado el precio por vivir en sociedad, aunque desde el principio hayan sido mal vistos por la población. El desarrollo de la civilización y, en especial, los avances tecnológicos alcanzados con el paso del tiempo, no deben ser obstáculo para la recaudación sino que, al contrario, la administración tributaria debe servirse de la tecnología para ser más eficaz al momento de ejercer su actividad.

En la actualidad es muy hacer cumplir el pago de impuestos directos a los contribuyentes que generan ingresos por medio de criptoactivos; sin embargo el reconocimiento y legalización de las criptomonedas como una divisa digital de curso legal podría ofrecer una vía para facilitar el inicio de la recaudación de impuestos indirectos, específicamente el ITBMS, a las transacciones de compra y venta de bienes y servicios que utilicen plataformas de pagos que acepten criptomonedas. Es decir que se decida comprar un artículo por internet y esa tienda virtual acepte pagos en criptomonedas, la empresa debería emitir una factura donde aplique el principio de discriminación de ITBMS por la compra del producto y se aplique el ITBMS sobre la base imponible del costo de mercancía en dinero fiat y la persona jurídica o natural que devengue ese ingreso se convierta en agente de retención del ITBMS; es más sencillo detectar a los comercios electrónicos que aceptan pagos con criptomonedas, debido a que estos siempre los tienen anunciado en su página web, ese sería el primer punto para iniciar la fiscalización.

Comprendemos que, día a día la tecnología avanza y es imposible que las normas y el derecho evolucionen al mismo ritmo que ella. Sin embargo, no debemos quedarnos rezagados y aprovechar la tecnología para ser más eficientes y productivos en nuestras funciones.

Bibliografía

Cantwell, F. P. (2017). *Los Derechos de Internet.* México: Editorial Flores.

Fernández, F. B. (2017). *Bitcoin: La Tecnología Blockchain y su investigación.* Madrid: OxWord

Computing S.L.

Navarro, S. N. (2016). *Mercado digital, principios y reglas jurídicas.* Valencia: Tirant Lo Blanch.

Preuskchat, A. (2017). *BLOCKCHAIN: La Revolución Industrial del Internet.* Barcelona: Gestión

2000.

Pujol, J. M. (2017). *Código Fiscal de la República de Panamá.* Panamá: Mizrachi & Pujol, S.A.

Velásquez, D. O. (2014). *Derecho Tributario: consideraciones y aplicación del concepto de establecimiento permanente.* Bogotá: Grupo Editorial Ibáñez. *www.fatf-gafi.org*. (junio de 2015). Obtenido de http://www.fatfgafi.

org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf
www.gerens.cl. (2010). Obtenido de http://www.gerens.cl/gerens/ModeloConvenioTributario.pdf
www.icann.org. (s. f.). Obtenido de https://www.icann.org/resources/pages/what-2012-02-25-es
www.oecd,org. (2018). Obtenido de http://www.oecd.org/ctp/OECD-Secretary-General-taxreport-
G20-Finance-Ministers-Argentina-March-2018.pdf
www.oecd.org. (2015). Obtenido de https://www.oecd.org/ctp/beps-nota-explicativa-2015.pdf

APLICACIÓN MÓVIL, HERRAMIENTA AUXILIAR EN EL PROCESO ELECTORAL MEXICANO

Por: ***Karen Flores Maciel***
México

Hoy en día, la tecnología ha dejado de ser sólo una herramienta para convertirse en un eje de organización social. Siendo internet un novedoso instrumento para la transformación y desarrollo de un país en el terreno de lo económico, cultural y social, así como en el ámbito institucional de la democracia, y ha servido como herramienta para el ejercicio de los derechos de participación ciudadana.

Así pues, vemos como la tecnología que en un inicio nos ayudó a modificar nuestra forma de trabajo y producción, hoy se transforma para estar presente en nuestra vida diaria, interactuando directamente con nosotros, creando una red social a través del uso de nuevas tecnologías y las tecnologías de la información y comunicación (TIC's), las cuales traen consigo un nuevo orden social, llamado ciberespacio, del cual una comunidad cada vez más amplia forma parte, por lo que el gobierno, sus instituciones, los partidos políticos y la propia ciudadanía, no pueden desvincularse.

Las TIC's hoy día han permitido modificar la comunicación política e interacción entre gobiernos y ciudadanos, se vive en un mundo donde nada es secreto, todo se comunica y todo es discutible; así, el ciudadano de la mano con las herramientas tecnológicas existentes, puede contar con una participación activa en la vida democrática de un Estado.

De tal suerte, en el presente trabajo, se pretenderé flejar una nueva forma de participación ciudadana, derivada de la creación de una Aplicación móvil (App), desarrollada por el Instituto Nacional Electoral, para la captación del apoyo ciudadano para los aspirantes a contender por la vía independiente en el proceso electoral mexicano 2017-2018.

2. LA PARTICIPACIÓN CIUDADANA EN EL PROCESO ELECTORAL MEXICANO 2017-2018

Uno de los aspectos relevante en la utilización de los avances tecnológico encaminados a la búsqueda de una efectiva democracia, es el tema de la participación ciudadana, entendida esta como el conjunto de acciones o iniciativas que pretenden impulsar la democracia participativa, a través de la integración de la comunidad al ejercicio de la política, mediante mecanismos donde la ciudadanía tenga acceso a las decisiones de gobierno de manera independiente[1].

La participación ciudadana es un derecho y una obligación de las personas, que busca el bien común, en donde la era digital nos da la oportunidad de ejercer este derecho mediante el uso de las nuevas tecnologías, fortaleciendo el Estado democrático del cual formamos parte.

[1] EcuRed [en línea]. [Consulta: 29-5-2018]. Disponible en: https://www.ecured.cu/Participaci%C3%B3n_ciudadana

Como bien lo refiere Karl W. Deutsch, las democracias son superiores a todo otro sistema político. Lo son porque permiten que la opinión pública sea una instancia crítica que obliga al sistema social y político a un permanente aprendizaje. Los sistemas políticos únicamente son capaces de corregir sus defectos en la medida en que exista un adecuado funcionamiento de la opinión pública[2].

Internet ha venido a facilitar la participación ciudadana, –al menos en los países más desarrollados-, hoy ya existen los medios técnicos, para dotar a cada domicilio de dicha herramienta tecnológica, de modo que cada ciudadano puede expresar instantáneamente, desde su pantalla del ordenador o dispositivos móviles, su punto de vista sobre las cuestiones que se sometan a su elección o sobre las que se recabe su opinión, optando a favor o en contra de ellas[3]. En ese sentido, las Apps móviles, han jugado un papel muy importante para la participación activa de la ciudadanía en la toma de decisiones de un Estado.

Debe entenderse por Apps los programas dirigidos fundamentalmente a Smartphones y tabletas y caracterizados por ser útiles, dinámicos, fáciles de instalar y sencillos de manejar, algunas de ellas dependen de Internet para funcionar[4]. Así pues, el auge de las aplicaciones en un mundo cada vez móvil, es una gran historia social, política y económica que (…) hemos estado documentando desde hace años[5].

Por lo que, algunos mecanismos de la democracia directa se han visto fortalecidos por el uso de las Apps, sobre todo en sociedades con una densidad demográfica grande, en las que resulta más complejo acercar a los ciudadanos en la toma de decisiones de públicas.

Peces-Barba hace énfasis a la relación trascendental de la democracia y la ciudadanía al referir que: "No hay verdadera democracia sin suficiente participación de los ciudadanos, ni los individuos son considerados ciudadanos si no es en un régimen democrático".[6]

Hoy como nunca, gracias a la era digital, es posible que exista una sociedad civil más organizada, que participe para exigir políticas públicas, mejores funcionarios, intervención del gobierno en acciones para su comunidad o para tomar consciencia de los candidatos y partidos políticos, así como respaldar a un ciudadano que pretenda participar en la vida política de un Estado.

El 1º de julio 2018, se vivió la elección más grande de la historia de México, con más de 3,400 cargos de elección popular en disputa, entre ellos, se eligió al Presidente de la

---

[2] DEUTSCH, K. *The Nerves of Government; Models of Political Comunication and Control*, Nueva York: Kindle edition, 2009.
[3] PÉREZ LUÑO, A. *Los Derechos Humanos en la Sociedad Tecnológica*, Madrid: Editorial Universitas, S.A., 2012, p. 52.
[4] PEÑA GALAVIZ, J. Tlatemoani Revista Académica de Investigación [en línea]. [Consultada: 31-5-2018]. Disponible en: http://www.eumed.net/rev/tlatemoani/15/tecnologia-educacion.html
[5] CARRAZO BARRANTES, C. *El nuevo contexto de las campañas electorales: El caso del App Mivotohoy.* Pew Reseach Center, 2015
[6] PECES-BARBA, G., *Educación para la ciudadanía y derechos humanos*, Madrid: Grupo Edebé, 2007, p. 240.

República quien estará en el cargo de 2018 a 2024, se renovó el Congreso de la Unión, con 500 Diputados y 218 Senadores; ocho gubernaturas y la jefatura de gobierno de la Ciudad de México, diversas diputaciones locales, alcaldías, concejales, regidores, integrantes de las juntas municipales y sindicaturas. Cargos de elección popular que fueron votados por cerca de 45 millones de mexicanos, es decir, que cerca del el 66% del Padrón Electoral Mexicano (el cual se conforma por 89 millones de ciudadanos) participó en dichos comicios.

En ese sentido, la organización de la elección 2018, llevó implícito un gran trabajo por parte de las autoridades administrativas electorales, como lo son: el Instituto Nacional Electoral (INE), y los Organismos Públicos Locales (OPLES) de cada entidad federativa, en atención lo mandatado en el artículo 41, base V, de la Constitución Política de los Estados Unidos Mexicanos.

Cabe señalar que desde el 2014 es posible que cualquier ciudadano pueda registrar una candidatura sin el respaldo de partidos, bajo la figura de una candidatura independiente. Sin embargo, para que pueda aparecer en la boleta, es necesario que cuente con los apoyos ciudadanos suficientes.

En ese sentido, resulta incuestionable el hecho de que actualmente, la tecnología juegue un papel muy importante en el desarrollo de una sociedad, pues la misma ha venido a simplificar y transformar diversas actividades como es el caso de lo relacionado con el ámbito electoral y la participación ciudadana.

Por lo que, en el presente proceso electoral que se vivió en México, tanto actores políticos, como autoridades electorales y la misma ciudadanía interesada en estos tópicos, se posicionaron a través del uso de herramientas tecnológicas, ya sea a través de las redes sociales, o la creación de aplicaciones para propiciar una interacción entre estos y el conglomerado social común.

3. APLICACIÓN MÓVIL, PARA RECABAR EL APOYO CIUDADANO DE UN ASPIRANTE A CONTENDER POR LA VÍA INDEPENDIENTE A UN CARGO DE ELECCIÓN POPULAR EN MÉXICO

En México, la Constitución Federal reconoce como uno de los derechos de todo ciudadano, el poder ser votado para cargos de elección popular; por lo que, el derecho de solicitar el registro de candidatos ante la autoridad electoral, corresponde a los partidos políticos, así como a los ciudadanos que soliciten su registro de manera independiente y cumplan con los requisitos, condiciones y términos que determine la legislación[7].

En ese sentido, la ley secundaria en materia electoral, define como *candidato independiente*: el ciudadano que obtenga por parte de la autoridad electoral el acuerdo de registro, habiendo cumplido los requisitos de ley[8]. Dentro del mismo cuerpo normativo, se señala que los ciudadanos que cumplan tales requisitos, condiciones y términos, tendrán derecho a

[7] Constitución Política de los Estados Unidos Mexicanos, Artículo 35, fracción II.
[8] Ley General de Instituciones y Procedimientos Electorales, Artículo 3, párrafo 1, inciso c).

participar y, en su caso, a ser registrados como candidatos independientes para ocupar los cargos de: Presidente de los Estados Unidos Mexicanos, Diputados y Senadores del Congreso de la Unión por el principio de mayoría relativa[9].

Así, el proceso de selección de candidaturas independientes en México, comprende las etapas de: convocatoria; actos previos al registro de candidatos independientes, obtención de apoyo ciudadano; y, registro de candidatos independientes[10].

Por lo que, una vez emitida la convocatoria por parte del Consejo General del Instituto Nacional Electoral, dirigida a los ciudadanos interesados en postularse como independientes, éstos deberán hacerlo del conocimiento de dicha autoridad, adquiriendo la calidad de aspirantes.

Al día siguiente en que se obtenga la calidad de aspirante, es que dichos ciudadanos podrán realizar actos tendentes a recabar el porcentaje de apoyo ciudadano requerido, los cuales podrán consistir en: reuniones públicas, asambleas, marchas y toda aquella actividad dirigida a la ciudanía en general, con el objeto de obtener dicho respaldo.

Siendo la etapa de *obtención de apoyo ciudadano*, sobre las que nos abocaremos en el presente apartado. El apoyo ciudadano, se acredita ante el Instituto Nacional Electoral, mediante una cédula de respaldo que contendrá: el nombre, firma y clave de elector o el número identificador al reverso de la credencial de elector derivado del reconocimiento óptico de caracteres (OCR) de la credencial para votar con fotografía vigente de cada uno de los ciudadanos que manifiestan el apoyo en el porcentaje requerido[11], así como copia de las credencial para votar vigente de quienes respalden la candidatura.

Destacando que, para tal efecto, el Reglamento de Elecciones, establece que el procedimiento técnico-jurídico para verificar que se haya reunido el porcentaje de apoyo ciudadano requerido, según el tipo de elección de que se trate, será el que se establezca en los Lineamientos aprobados para tal efecto, en el que *se priorizará la utilización de medidas tecnológicas avanzadas* al alcance del Instituto Nacional Electoral; ello, con la finalidad de dotar de certeza el proceso de verificación[12].

En ese sentido, durante la preparación de las elecciones en México, el Instituto Nacional Electoral, lanzó una aplicación móvil (App) para recabar dicho apoyo ciudadano, desarrollada por el Grupo Tecno, la cual tuvo un costo aproximado de 4.6 millones de pesos[13].

Por lo que, en fecha 28 de agosto de 2017, emitió Acuerdo General de clave INE/CG387/2017, mediante el cual se aprobaron los "Lineamientos para la verificación del

---

[9] Ley General de Instituciones y Procedimientos Electorales, Artículo 362, párrafo 1, incisos a) y b).
[10] Ley General de Instituciones y Procedimientos Electorales, Artículo 366, párrafo 1, incisos a) y b).
[11] Ley General de Instituciones y Procedimientos Electorales, Artículo 383, párrafo1, inciso c), fracción VI.
[12] Reglamento de Elecciones, Artículo 290, párrafo 1.
[13] Expansión en alianza con CNN [en línea]. [Consultada: 15-6-2018]. Disponible en: https://expansion.mx/tecnologia/2017/10/31/la-apuesta-del-ine-por-apps?internal_source=RELATED_ARTICLE

porcentaje de apoyo ciudadano que se requiere para el registro de candidaturas independientes a cargos federales de elección popular para el proceso electoral federal 2017-2018".

De la exposición de motivos de dicho acuerdo, se desprende que, con la implementación de la aplicación móvil, los aspirantes a candidaturas independientes podrán recabar la información de las personas que respalden su candidatura, sin la utilización de papel para la elaboración de cédulas de respaldo o para fotocopiar la credencial para votar, siendo esta la manera en la que anteriormente se recopilaba el apoyo en comento.

Por lo tanto, esta nueva herramienta se presenta como una solución tecnológica, desarrollada por el INE, la cual permite conocer a la brevedad el número de apoyos ciudadanos recibidos por cada aspirante, otorgando a la autoridad, certeza respecto a que el apoyo ciudadano es auténtico, aunado a que con la implementación de dicha App móvil, se evita el error humano en el procedimiento de captura de la información, además de que la misma garantiza la protección de datos personales de quienes respaldan alguna propuesta política que pretenda contender por la vía independiente en alguna elección, aunado al hecho de reducir los tiempos para la verificación del porcentaje de apoyo, situación que compete a la autoridad administrativa electoral referenciada.

La aplicación móvil, es compatible con Smartphone de gama media y alta, así como con tabletas que funcionen con los sistemas operativos *iOS* 8.0 y *Android* 5.0 en adelante.

Conforme a los Lineamientos[14], los pasos a seguir -de manera general- para el uso de la aplicación de referencia, son los siguientes:

1) El aspirante debe acudir a las oficinas del INE con su documentación para ser registrado.
2) La autoridad electoral, registra al aspirante en el Portal Web y le envían los datos para acceder al portal de la App.
3) El aspirante accede al Portal Web para registrar a sus auxiliares y/o gestores, o en su caso, darlos de baja.
4) El auxiliar y/o gestor descarga la App -en su celular o tableta- e ingresa los datos para acceder a la misma, generando un usuario y contraseña.
5) El auxiliar y/o gestor realiza la captación de apoyo ciudadano para el proceso electoral correspondiente, generando en cada ocasión un folio único, para lo cual:
    - Debe ingresar a la App móvil con su clave de usuario y contraseña.
    - Capturar el anverso y reverso de la credencial para votar del ciudadano.

[14] Lineamientos para la verificación del porcentaje de apoyo ciudadano que se requiere para el registro de candidaturas independientes a cargos federales de elección popular para el proceso electoral federal 2018-2018 [en línea]. [Consultados: 15-6-2018]. Disponible en: http://www.ine.mx/wp-content/uploads/2017/09/ANEXO-1-CG387-17.pdf

- El sistema realiza un proceso de reconocimiento óptico de caracteres y verifica los datos del ciudadano; una vez hecho lo anterior, el sistema elabora un formulario que contiene los datos capturados.
- El auxiliar y/o gestor verifica los datos del ciudadano, pudiendo realizar correcciones -de ser el caso-, cuando los datos del formulario no sean coincidentes con los contenidos en la credencial para votar.
- El auxiliar y/o gestor tomará una fotografía al ciudadano, siempre y cuando cuente con la autorización de éste, y le solicitará firme en la pantalla del dispositivo móvil.
- Acto seguido, se deberá proceder al cifrado de los datos obtenidos y al envío de la información.

6) El INE recibe la información, descifra, clasifica y almacena en la base de datos para su procesamiento.
7) Se envía la notificación de recepción al dispositivo móvil y se elimina la información captada en éste.
8) El solicitante puede consultar su avance de captura en el Portal Web (el resultado de dicha verificación se verá reflejada a más tardar dentro de los tres días siguientes a la recepción de la información en el servidor).

Ahora bien, el Instituto Nacional Electoral, al emitir los Lineamientos de referencia, determinó que los dispositivos móviles (celulares o tabletas) no serían proporcionados a los aspirantes por parte de dicha autoridad, toda vez que el número de equipos resulta proporcional a la cantidad de auxiliares y/o gestores que colaboren con el aspirante en la captura del apoyo ciudadano.

Cabe señalar que, el acuerdo emitido por el INE -que dio origen a los Lineamientos multicitados, y con estos la autorización para la App móvil-, fue impugnado ante la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación, por diversos actores, integrándose el juicio ciudadano de clave SUP-JDC-841/2017, en donde -sustancialmente- se controvirtió la utilización de medidas tecnológicas avanzadas, considerando la utilización de la App como un requisito adicional impuesto a los aspirantes que pretendan contender con carácter de independiente a un cargo de elección popular, para recabar el apoyo ciudadano correspondiente.

El juicio en comento, se resolvió en fecha 25 de septiembre de 2017, en donde la Sala Superior del Tribunal Electoral, confirmó el acuerdo impugnado, considerando que la App móvil es constitucional, puesto que no es un requisito adicional o injustificado para los aspirantes, pues ésta se trata de un mecanismos que simplifica de manera importante la obtención de apoyo ciudadano, y los datos recabados a través de la misma, únicamente sustituyen la forma tradicional de recolección de las cédulas de respaldo (en papel) y la copia de las credenciales para votar exigidas por la ley de la materia; mismos que ya no resultan necesarios ser presentados mediante documentos físicos, ya que los archivos digitales los sustituyen.

En ese mismo sentido, la Sala Superior, consideró la validez del uso de los avances tecnológicos disponibles, como lo es la App móvil, para dotar de mayor agilidad y certeza la obtención, resguardo y verificación de los apoyos que se emitan a favor de quien aspira a una candidatura independiente. Por lo que, se estimó que la App, contaba con un fin legítimo, el cual consistía en facilitar a los aspirantes a candidatos independientes la acreditación del número o porcentaje exigido por la ley -en atención al cargo a contender- de cédulas de respaldo ciudadano[15].

Así pues, en esta ocasión se optó por el uso de tecnología generalizada, con la intención de simplificar la tarea impuesta a quienes pretendan postularse por la vía independiente, auxiliándose, en todo momento, de las personas que consideren pertinente.

De igual modo, la autoridad jurisdiccional precisó que dicha medida constituye una posibilidad real y objetiva de ejercer el derecho fundamental de ser votado, tomando como referencia el uso de manera general por parte de la ciudadanía de los teléfonos celulares e internet, puesto que los mismos han facilitado la comunicación, así como la forma en que se realizan diversos actos por medio del uso de aplicaciones[16].

Por lo que, dicha aplicación fue utilizada por primera ocasión para recabar el apoyo ciudadano de quienes pretendían contender de manera independiente, durante el presente proceso electoral federal 2017-2018 en México; teniendo la facultad cada organismos públicos local, quien -como ya se señaló- es la autoridad encargada de organizar las elecciones en las entidades federativas del país, de implementar el uso de la App móvil multicitada.

Ahora bien, lo señalado con anterioridad es una descripción de lo contenido en los documentos oficiales que sirvieron a las autoridades electorales -tanto administrativa como jurisdiccional- para implementar y validar, correspondientemente, la aplicación en comento.

En ese sentido, y por lo que hace únicamente a las elecciones federales, la tarea de los aspirantes al cargo de Presidente de la República (48 ciudadanos, que manifestaron su intención de contender en el presente proceso electoral), consistió en presentar un apoyo ciudadano con la firma de una cantidad de ciudadanos equivalente al 1% de la lista nominal de electores con corte al 31 de agosto del año previo al de la elección, además de estar integrado por electores de por lo menos 17 entidades federativas, es decir, que sumen cuando menos el 1% de respaldos que figuren en la lista nominal de electores de cada una de ellas. Lo que se tradujo en 866,593 respaldos ciudadanos, contando con un periodo de 120 días para ello (del 09 de octubre de 2017 al 06 de febrero de 2018).

---

[15] Sentencia de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación, de clave SUP-JDC-841/2017 [en línea]. [Consultada: 18-6-2018]. Disponible en: http://www.te.gob.mx/Informacion_juridiccional/sesion_publica/ejecutoria/sentencias/SUP-JDC-0841-2017.pdf

[16] Sentencia de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación, de clave SUP-JDC-841/2017 [en línea]. [Consultada: 18-6-2018]. Disponible en: http://www.te.gob.mx/Informacion_juridiccional/sesion_publica/ejecutoria/sentencias/SUP-JDC-0841-2017.pdf

Por otro lado, para el cargo de Senador por el principio de mayoría relativa, la cédula de respaldo debía contener cuando menos la firma de una cantidad equivalente al 2% de la lista nominal de electores correspondiente a la entidad federativa de que se trate, y estar integrada por ciudadanos de por lo menos la mitad de los Distritos electorales que sumen como mínimo el 1% de los ciudadanos que figuren en la lista de electores de cada uno de ellos. Por lo que, el número de respaldo ciudadano, varió en atención a los electores registrados en los Distritos que conforman cada Estado, dicho respaldo iba desde 9,990 en el caso de Baja California Sur, hasta 228,376 para el Estado de México[17], siendo éstas las entidades con menor y mayo número de electores, respectivamente, teniendo para este supuesto un término de 90 días (del 10 de octubre al 8 de enero).

Asimismo, para el cargo de Diputados de mayoría relativa, por la vía independiente, se exigió el respaldo del 2% de la lista nominal correspondiente al Distrito electoral a contender, estando integrado por ciudadanos de por lo menos la mitad de las secciones electorales que sumen el 1% de los que se encuentran en la lista nominal de éstas. Al igual que el caso anterior, el número de respaldo ciudadano varió en atención al Distrito correspondiente, así, en el Distrito 02 de Chihuahua se requirió el respaldo de 3,726, mientras que en el Distrito 12 de Nuevo León 13,726, en un periodo de 60 días (del 05 de octubre al 04 de diciembre de 2017).

Advertido lo anterior, se tiene que, en los hechos, y durante la utilización de la App móvil, diversos medios periodísticos se pronunciaron sobre la situación que pasaban aquellos que la manejaban, se hizo notorio el disgusto de los aspirantes a alguna candidatura independiente, sobre la App, derivado de problemas operativos en su utilización durante la recolección del respaldo ciudadano, manifestando -en muchos de los casos- que las fallas en la misma, les impedía recabar 'firmas electrónicas' al ritmo necesario para conseguir las miles exigidas por la ley -en atención al cargo popular a contender-.

Por lo que, en el mes de noviembre de 2017, el Instituto Nacional Electoral se vio obligado a anunciar una actualización de su herramienta, confirmando la versión 2.0[18], la cual cuenta con cinco mejoras, a saber:

1) Mejora en el uso de la cámara, aumentando su eficiencia respecto al enfoque de la misma, para tomar los datos necesarios de las credenciales para votar.

2) Más ágil, ya que se puede capturar la información de las credenciales de manera manual, después de un solo intento de captación de datos con la cámara mediante OCR.

3) Mejor desempeño, ya que trabaja mejor con otro tipo de aplicaciones en funcionamiento como las llamadas o mensajes.

---

[17] INE/CG387/2017 Acuerdo del Consejo General del Instituto Nacional Electoral por el que se emiten los Lineamientos para la verificación del porcentaje de apoyo ciudadano que se requiere para el registro de candidaturas independientes a cargos federales de elección popular para el proceso electoral federal 2017-2018[en línea]. [Consultada: 25-6-2018]. Disponible en: https://www.ine.mx/wp-content/uploads/2017/09/CGex201708-28-ap-12.pdf

[18] Según se desprende del Manual de Auxiliar/Gestor Dispositivo con Android, correspondiente a la segunda versión de la aplicación [en línea]. [Consultada: 28-6-2018]. Disponible en http://www.ine.mx/wp-content/uploads/2017/10/Manual-de-Auxiliar_Gestor-App_Android-V-2.0_.pdf

4) Mayor seguridad, se fortalecen las validaciones en la seguridad de los dispositivos móviles, así como estabilidad.

5) Envíos más rápidos, optimizando el envío de apoyos ciudadanos aunque las condiciones de la conexión no sean las ideales.

Resultando obligatoria la actualización de la App móvil para todos los aspirantes. Ahora bien, cabe señalar que pese a los intentos de subsanar las irregularidades que presentó la App móvil de origen, lo cierto es que las quejas presentadas por diversos aspirantes ante el Instituto Nacional Electora, y hechas del conocimiento público mediante sus redes sociales, así como las impugnaciones presentadas en contra de la misma ante el Tribunal Electoral del Poder Judicial de la Federación, hicieron visible el problema, respecto a la situación que se vivía por parte de sus usuarios, principalmente auxiliares o gestores al servicio de algún simpatizante.

En ese sentido, las principales inconformidades que se suscitaros durante su uso, consistieron en que: el sistema se "caía" o no era posible acceder a éste; o que para acceder al sistema todo auxiliar o gestor, debía ser autorizado previamente por el aspirante; se destacó el acceso limitado a internet, principalmente en zonas marginadas del país, resultaba complejo la captación del respaldo ciudadano; además se señaló que la aplicación presentaba inconsistencias en dispositivos móviles de gama media, segregando a su vez a quienes contaban con un celular con características inferiores a ésta, lo que a juicio de los aspirantes disconformes, representaba una clara violación de sus derechos humanos de igualdad, discriminación y acceso a internet, y en consecuencia, se transgredió el derecho a votar y ser votado.

Solicitando: la reposición del tiempo perdido en la obtención del apoyo ciudadano respecto al periodo en que se obligó a utilizar la versión primigenia (cerca de un mes aproximadamente); o de ser el caso, la posibilidad de recolectar las firmas en formato físico/documental; así como, una auditoría externa y ampliación de información sobre el funcionamiento de la App; equipo electrónico en los módulos del Instituto Nacional Electoral para que los ciudadanos tuvieran la posibilidad de registrar ahí sus firmas a favor de los aspirantes; e incluso, se solicitó la cancelación de la aplicación móvil.

Pese a que la autoridad señaló desde la creación de la multicitada herramienta tecnológica, que previó diversos tutoriales, manuales de operación de la App, micro sitio en el portal para aspirantes y candidatos, así como la posibilidad de llamada a INETEL, y la creación de un correo electrónico específico para atender únicamente cuestiones técnicas con un apartado de preguntas frecuentes[19].

Lo cierto es que, ante dicho escenario de inconformidades por parte de los interesados, el Instituto Nacional Electoral emitió acuerdo administrativo, por el cual resolvió otorgar una

[19] Nota periodística: Descarta INE fallas en aplicación móvil para independientes. Periódico digital El Siglo de Durango. [Consulta: 02-07-2018]. Disponible en: https://www.elsiglodedurango.com.mx/noticia/913492.descarta-ine-fallas-en-aplicacion-movil-para-independientes.html

ampliación de 7 días para recabar el apoyo ciudadano, considerando que los errores presentados durante la utilización de la App móvil, forman parte de la "curva de aprendizaje"[20].

Cabe señalar, que ante la presencia de tales irregularidades señaladas por los operadores de la App móvil -con independencia de la referida actualización-, unos aspirantes optaron por transgredir las reglas establecidas para la captación del respaldo ciudadano; así, algunos unos independientes para el cargo de Presidente de la República hicieron públicos los códigos de acceso a la App (otorgados a éstos por la autoridad administrativa electoral) para poder capturar firmas.

Lo anterior, con la intención de que los ciudadanos que quisieran apoyarlos pudieran registrarse con los datos de un promotor y/o gestor del voto -dado de alta previamente por el aspirante- y capturar su propio apoyo[21]. Sin embargo, dichos códigos fueron cancelados por el Instituto Nacional Electoral.

De lo detallado con antelación, se advierte que el camino que tuvieron que recorres los aspirantes a un cargo federal de manera independiente, no fue del todo fácil para conseguir el respaldo de miles de ciudadanos, a través de la aplicación móvil implementada en estas elecciones, lo anterior se corrobora con los resultados obtenidos en el proceso electoral, en donde sólo unos poco, lograron cumplir con la meta que se fijó tanto por la norma electoral como por parte de la autoridad.

Quizás ello sea el reflejo de una mala difusión respecto al manejo colectivo de las TIC's como herramienta para la participación ciudadana, o simplemente se debió a la decisión de la sociedad, quienes no consideraron como una opción viable a las propuestas que se les presentaron para representarlos, por lo que los aspirantes no se hicieron acreedores de su respaldo.

Al respecto, se tiene que, por lo que hace al cargo de Presidente de la República, 48 ciudadanos iniciaron la captación de apoyo, y al final únicamente dos candidatos aparecieron en la boleta electoral el pasado 1 de julio en su calidad de independientes (pese a que durante el la etapa final de la campaña, una candidata desertó de la contienda electoral)[22].

En ese sentido, se contó con 55 aspirantes a senadurías al comienzo de la recaudación del apoyo, y sólo 7 de ellos, participaron en la contienda electoral. En el caso de los Diputados Federales, se contaba con 187 ciudadanos al inicio, de los cuales únicamente 40 contendieron en las elecciones pasadas[23].

---

[20] Nota periodística. Periódico digital Vanguardia [en línea]. [Consultada: 02-07-2018]. Disponible en: https://www.vanguardia.com.mx/articulo/justifica-ine-error-en-la-app-para-independientes-son-parte-de-la-curva-de-aprendizaje

[21] Nota periodística. Periódico digital Reporte Índigo [en línea]. [Consulta: 02-07-2018]. Disponible en: https://www.reporteindigo.com/reporte/burlar-al-ine/

[22] Candidaturas Independientes 2018 [en línea]. [Consulta: 06-07-2018]. Disponible en: http://www.ine.mx/candidaturasindependientes/

[23] Candidaturas Independientes 2018 [en línea]. [Consulta: 06-07-2018]. Disponible en: http://www.ine.mx/candidaturasindependientes/

Ante tales resultados, se considera que si bien, la utilización de la App móvil multicitada fue un instrumento relevante en el proceso electoral 2017-2018 que vivió México, respecto a quienes contendieron por la vía independiente, lo cierto es que se pudieran hacer algunas modificaciones a la misma para potenciar -efectivamente- el derecho de los ciudadanos de ser votados sin el respaldo de un partido político, así como el de la ciudadanía de participar dando su apoyo a quien consideren como una mejor opción de representación política.

En primer término, se hace una crítica a la aplicación, ya que aún y cuando la misma puede ser descargada por cualquier persona con un dispositivo móvil compatible con *iOS* y *Android* (gama media y alta), desafortunadamente la captación de las firmas se debe llevar a cabo por un auxiliar, autorizado previamente por el aspirante; en ese sentido, una persona que simpatiza con alguna propuesta que pretenda llegar por la vía independientes, se verá limitado a ubicar -en el mejor de los caso- a un auxiliar para que este recabe dicho apoyo; asimismo, en el caso de los ciudadanos que vivan el extranjero, tal posibilidad se ve limitada, pese a tener la posibilidad de votar si residen fuera del país.

Por lo que, lo ideal sería que cualquier persona pudiera utilizar dicha aplicación; cierto es que, el Instituto Nacional Electoral limitó esta actuación bajo el argumento de la protección de los datos sensibles que se capturan en la misma, sin embargo -y como ha quedado advertido en párrafos anteriores- al obtenerse la información de quien apoye a un aspirante, la misma debe ser remitida mediante el acceso a red o WiFi a la plataforma habilitada por el INE la cual llega de manera encriptada, así la autoridad recibe dicha información, la descifra, clasifica y almacena en la base de datos para su procesamiento, y acto seguido, se recibe una notificación de ello en el dispositivo móvil que la envió y se elimina la información captada en éste; resaltando que, la información que es recibida en dicho Instituto es cruzada con la base de datos que se creó para ese fin.

En ese sentido, la participación de la ciudadanía abiertamente, con la liberación de códigos y contraseñas por parte de la autoridad electoral, facilitaría la recaudación en menor tiempo de firmas a favor de un aspirante a candidato independiente, aunado al hecho de que los datos sensibles no se pondrían en riesgo pues la información se elimina del dispositivo móvil al momento de ser recibida por el INE.

Máxime que, en la realidad hay aspirantes que encuentran limitada su actuación en atención a los recursos con los que cuentan, ya que a diferencia de los candidatos postulados por los partidos políticos, éstos tienen un respaldo económico; mientras que, los aspirantes no tienen esta posibilidad, y algunos de los inconvenientes en esta ocasión, fue incluso el tipo de dispositivo móvil que se requería para poder ejecutar la aplicación móvil de la que hemos venido tratando en este apartado, pues los auxiliares no contaban con el modelo requerido para su ejecución.

Lo anterior, en atención al número de mexicanos que sí cuentan con acceso a internet, pues si esto es tomado en consideración, resultaría -en gran medida- beneficioso para la causa que persigue un aspirante. Cabe señalar que en México, para 2018 se estima la existencia de alrededor de 79 millones de usuarios de internet, de los cuales el 66% cuentan con edad para votar (18 años en adelante); y del universo de usuarios, el 76% cuenta con un Smartphone (7 de cada 10), y el 51% con tableta; en promedio los mexicanos pasan alrededor de 8 horas

con 11 minutos al día en internet; aunado al hecho de que el 64% de los internautas perciben que se encuentran conectados las 24 horas a internet[24].

Advertido lo anterior, es dable señalar que al tener mayor presencia el uso de internet en la vida del mexicano, le resultaría a éste -en ese supuesto- más fácil acceder a la aplicación móvil creada por el Instituto Nacional Electoral, para otorgar su respaldo a favor de un aspirante independiente, y no, que tenga que buscar a los auxiliares o que sea el aspirante quien lo busque, para la captación del mismo.

Finalmente, no debe pasar desapercibido, los contrastes sociales que se viven en México, en donde desafortunadamente existen zonas con una amplia marginación, por lo que, en los "Lineamientos para la verificación del porcentaje de apoyo ciudadano que se requiere para el registro de candidaturas independientes a cargos federales de elección popular para el proceso electoral federal 2018-2018" se contempló un régimen de excepción para poder recabar el apoyo en cédulas de papel en 283 municipios clasificados como de *muy alto grado de marginación*, conforme el índice de marginación elaborado por el Consejo Nacional de Población, con información respaldada por el Instituto Nacional de Estadística y Geografía[25]; sin embargo, debe decirse que en atención al estudio referenciado, también aquella población mexicana clasificada como de *alta marginación*, en muchas de las ocasiones cuenta con viviendas sin energía eléctrica, sin agua entubada, y con piso de tierra, y en consecuencia sería desatinado considerar que este sector tiene acceso a internet de manera libre, que le permita formar parte de la vida política del país por medios tecnológico.

Así pues, debería analizarse un poco más a fondo el régimen de excepción planteada para la captación del respaldo ciudadano, y que la obtención de las firmas, pueda ser también obtenida, en ese supuesto- bajo el esquema de papel, sobre todo porque la verificación de la información otorgada se corrobora en la base de datos del INE que se creó para tal fin.

4. CONCLUSIONES

PRIMERA.- La tecnología permite hoy día modificar la comunicación política e interacción entre gobiernos y ciudadanos; así, este último de la mano con las herramientas tecnológicas existentes, puede contar con una participación activa en la vida democrática de un Estado.

SEGUNDA.- México vivió la celebración de las elecciones más grandes en su historia, en donde tanto actores políticos, como autoridades electorales y la misma ciudadanía interesada en transformar la vida democrática del país, se posicionaron a través del uso de herramientas tecnológicas que buscaban el bien común.

---

[24] 14° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018 [en línea]. [Consulta: 11-07-2018]. Disponible en: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/14-Estudio-sobre-los-Habitos-de-los-usuarios-de-Internet-en-Mexico-2018/lang,es-es/?Itemid=

[25] Índices de marginación [en línea]. [Consulta: 12-07-2018]. Disponible en: http://www.conapo.gob.mx/en/CONAPO/Indices_de_Marginacion

TERCERA.- Durante la preparación de las elecciones en México, el Instituto Nacional Electoral, utilizó por primera ocasión una aplicación móvil para recabar el apoyo ciudadano de los aspirantes a un cargo de elección popular por la vía independiente, teniendo la finalidad el dotar de certeza la verificación del respaldo ciudadano.

CUARTA. Sin embargo, la utilización de la App, generó discriminación y desigualdad en algunos sectores de la población, así como la merma en la efectiva participación de la ciudadanía que pretendía apoyar a un aspirante por no ser de acceso público.

5. REFERENCIAS BIBLIOGRÁFICAS

- 14° Estudio sobre los Hábitos de los Usuarios de Internet en México 2018[en línea]. [Consulta: 11-07-2018]. Disponible en: https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/14-Estudio-sobre-los-Habitos-de-los-usuarios-de-Internet-en-Mexico-2018/lang,es-es/?Itemid=
- Candidaturas Independientes 2018 [en línea]. [Consulta: 06-07-2018]. Disponible en: http://www.ine.mx/candidaturasindependientes/
- CARRAZO BARRANTES, C. *El nuevo contexto de las campañas electorales: El caso del App Mivotohoy.* Pew Reseach Center, 2015
- Constitución Política de los Estados Unidos Mexicanos, Artículo 35, fracción II.
- DEUTSCH, K. *The Nerves of Government; Models of Political Communication and Control,* Nueva York: Kindle Edition, 2009.
- EcuRed [en línea]. [Consulta: 29-5-2018]. Disponible en: https://www.ecured.cu/Participaci%C3%B3n_ciudadana
- Expansión en alianza con CNN [en línea]. [Consultada: 15-6-2018]. Disponible en: https://expansion.mx/tecnologia/2017/10/31/la-apuesta-del-ine-por-apps?internal_source=RELATED_ARTICLE

- Índices de marginación [en línea]. [Consulta: 12-07-2018]. Disponible en: http://www.conapo.gob.mx/en/CONAPO/Indices_de_Marginacion
- INE/CG387/2017 Acuerdo del Consejo General del Instituto Nacional Electoral por el que se emiten los Lineamientos para la verificación del porcentaje de apoyo ciudadano que se requiere para el registro de candidaturas independientes a cargos federales de elección popular para el proceso electoral federal 2017-2018[en línea]. [Consultada: 25-6-2018]. Disponible en: https://www.ine.mx/wp-content/uploads/2017/09/CGex201708-28-ap-12.pdf
- Ley General de Instituciones y Procedimientos Electorales
- Lineamientos para la verificación del porcentaje de apoyo ciudadano que se requiere para el registro de candidaturas independientes a cargos federales de elección popular para el proceso electoral federal 2018-2018 [en línea]. [Consultados: 15-6-2018]. Disponible en: http://www.ine.mx/wp-content/uploads/2017/09/ANEXO-1-CG387-17.pdf
- Manual de Auxiliar/Gestor Dispositivo con Android, correspondiente a la segunda versión de la aplicación [en línea]. [Consultada: 28-6-2018]. Disponible en http://www.ine.mx/wp-content/uploads/2017/10/Manual-de-Auxiliar_Gestor-App_Android-V-2.0_.pdf

-PECES-BARBA, G., *Educación para la ciudadanía y derechos humanos,* Madrid: Grupo Edebé, 2007, p. 240.
-PEÑA GALAVIZ, J. Tlatemoani Revista Académica de Investigación [en línea]. [Consultada: 31-5-2018]. Disponible en: http://www.eumed.net/rev/tlatemoani/15/tecnologia-educacion.html
- PÉREZ LUÑO, A. *Los Derechos Humanos en la Sociedad Tecnológica,* Madrid: Editorial Universitas, S.A., 2012, p. 52.
- Periódico digital El Siglo de Durango. [Consulta: 14-06-2018]. Disponibilidad y localización: https://www.elsiglodedurango.com.mx/noticia/913492.descarta-ine-fallas-en-aplicacion-movil-para-independientes.html
-Periódico digital Reporte Índigo [en línea]. [Consulta: 02-07-2018]. Disponible en: https://www.reporteindigo.com/reporte/burlar-al-ine/
-Periódico digital Vanguardia. [en línea]. [Consultada: 02-07-2018]. Disponible en: https://www.vanguardia.com.mx/articulo/justifica-ine-error-en-la-app-para-independientes-son-parte-de-la-curva-de-aprendizaje
-Reglamento de Elecciones
-Sentencia de la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación, de clave SUP-JDC-841/2017 [en línea]. [Consultada: 18-6-2018]. Disponible en: http://www.te.gob.mx/Informacion_juridiccional/sesion_publica/ejecutoria/sentencias/SUP-JDC-0841-2017.pdf

PLATAFORMAS COLABORATIVAS DE COMERCIO ELECTRÓNICO Y RESOLUCIÓN DE CONFLICTOS

Por: ***Bibiana Beatriz Luz Clara***[1]
Argentina

Introducción.

La permanente actividad en distintas plataformas ha permitido el desarrollo de un modelo económico basado en la colaboración, en el compartir, bienes o servicios entre particulares a través de cierta compensación que ambas partes pactan. Es la comunidad la que se encarga de dotar de poder a esta economía y hacerla crecer.

Son muchos los proyectos que encontramos hoy basados en economía colaborativa y el éxito que alcanzan se basa en la posibilidad de brindar soluciones agiles y rápidas, efectivas y a menores costos, ya que se inspiran en nuevos conceptos como el "coworking" y el de compartir con otros a través de las tecnologías y las comunicaciones.

Todo se redefine muy velozmente en este entorno electrónico con las tecnologías y las comunidades, que permite que se involucren todos los actores de la sociedad de un modo directo si así lo desean. Sin duda esto traerá beneficios económicos, así como retos regulatorios en los diferentes sectores de la economía, pero ello debe lograrse de un modo tal que no se trabe la innovación y el efecto de la tecnología en pleno desarrollo.

I. Las plataformas de economía colaborativa.

Las plataformas de economía colaborativa[2], que según Rachel Botsman[3], se basan en *"redes distribuidas de individuos conectados y comunidades, que se contrapone a las instituciones centralizadas tradicionales".* Estas se han transformado en un negocio sumamente dinámico y rentable, donde las personas adquieren nuevas posibilidades y poderes fundados en la coordinación de oportunidades de negocios entre iguales, a una escala masiva. Así pueden conseguir lo que necesitan de modo directo, sin tener que pagar más por intermediaciones que ya no se requieren.

Se ha creado una nueva e insospechada tendencia de consumo, que tiene su origen en el desarrollo del mundo digital, la expansión de la interacción en las redes, y las crisis económicas, que llevan a las personas a buscar mecanismos que se adapten al momento del modo más eficiente posible. Se comparten de esta manera bienes, servicios, espacios.

---

[1] Magister en Derecho de Internet y Telecomunicaciones. Doctoranda de la Universidad de Salamanca. Profesora e investigadora de la Universidad FASTA. Abogada y mediadora.

[2] También denominadas sharing economy, economía p2p, o gig economy, conceptos que la Revista Time incluyo en 2011 en la lista de" 10 ideas para cambiar el mundo. Disponible ultimo ingreso 20/06/2018 en http://content.time.com/time/specials/packages/article/0,28804,2059521_2059717_2059710,00.html

[3] Autora del libro "<What's Mine in yours: the rise of collaborative consumption"

ra poner solo unos ejemplos en los casos de alquiler de autos particulares Social Car[4] ofrece alquilar un vehículo a otra persona, como también Amovens[5], y Drivy[6].

Para compartir un vehículo cerca o CarSharing, por unas horas Bluemove[7], Respiro[8], Car2Go[9] y Avancar[10]

El CarPooling para compartir trayectos podemos encontrarlo en BlaBlaCar[11]que se encuentra en distintos países del mundo.

En cuanto al alojamiento y alquiler de casas por corta duración, Airbnd[12] es la alternativa más conocida entre otras similares. Luego para conseguir guías locales para una ciudad se puede recurrir a Vayable[13] o Trip4Real[14], y para ir a comer y conocer gente Eatwith[15] y Vizeat[16], y Bicing[17] para el alquiler de bicicletas.

Estas prácticas y modelos de negocios horizontales van transformando nuestras maneras de vivir, trasladarnos, viajar, trabajar, etc.

El sitio OuiShare[18] impulsa y promociona a emprendedores, y organiza eventos en este esquema de economía colaborativa desde Francia, hacia otros países, en nuevos modelos de intercambio de valor. Algunas personas elaboran sus propios productos[19], convirtiéndose en agentes económicos en pequeña escala, en un modelo donde la gente consigue lo que necesita, unos de otros en forma directa. Este esquema llamado de panal de abejas produce impacto en diversos sectores económicos. Estos bienes y servicios son intercambiados en las plataformas digitales, donde la confianza y el crear una buena reputación digital, constituyen el factor que impulsa la decisión de los clientes al momento de elegirlos.

Las aportaciones de los consumidores, con sus valoraciones, y referencias ayuda a crear perfiles de confianza digital.

Los ciudadanos tienen hoy el poder de impactar en su entorno a través de un click, y eso otorga mayor capacidad técnico- cultural, que permite reforzar este nuevo modelo de negocios, donde su potencial radica en la posibilidad de integrar a diversas personas, desde

[4] https://www.socialcar.com/
[5] www.amovens.com
[6] https://www.drivy.es/
[7] https://bluemove.es/es
[8] https://www.respiro.es/
[9] https://www.car2go.com/ES/es/
[10] http://www.avancar.com/
[11] https://www.blablacar.es/
[12] https://www.airbnb.com
[13] https://www.vayable.com/
[14] http://turismososteniblemedia.com/trip4real/
[15] https://es.eatwith.com
[16] Recientemente absorbida por Eatwith
[17] https://www.bicing.cat/es/
[18] https://www.ouishare.net/our-dna
[19] Lo que se conoce como" movimiento maker".

el ámbito de su especialidad, en el proceso de generación de valor, tanto a nivel económico como social. Esto implica un cambio cultural que a veces no es fácil de absorber pues deriva en la afectación de modelos tradicionales, que lo ven como una amenaza o competencia desleal. (caso de los choferes de UBER[20] con los modelos de taxis y remises tradicionales).
La rapidez, facilidad y sencillez de este sistema de intercambio en las plataformas de economía colaborativa impulsa su desarrollo, haciendo que las cifras de su intercambio comercial en auge, aumenten geométricamente. Este sistema pone el acento en el consumo responsable y en el cuidado del medio ambiente, fomentando la reutilización de los objetos que aún pueden brindar utilidad, favoreciendo la creatividad y la innovación.

El marco legal de este tipo de modelo no está claro todavía, al carecer de una regulación específica, aunque se cree que esta podría obstaculizar el interés general de los actores que intervienen en ellas. Se desplaza entre la normativa aplicable para contrataciones ordinarias en el ámbito civil o mercantil, y las normas de protección de los derechos de los consumidores. También como apuntábamos antes se basa en los códigos de conducta y de buenas prácticas, y los mecanismos extrajudiciales de resolver conflictos, para generar mayor confianza y seguridad en el sistema.

II. Regulación de la economía colaborativa.

La economía colaborativa incluye distintas formas de comprar, vender, compartir, intercambiar bienes y servicios, en una amplia gama de actividades unas remuneradas y otras no, todo esto apoyado en la conectividad, en el entorno electrónico, sin que encontremos aun, una normativa especial que regule esta nueva realidad.

Por ello se aplica a estas situaciones la normativa general para contrataciones ordinarias civiles y comerciales y la de defensa de los consumidores existente, y se sujetan a la responsabilidad civil, penal y administrativa, que pudiera corresponderles por su accionar.

Organizaciones como ADICAE[21] en España, llaman la atención de manera crítica a los usuarios de consumo colaborativo, recomendando que se acerquen a este tipo de opciones con una actitud preventiva, ante posibles amenazas que pudieran comprometer sus intereses, atento a las fragilidades que todavía presenta el sistema.

Frente a esta situación se genera el debate sobre si es necesario crear una nueva normativa, en cada país, o una corregulación entre estados. Otros opinan que lo mejor sería dejarla a la autorregulación del mercado, a partir de ciertas buenas prácticas y códigos de conducta que protegen a los usuarios y consumidores y que de no ser respetados harán que baje su reputación digital y dejen de ser elegidos, dado que dicha información es fácilmente accesible en las redes.

Aquellos que voluntariamente se comprometen a respetar las reglas de conducta pueden ser identificados con determinado sello de calidad para beneficio y garantía de los consumidores.

[20] https://get.uber.com
[21] https://www.adicae.net/ ADICAE :Asociación de Usuarios de Bancos y Cajas de Seguros.

Los códigos de conducta se siguen extendiendo indicando parámetros de respeto por la legalidad, brindando confianza en la plataforma y otorgando una seguridad adicional.
La tendencia parece acercarse más a la idea de una corregulación que tenga a los códigos de conducta y a las buenas prácticas como un complemento a los sistemas legales y jurisdiccionales, para dar mayor amplitud a la seguridad y protección de todos los que operan en las plataformas.

En la misma línea se posiciona a los mecanismos extrajudiciales de resolver conflictos como una alternativa que debe beneficiarse, e impulsarse la creación y consolidación de los mismos. Los códigos de conducta y los mecanismos de resolución de conflictos son tan dinámicos como lo requiere la economía colaborativa y pueden ser aplicados en su mismo entorno, haciendo que los usuarios se sientan siempre protegidos y puedan informarse adecuadamente sobre a quién pueden recurrir rápidamente en el caso de necesitarlo.

Los ODR y las reglas de conducta, por su tendencia a la integración y coordinación con sentido global, ayuda a superar los problemas de la territorialidad. La aceptación y credibilidad de estos sistemas viene de la mano de la eficacia que puedan demostrar en la gestión de los conflictos y la promoción de la corrección ética en su accionar.

Las empresas que se adhieren a ellos[22] deben poder demostrarlo a sus usuarios y brindarles toda la información, de manera que estos puedan conocerla acabadamente y ejercer sus derechos.

Al hablar de las buenas prácticas para favorecer el Comercio Electrónico, y con la finalidad de brindar mayor confianza y seguridad entre empresas y consumidores, o entre estos mismos en sus transacciones en las plataformas colaborativas, debemos tener en consideración, la seguridad de los medios de pago, la información que se brinda, el resguardo y manejo de los datos personales, la publicidad, la contratación electrónica, la atención dispensada y los ODR[23].

Pero cualquiera sea el mecanismo elegido siempre deberá ser respetado el principio de legalidad, en la contratación de bienes y servicios de manera electrónica, siguiendo la legislación vigente y los principios constitucionales.

En el caso de presentarse conflictos por la deficiente ejecución de las contrataciones, el usuario se dirigirá a la plataforma, que en el caso de las que resultan intermediarios, seguramente tendrán una exención de responsabilidad ya aceptada por el usuario, por lo cual habrá de resolverse el tema entre los interesados directos, o en el mejor de los casos al Servicio de atención al cliente de la propia plataforma.
En el caso que el conflicto sea con la plataforma esta tendrá articulado un sistema de resolución on line (ODR) con la posibilidad de acceder a la mediación o al arbitraje y detallados sus códigos de conducta.

[22] Como el caso de www.confianzaonline.es que publica sus memorias de actividad, desde el año 2003.
[23] Online Dispute Resolution.

III. Las plataformas electrónicas de resolución en línea.

En el ámbito del comercio electrónico se producen todo tipo de conflictos, y hacerlos depender del sistema judicial, constituye un serio problema, que impacta negativamente en el crecimiento y desarrollo del sistema comercial, dadas las tardanzas y complejas situaciones por todos conocidas, además de los altos costos, y las dificultades en procesos transnacionales.

Frente a esta situación surgieron las plataformas electrónicas de resolución en línea, que tienen la forma de un sitio de Internet interactivo. Permiten que los consumidores resuelvan sus reclamos extrajudicialmente de modo rápido y eficaz, aportando confianza al comercio electrónico, especialmente para compras transfronterizas, siendo la legislación sobre ODR una de las prioridades para fomentar y reforzar el crecimiento en la dimensión digital del mercado.

Las plataformas facilitan información sobre los métodos ODR, permiten ingresar los reclamos mediante formularios electrónicos disponibles en varios idiomas, y adjuntar documentos, mantener el intercambio seguro de datos que transmiten las partes, informándolas sobre sus derechos y mediante su consentimiento para el tratamiento de los datos personales.

Los comerciantes que celebren contratos de compraventa o de prestación de servicios en línea pueden proporcionar en sus sitios de internet un enlace electrónico a las plataformas de resolución a las que estén adheridos y proporcionar su correo electrónico de contacto.

Se promueve en general, que para los problemas generados en la contratación electrónica, se utilicen los mecanismos ODR, como la alternativa más eficaz a la justicia, por sus caracteres específicos de rapidez, la privacidad que se mantiene sobre lo discutido y acordado, la flexibilidad del sistema, la confianza, y la gratuidad en el caso de los consumidores.

La misma se puede llevar a cabo mediante entidades acreditadas o mediante la plataforma que el usuario acepta al interactuar con ella, pero teniendo en cuenta que conforme al principio de libertad[24]de elección, no será válido el acuerdo de sumisión obligatoria al arbitraje para el consumidor antes de presentarse el conflicto, y que lo prive de acceder a la tutela judicial efectiva.

El buen desarrollo de los ODR, requiere de ciertos elementos que se consideran esenciales según nos indica Naon Ebner[25], son la confianza, la equidad y la seguridad. Sin estas tres condiciones las operaciones de comercio electrónico se verían disminuidas o afectadas en distinta medida, ya que las partes no querrían participar de procesos de resolución en línea.

[24] Consagrado en el art, 10 de la Directiva 2013/11

[25] Ebner, Noam and Zeleznikow, John (2015) "Fairness, rust and Security in Online Dispute Resolution," Hamline University's School of Law's Journal of Public Law and Policy: Vol. 36: Iss. 2, Article 6. Available at: http://digitalcommons.hamline.edu/jplp/vol36/iss2/6

La *seguridad informática*, es esencial para que las partes puedan brindar información con la tranquilidad necesaria para obtener una resolución rápida fundada en la confidencialidad de lo que allí se expresa, y el resguardo de los datos que se vuelcan en el sistema, bloqueando los accesos no autorizados que pueden vulnerar la privacidad.

Confiable para brindar a las partes en conflicto la certeza acerca de la imparcialidad que ofrecen las plataformas ODR. Las transacciones requieren confianza, y esta debe ser construida sobre la base de que la tecnología utilizada por la plataforma no fallara, que el proceso será neutral y competente, y que los costos y los tiempos a invertir no superaran lo esperado.
La *equidad*, que requiere actuar por igual con todas las partes, dando a cada una igual oportunidad, para expresarse, y tomar decisiones sobre cómo llegar a lograr sus objetivos, en un marco de transparencia, consensuando un conjunto de reglas a respetar para garantizar la organización del intercambio de información.

Cuando se elija un mecanismo ODR, además de respetar los requisitos generales de este tipo de sistema alternativo, se deberá tener especialmente en cuenta : la *disponibilidad* para cualquier persona desde cualquier lugar y momento; la *accesibilidad* por los medios de conectividad a su alcance; la *facilidad de uso*, que lo haga interactivo, amigable y rápido; y la *seguridad y fehaciencia* utilizando todas las herramientas disponibles para brindar confidencialidad, asegurar la recepción de las notificaciones, y la seguridad de las comunicaciones.

Actualmente se habla de la tecnología como la "cuarta parte" que integra el esquema de ODR, a partir de las enseñanzas de E. Katsh y J. Rifkin[26] Las tecnologías permiten vínculos internacionales que tiempo antes no hubieran sido posibles. Ofrecen a las partes inmediatez, interactividad, y opciones multimedia para aplicar y elegir, basadas en nuevas plataformas de comunicación que se utilizan para intercambiar propuestas entre las partes.

La posibilidad de resolver los conflictos del mismo modo y con la misma velocidad con la que se producen, abre la puerta a un nuevo esquema de acceso a justicia, donde las herramientas tecnológicas cumplen un rol fundamental.

En la U.E,. en su búsqueda de una continua construcción del derecho procesal y solución de controversias común, encontramos la Directiva U.E. 11/2013, el Reglamento (UE) n.º 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo y por el que se modifica el Reglamento (CE) n.º 2006/2004 y la Directiva 2009/22/CE. Esto ha permitido que desde el 15 de febrero de 2016 se haya puesto en marcha para todos los países de la Unión Europea una plataforma de resolución de conflictos en materia de consumo entre empresas y consumidores[27]. Las empresas deben registrarse en la plataforma y facilitar su correo a fin de que, quien quiera realizar una reclamación pueda hacerlo.

[26] "On line dispute resolution: resolving conflicts in cyberspace" Ed. Jossey- Bass San Francisco 2001.
[27] https://ec.europa.eu/consumers/odr/main/?event=main.trader.register

La tramitación es sencilla para los consumidores que quieren hacer un reclamo. Deben llenar un formulario desde la página web http://ec.europa.eu/consumers/odr/, que se remite a la contraparte con la finalidad de que acuerde con el requirente la elección del órgano de resolución de conflictos, entre los que ofrece la plataforma, y que deberá resolver el tema dentro del plazo de noventa días.

En España la ley 7/2017 incorpora la directiva 11/2013, relativa a la resolución de conflictos en materia de consumo, y regula las entidades de resolución acreditadas (ERA), a las que pueden adherirse las empresas para integrarse al sistema. La adhesión es por el plazo de dos años en los cuales no puede apartarse.

AECOSAN[28] es en dicho país, la encargada de recibir y valorar las solicitudes de incorporación al listado de entidades de resolución, y remitirlo a la Comisión Europea para la integración a un listado único. Los procedimientos son voluntarios para ambas partes y deben respetar los principios de independencia, imparcialidad, transparencia, equidad y eficacia.

Otras plataformas existentes por citar solo algunas son: Ecodir[29] que provee una red de instituciones ODR asociadas a las que se puede recurrir mediante su plataforma.
Mediate.com[30] en la que se pueden elegir entre los distintos sistemas de resolución de conflictos, obtener información, y seleccionar según el tipo de materia a tratar.
Themediationroom[31]en Inglaterra, provee un servicio ODR para quienes quieren resolver rápidamente sus diferencias, a menor costo que ante un tribunal, y manteniendo las relaciones interpersonales. También organiza jornadas y eventos para difundir las actividades de resolución de conflictos on line a través de profesionales especializados.

Risolvionline[32] es una plataforma italiana, perteneciente a la Cámara de Comercio de Milán, que permite resolver conflictos, iniciando un requerimiento desde la página de inicio de su plataforma. Describe el procedimiento en varios pasos, y contiene un tutorial que sirve de guía informativa, para saber cómo llenar los formularios, incorporar los datos solicitados, describir el problema, e informar sobre el procedimiento a utilizar optando por mediación o arbitraje, e indica el costo del mismo.
Aryme[33]provee un directorio de instituciones y profesionales adheridos para brindar servicios ODR, además de jurisprudencia e información sobre eventos, artículos y documentos de interés para la resolución de conflictos.

[28] Agencia Española de Consumo
[29] http://www.arbitration-adr.org/network/
[30] https://www.mediate.com/odr/
[31] https://www.themediationroom.com/
[32] https://www.risolvionline.com/index.php
[33] https://aryme.com/

Finalmente es necesario comentar que la CNUDMI[34] aprobó las Notas Técnicas[35] sobre la resolución de disputas en línea, en su reunión del 5 de julio de 2016, en su 49º periodo de Sesiones, en New York, atento al fuerte incremento de las transacciones transfronterizas en línea, y la necesidad de resolver las disputas que pudieran suscitarse en dicho ámbito, de modo rápido y eficaz.

Las Notas son descriptivas y no vinculantes, recogen los principios fundamentales de imparcialidad, independencia, eficiencia, eficacia, rendición de cuentas, transparencia, equidad, debido proceso, y esperan servir de ayuda a compradores y vendedores a encontrar la solución a sus diferencias.

Dichas notas son el fruto del Grupo de Trabajo III[36] establecido en 2010, con tal finalidad, luego de consultas con gobiernos, organizaciones no gubernamentales internacionales, y la participación de organizaciones invitadas como observadores. Se recomienda a los Estados que utilicen las notas técnicas cuando delineen y lleven a la práctica sus sistemas de resolución de controversias.
La finalidad de las Notas Técnicas es promover el desarrollo, y prestar asistencia a los administradores ODR, a las plataformas ODR, a los terceros neutrales, y a las partes en el proceso ODR. Describiendo los distintos sistemas posibles, así como el proceso y sus etapas.

Conclusión:

EL incremento notable de las actividades en las plataformas de economía colaborativa, este nuevo modelo electrónico de hacer negocios, trae aparejada la necesidad de contar con mecanismos eficaces y agiles de resolver los conflictos que en dicho entorno se producen.

Cuando las posibilidades de resolución rápidas y en línea, se hacen efectivas se agrega un plus de valor y de confianza en el sistema, que todos tendrán en consideración a la hora de elegir un determinado sitio o plataforma, favoreciendo el desarrollo y crecimiento del comercio electrónico, creando confianza en las relaciones, y permitiendo hacer valer efectivamente los derechos de los consumidores en Internet. De otro modo los altos costos de traslados y de litigar en muchos casos, en el extranjero, dejarían las situaciones sin resolver. Estamos frente a un incremento de los negocios en las plataformas de economía colaborativa que crece a cada momento e invade áreas de la economía tradicional que parecían intocables. Las plataformas de resolución de conflictos en línea constituyen la herramienta facilitadora para dar solución a las situaciones que se produzcan, de modo sencillo y rápido y de la misma manera con la cual sus actores están acostumbrados a operar diariamente.

[34] Comisión de las Naciones Unidas para el Derecho Mercantil internacional: Órgano jurídico central del sistema de las Naciones Unidas para el Derecho Mercantil Internacional, cuya misión es eliminar los obstáculos al comercio internacional y armonizar y modernizar la legislación.
[35] Las Notas Técnicas se pueden visitar en:
http://www.uncitral.org/pdf/spanish/texts/odr/V1700385_Spanish_Technical_Notes_on_ODR
[36] Grupo de trabajo en Solución de Controversias en línea.io

Bibliografía consultada:

ADICAE "La plataforma ODR: ¿Un mecanismo al alcance de todos los consumidores? Editorial Adicae España 2016.
Alzate Sáez de Heredia, Ramón y Vásquez de Castro, Eduardo "Resolución de disputas en línea" Ed. Reus España 2013
Ebner, Noam and Zeleznikow, John (2015*) "Fairness, trust and Security in Online Dispute Resolution,"* Hamline University's School of Law's Journal of Public Law and Policy: Vol. 36: Iss. 2, Article 6. Available at: http://digitalcommons.hamline.edu/jplp/vol36/iss2/6
Fisas Vincen : Cultura de paz y gestión de conflictos. Ed. Icaria, Barcelona 2001
García Peña, José Heriberto: *"La regulación del comercio, retos ante el cambio tecnológico"* Revista IUS México No. 41 Volumen 12 enero 2018. https://revistaius.com/index.php/ius/article/view/456
Katsh E. y J. Rifkin "*On line dispute resolution: resolving conflicts in cyberspace*" Ed. Jossey- Bass San Francisco 2001.
Notas Técnicas de CNUDMI 49º Periodo de Sesiones:

http://www.uncitral.org/pdf/spanish/texts/odr/V1700385_Spanish_Technical_Notes_on_ODR
Reglamento (UE) n.º 524/2013 del Parlamento Europeo y del Consejo, de 21 de mayo de 2013, sobre resolución de litigios en línea en materia de consumo.
Sigmund, Karen: *"El comercio electrónico en los tratados de libre comercio en México"* Revista IUS México No. 41 Volumen 12 enero 2018. https://revistaius.com/index.php/ius/article/view/370/628
Vilalta Nicuesa, Aura Esther. "Mediación y Arbitraje electrónicos" 1era. Edición. Editorial Aranzadi, Pamplona, España 2013.
https://www.revista-uno.com/numero-20/economia-colaborativa-la-revolucion-del-consumo-mundial/
Observación: Todas las páginas indicadas a pie de página han sido chequeadas durante el mes de junio de 2018 y se encontraban activas.

LIMITACIONES CONSTITUCIONALES DEL DERECHO DE INFORMACIÓN EN UN MUNDO GLOBALIZADO

Por: ***Danny Alejandra Cuevas López***
Colombia

INTRODUCCIÓN.

WikiLeaks es un sitio web que fue reconocido a partir del año 2007 en internet, el cual alcanzó su auge en el año 2010 tras publicar un video en el que asesinaban a dos periodistas de la agencia Reuters en Irak. Según lo explica su fundador Julián Assange, la etimología de la palabra WikiLeaks significa filtraciones rápidas, de este modo para los hackers y periodistas, WikiLeaks es una página web que permite desde cualquier parte del mundo acceder y publicar información de cualquier índole, incluso carácter confidencial.

El programador, periodista y ciber-activista de internet australiano Julián Assange, fundador, editor y portavoz del sitio web WikiLeaks; coloca a diario su vida en peligro y la seguridad nacional de varios Estados como Noruega, Dubái, Goa, Afganistán, Dinamarca, al desarrollar su actividad profesional, debido a la labor que WikiLeaks despliega a nivel mundial desafiando los gobiernos del mundo, no solo por filtrar información y documentos militares y diplomáticos, sino por su difusión, almacenamiento en bases de datos y lograr que se multipliquen masivamente en ordenadores alrededor del mundo para que dicho contenido no desaparezca.

Assange recibe amenazas de asesinato, prohibición en países para entrar en sus jurisdicciones; judicializaciones por delitos; y varios pronunciamientos de altos funcionarios públicos al estar en desacuerdo por divulgar información restringida de cada gobierno, especialmente sobre los países que son superpotencias en el mundo como EEUU, China, Japón, Irak, Reino Unido, Francia, Australia.

La labor que WikiLeaks desarrolla a nivel mundial, desafía los gobiernos del mundo al filtrar información que es de carácter público, pero con una restricción confidencial. Su trabajo consiste en difundir dicha información por medio de su sitio web, permitiendo el acceso a cualquier persona desde cualquier parte del mundo. Aquellos países que se han visto afectados por el funcionamiento de WikiLeaks y su uso para transferir archivos gubernamentales de forma internacional, sustentan una reserva sobre sus archivos estatales por ser de carácter confidencial y cuyo contenido al ser divulgado puede afectar la seguridad nacional de sus países.

La información de reserva legal está definida en la ley 1437 del 2011 en el artículo 24 que determina como únicos documentos e informaciones sometidos a reserva los que expresamente indique por la Constitución o la ley, y nombra algunos casos en los cuales son de especial derecho de reserva legal como:

1. Los protegidos por el secreto comercial o industria.

2. Los relacionados con la defensa o seguridad nacionales.

3. Los amparados por el secreto profesional.

4. Los que involucren derechos a la privacidad e intimidad de las personas, incluidas en las hojas de vida, la historia laboral y los expedientes pensionales y demás registros de personal que obren en los archivos de las instituciones públicas o privadas, así como la historia clínica, salvo que sean solicitados por los propios interesados o por sus apoderados con facultad expresa para acceder a esa información.

5. Los relativos a las condiciones financieras de las operaciones de crédito público y tesorería que realice la Nación, así como a los estudios técnicos de valoración de los activos de la Nación. Estos documentos e informaciones estarán sometidos a reserva por un término de seis (6) meses contados a partir de la realización de la respectiva operación. (CONGRESO DE COLOMBIA, 2011, pág. 13)

En Colombia la ley 1621 de 2013 por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, permite judicializar al infractor por el delito de divulgación de información no autorizada y la ley 1712 de 2014 donde en su artículo 2 expresa que "Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con la presente ley" (Congreso de la Republica de Colombia, 2014, pág. 1). Sin embargo, en el marco jurídico constitucional el Estado se compromete a brindar a las personas y ciudadanos residentes en Colombia, unas garantías constitucionales dentro de las cuales se encuentran "libertades" establecidas en la constitución de 1991 que se ven desarrolladas en el Artículo 16, 20. 23, 73 y 74 que corresponden a esos derechos que permiten el acceso a la información, divulgación y al libre desarrollo de la personalidad.

Límites a la libertad del acceso de información pública confidencial en Colombia

El derecho de petición establecido en el Artículo 23 de la Constitución Política de Colombia permite a todo ciudadano colombiano reclamar información no secreta sobre asuntos de interés general, como mecanismo de control a las entidades estales del Estado. Por otra parte, es el derecho de libertad de información y libertad de prensa quien concede un ejercicio eficaz del derecho de petición, que en conjunto permite a su vez un control contra la influencia o la arbitrariedad de los gobernantes.

Si el Estado restringe el derecho de libertad de información y libertad de prensa estaría cerrando una garantía constitucional y a su vez estaría violando el artículo 19 de la declaración Universal de los Derechos Humanos

> *Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. (Unidas, 1948)*

Si se restringe este derecho se estaría cohibiendo la posibilidad de conocer las actuaciones estatales y no contando con un régimen objetivo para acceder a las actuaciones de los entes gubernamentales.

En contra posición para acceder a información catalogada con reserva legal, el ejercicio este derecho debe estar sometido ciertos imperativos que permitan de manera excepcional y en ciertos casos, conocer y difundir esta información, como lo son:

1. Vulneración de derechos humanos: este imperativo es la justificación clave y trascendente, en virtud de que de manera excepcional se pueda publicar información con reserva legal, justamente para demostrar que el derecho concedido constitucionalmente a funcionarios públicos y/o personas jurídicas como es el caso del secreto comercial o industrial, pueden contener vulneración de derechos humanos, siendo de vital importancia que dicha información sea revelada. El sustento jurídico de este imperativo se encuentra en los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información, el cual se explicará más adelante.

2. La exactitud: consiste en que la información publicada o difundida no afecte o atente la seguridad del Estado y la defensa Nacional, es decir, la información pública debe ir en armonía con el bienestar del Estado, si un documento con reserva legal, contiene información que evidencia la vulneración de derechos humanos, pero a su vez la divulgación o publicación de esté no atenta la seguridad del Estado, ni la defensa Nacional, cumpliría con el segundo requisito, que es el de exactitud o no transgresión al bienestar del Estado.
   El derecho de acceso a la información genera una obligación conjunta tanto las entidades públicas y las personas que ejercen actividades en representación del Estado están obligados a garantizar el pleno ejercicio de este derecho.
   A su vez, los ciudadanos y funcionarios públicos deben comprometerse a no transgredir, ni ir en contra de los límites impuestos por las leyes para ejercer este derecho.
   Por lo tanto, WikiLeaks en el caso del Estado colombiano no puede tener publicado en su sitio web información que atente en contra de la seguridad y defensa nacional, ya que si incurre en esta prohibición estaría cometiendo al menos el delito de Acceso abusivo a un sistema informático, artículo 269A; Interceptación de datos informáticos, articulo 269C; Artículo 269H. Con al menos una circunstancia de agravación punitiva que es la numero 6 Que es que cuando se comete uno de los delitos anteriormente mencionados con fines terroristas o generando riesgo para la seguridad o defensa nacional, consagrados en la Ley 599 del 2000. (Congreso de la Republica,, 2000)
3. Veracidad: la información publicada o difundida debe ser verídica, es decir, aquella información debe ir acorde con la realidad, no puede haber sido alterada, modificada o parcialmente oculta.
   Este imperativo constituye un eximente de responsabilidad ya que como dice Jaime Lombana "Nuestra Constitución sólo protege la información veraz: resaltando que la Constitución y Ley colombiana no protegen al informador negligente". (Lombana, 2006) en otras palabras, siempre y cuando la información publicada este constituida por una prueba verídica que sirva como soporte para dicha información, puede ser eximido de responsabilidad quien la publico y a su vez tiene una protección constitucional.

4. El interés social: el contenido de la información debe ser de interés general para la sociedad, en caso de que se demuestre que cumple con ese interés general, estará entonces expresando a plenitud el fin esencial de todo Estado democrático: el de la formación libre y plural de la opinión pública.

El secreto es un derecho por el cual cada persona por la autonomía dispositiva que le atribuye el Estado, puede ejercerlo de carácter discrecional. Si en el ejercicio al secreto discrecional contiene información de carácter confidencial que viole la ley, la constitución o normatividad de ámbito internacional, éste estaría atentando contra el Estado y violando el principio de interés general. La vulneración de derechos humanos, la exactitud, la veracidad, y el interés social, serán siempre lo más importantes límites a la libertad del acceso de información pública confidencial en Colombia.

El papel de WikiLeaks en la normatividad colombiana, ponderación de las normas de carácter especial frente al marco constitucional e intervención de entidades administrativas frente a la problemática de delitos contra la ciberinformación.

En Colombia la ley 1621 de 2013 Ley de Inteligencia, le permite al Estado de Colombia judicializar al infractor por el delito de divulgación de información no autorizada. En este caso es pertinente hacer un análisis jurídico si esta ley de carácter especial va en contravención de la Norma Superior que rige el Estado de Colombia.

En un marco constitucional el artículo 2 de la carta política hace mención a las garantías que el Estado se compromete para con las personas y ciudadanos de Colombia, es preciso hacer referencia a que en ella se mencionan unas "libertades" que se ven desarrolladas en los artículos 16, 20, 23 y 73 según corresponden al tema a tratar; la Corte Constitucional hace énfasis en la sentencia C-442 del 2011 en la especial importancia del derecho a la libertad de expresión en el ordenamiento jurídico colombiano como manifestación máxima de personalidad, ideales, intereses, ideologías a los colombianos. Además, "ha señalado que ocupa un lugar privilegiado dentro del catálogo de derechos fundamentales" (Demanda de inconstitucionalidad , 2011)

El articulo 16 y 20 de la Constitución Política de Colombia de 1991 denotan una gran conexión permitiendo a todas las personas el libre desarrollo de su personalidad y "garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación" (Constitución Política de Colombia, 1991), si bien este derecho es protegido en una norma nacional, del mismo modo tiene un sustento en el marco jurídico internacional en el artículo 13 de la Convención Americana, la libertad de expresión es un derecho de toda persona, sin discriminación por motivo alguno.
Contextualizando la labor de Assange con WikiLeaks en Colombia él estaría bajo los lineamientos constitucionales de expresar sus ideales sin perjuicio alguno. Tal es el caso que el Estado se compromete a garantizar dichos derechos.

La ley 1712 de 2014 tiene como objetivo regular el derecho de acceso a la información pública, los procesos para el buen ejercicio de este derecho y las garantía que brinda a los

colombianos, de igual manera determina las excepciones a la publicidad de información, donde las pertinentes al tema de estudio son la defensa y seguridad nacional, la seguridad pública y las relaciones internacionales.

Además, artículo 23 de la Constitución concede a las personas el derecho de solicitar información pública de manera oportuna compartiendo un núcleo axiológico con el artículo 20 porque en él se hace alusión de informar y recibir información veraz e imparcial por parte del Estado, prevaleciendo el interés general si dicha información exenta a la publicación por constituir temas defensa y seguridad nacional; seguridad pública; o relaciones internacionales atentan contra el interés general, en ejercicio del derecho que concede el Art 23. podría solicitar dicha información.

En el proceso de investigación del tema a estudio, se realizó un trabajo de campo donde se enviaron derechos de petición a entidades públicas en Colombia para que dieran una perspectiva respeto a la problemática. Primero el Ministerio de Tecnologías de la Información y las Comunicaciones se le solicito que diera su postura frente a los delitos de divulgación de información con reserva legal por vía electrónica.

La postura que el MinTIC tiene frente a los delitos de divulgación de información es que las entidades deben acogerse a la legislación aplicable a Colombia en estas temáticas como la ley 1273 de 2009, ya que es la única regulación existente para penalizar este tipo de conductas en el entorno digital. (Ministerio de Tecnologías de la Información y las comunicaciones, 2018)

Conforme a lo establecido en la Ley 1273 de 2009 se modificó el código penal colombiano adicionando el Título VII BIS denominado "De la Protección de la información y de los datos" donde crea un nuevo bien jurídico tutelado anteriormente mencionado, con el fin de preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Así mismo las entidades públicas deben acogerse a lo establecido en la ley 1712 de 2014, que permite determinar qué información debe y/o puede ser publicada, y cuál debe ser clasificada o reservada, según su contenido y siempre que cuente con un sustento legal o constitucional para dicha reserva. (Ministerio de Tecnologías de la Información y las comunicaciones, 2018)

Como ya se explicó anteriormente la ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional tiene por objeto regular todo lo referente a el acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

Dicho lo anterior, como algunos de los delitos informáticos pueden ser de carácter transnacional, también se debe precisar que el Gobierno nacional está tramitando su adhesión al convenio de Budapest (aprobados 3 de 4 debates hasta ahora), el cual permitiría operar de manera coordinada contra estos delitos a través de la cooperación internacional. (Ministerio de Tecnologías de la Información y las comunicaciones, 2018)

Se resalta el trabajo realizado por el Ministerio de Tecnologías de la Información y las Comunicaciones, porque se encuentra al día de la normatividad de delitos informáticos y a su vez tiene el conocimiento de nuevos tratados internacionales que el gobierno colombiano piensa implementar para la regulación de delitos informáticos internacionales, siendo conscientes de que la capacidad de la internet no permanece únicamente en el territorio nacional, sino que se expone a nivel mundial a ser transgredido.

La segunda pregunta que se realizó al Ministerio de Tecnologías de la Información y las Comunicaciones fue ¿Cuál es el aporte que hace el MinTIC a los organismos y entidades del Estados para proteger información con reserva legal?

Su respuesta fue que por "otra parte, en lo relacionado con la seguridad de la información se debe resalta que el Ministerio TIC trabaja desde diferentes perspectivas:

Desde el punto de vista preventivo y de acuerdo con lo establecido en el decreto 1078 de 2015, la Dirección de Gobierno Digital genera lineamientos y políticas en materia de seguridad de la información (como lo es el Modelo de Seguridad y Privacidad de la información – IMPI y sus guías anexas) las cuales deben ser implementadas de carácter obligatorio por la rama ejecutiva del poder público. Así mismo, sin embargo, el Ministerio TIC invita que a que cualquier parte interesada emplee los lineamientos emitidos con el objetivo de proteger los activos de información (esto incluye la información pública, reservada o clasificada que una entidad cree administre o custodie, conforme a lo establecido en las Leyes 1581 de 2012 y 1712 de 2014). (Ministerio de Tecnologías de la Información y las comunicaciones, 2018)

El Ministerio TIC brinda acompañamiento en la implementación de estos lineamientos de seguridad a las entidades públicas, por eso desde un punto de vista estratégico, el Ministerio ha logrado emitir los CONPES 3701 y 3854, cuyo fin es la protección del entorno digital no solo de las entidades públicas sino de las múltiples partes interesadas (Sector Publico, Sociedad Civil, Sector Privado). Pero, a pesar de las estrategias implementadas por el Ministerio no es suficiente para abarcar toda la problemática que se encuentra en la protección de los documentos con reserva legal porque aun estos siguen siendo filtrados desde cualquier parte del mundo.

Adicional a lo anterior, el Ministerio se encuentra trabajando en la creación del Modelo Nacional de Gestión de Riesgos de Seguridad Digital, que busca que todas las múltiples partes interesadas (Sector Publico, Sociedad Civil, Sector Privado), puedan gestionar los riesgos cuando interactúan con el entorno digital.

Finalmente, desde el punto de vista reactivo, el Ministerio ha creado un grupo de respuesta a incidentes en la gestión y respuesta adecuada a incidentes que puedan sufrir las entidades públicas. (Ministerio de Tecnologías de la Información y las comunicaciones, 2018)

El Ministerio TIC de Colombia se encuentra a la vanguardia en cuanto a legislación, procesos de vinculación de tratados internacionales, mecanismos de defensa contra los delitos informáticos y ciberataques, contrarrestando la posibilidad de que se pueda filtrar información confidencial o de reserva legal. A su vez, protege la información personal de los

ciudadanos colombianos mediante estrategias que vinculan entidades especializadas en esta área.

La segunda entidad que dio respuesta fue el Ministerio de Defensa Nacional a quien se le solicito que respondiera ¿Cómo combate los delitos de divulgación de información con reserva legal por vía electrónica?

A lo que su respuesta fue mencionar la Ley 489 de 1998 donde se encuentra determinada las funciones y o**rganización de las entidades del orden nacional**, haciendo énfasis en el artículo 5 en el que fija la **competencia** de los organismos y las entidades **administrativa** y el artículo 59 de la citada ley, acerca de las **funciones dispuestas que** corresponde a los ministerios **y** departamentos administrativos**.**

De igual manera, el Ministerio de Defensa Nacional expreso su participación en la definición, desarrollo y ejecución de las políticas de defensa y seguridad nacionales, para garantizar la soberanía nacional, la independencia, la integridad territorial y el orden constitucional y el orden constitucional, el mantenimiento de las condiciones necesarias para el ejercicio y el derecho de libertades públicas, y para asegurar que los habitantes de Colombia convivan en paz. (Ministerio de Defensa Nacional, 2018)

El Ministerio de Defensa Nacional tiene con fin contribuir con los demás organismos del Estado para alcanzar las condiciones necesarias para el ejercicio de los derechos, obligaciones y libertades públicas como lo es garantizar a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial. Por lo tanto, trabaja con las entidades cibernéticas del Ejército, la Armada y la Fuerza Aérea Colombiana, los cuales se encuentran encargados de la ciberdefensa del país y apoya la protección de las infraestructuras críticas digitales nacionales, un ejemplo es el Centro Cibernético Policial – CCP el que se encuentra encargado de la Ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos.

Colombia cuenta con la cooperación de las fuerzas armadas y la policía nacional para el combate de los delitos electrónicos, bajo la dirección de centros especializados a cargo de entidades del Estado para ayudar a cumplir las garantías constitucionales de acceder a información verídica.

Otra pregunta que se realizó al Ministerio de Defensa Nacional fue ¿qué políticas han desarrollo y ejecutoriado sobre la de defensa y seguridad nacional, para garantizar la soberanía nacional frente a los delitos de divulgación de información con reserva legal y por vía electrónica?

A lo que ellos respondieron que bajo este sentido ellos no diseñan políticas específicas respecto a la materialización de delitos, ni mucho menos frente a los delitos de divulgación de información con reserva legal, toda vez que no cuentan con facultades de investigación y/o policía judicial, tarea que se ha encaminado al Centro Cibernética Policial, respecto a delitos cibernéticos. Pero, aclaran que de "conocerse un delito de esta naturaleza por parte de las entidades creadas mediante documentos CONPES, inmediatamente se efectúa coordinación con la Fiscalía General de la Nación para iniciar el proceso investigativo,

aplicando las capacidades y herramientas necesarias" (Ministerio de Defensa Nacional, 2018)

El papel de WikiLeaks en el Derecho Internacional

Se puede presuponer que la labor de WikiLeaks es considerada delito en muchos Estados, debido a que la mayoría de información es de reserva nacional por ser de carácter confidencial y su contenido podría colocar en riesgo la seguridad nacional del país; siendo como regla general lo anteriormente dicho, pero, como criterio excepcional se trae a colación Los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información, el cual en su preámbulo hace hincapié intensamente conscientes de que algunas de las violaciones más graves de los derechos humanos y las libertades fundamentales son justificadas por los gobiernos como necesarias para proteger la seguridad nacional; Teniendo presente que es imprescindible que para que las personas puedan monitorear la conducta de su gobierno y participar plenamente en una sociedad democrática, que tengan acceso a información en posesión del gobierno; Deseando promover un claro reconocimiento del alcance limitado de las restricciones a la libertad de expresión y la libertad de información que se puedan imponer en el interés de la seguridad nacional, para disuadir a los gobiernos de servirse del pretexto de la seguridad nacional para imponer restricciones injustificables sobre el ejercicio de estas libertades" (Los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información ARTÍCULO 19, 1996)

Estos Principios han sido aprobados por el Relator Especial para la Libertad de Opinión y Expresión de la ONU Abid Hussain, en sus informes a las sesiones de 1996, 1998, 1999 y 2001 de la Comisión de Derechos Humanos de la Organización de las Naciones Unidas, el cual como punto principal, enfatiza que diversos países se salvaguardan con la condescendencia que brinda la restricción de información a los Estados, los cuales hay pruebas de que ellos han vulnerado y vulneran los Derechos Humanos de las personas e infringe el Derecho Internacional, donde se cobija el Principio 1.2: Protección de un interés legítimo de seguridad Nacional, para cometer dichos actos que revierten en características de delito. En consecuencia, dicho principio dice "Cualquier restricción sobre la expresión o la información que un gobierno procurará justificar por motivos de seguridad nacional deberá contar con el propósito genuino y el efecto demostrable de proteger un interés legítimo de seguridad nacional" (Los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información ARTÍCULO 19, 1996, pág. 4)*l".*

En contra posición, el trabajo de WikiLeaks no lo representa en algunos casos, ya que la información revelada puede resultar valiosa para la comunidad internacional si en esta se encuentra la vulneración de Derechos Humanos. A su vez WikiLeaks se encuentran protegido por en el Principio 2: Interés legítimo de seguridad nacional-

b) En particular, una restricción que se procurara justificar por motivos de seguridad nacional no será legítima si su propósito genuino o su efecto demostrable es el de proteger intereses inconexos con la seguridad nacional, incluso, por ejemplo, el de proteger a un gobierno de una situación embarazosa o de la revelación de algún delito, o el de ocultar información sobre el funcionamiento de sus instituciones públicas, o el de afianzar una ideología en particular,

o el de suprimir la conflictividad industrial. (Los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información ARTÍCULO 19, 1996, pág. 5)

Se puede considerar que WikiLeaks, puede convertirse en una fuente al margen de ser fuente principal sobre la violación de tratados y convenios firmados y ratificados por los Estados de la comunidad Internacional que aceptaron y acogieron su normatividad y que se encuentran haciendo caso omiso a su compromiso, ya mencionado anteriormente en el Principio 2.

El valor social desarrollado por Julián Assange hasta el momento ha sido enmarcado en el principio 7: Expresión protegida (a) Sujeto a los Principios 15 y 16, el ejercicio pacífico del derecho de la libertad de expresión, acceso a la información y libertad de prensa, no es considerado una amenaza cualquiera a la seguridad nacional ni debería ser sometido a restricción o sanción alguna por parte de los Estados. La expresión que no constituirá una amenaza a la seguridad nacional contiene lo siguiente "IV tenga como propósito la comunicación de información sobre supuestas violaciones de los estándares internacionales de derechos humanos." (Los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información ARTÍCULO 19, 1996, pág. 7)

Conclusiones

Existe unos límites para la libertad del acceso a la información confidencial pública en Colombia, por lo cual se debe analizar cada caso en concreto, si documento publicada en el sitio web WikiLeaks bajo reserva legal, cumple con todos los principios imperativos de vulneración de derechos humanos, exactitud, veracidad e interés social.

En materia de ciberdelitos Colombia cuenta con una amplia cobertura de regulación de la materia. Así mismo, cuenta con la vinculación de varias entidades administrativas que trabajan en conjunto para judicializar la violación de Derechos Humanos.

Si WikiLeaks demuestra que la información publicada en su sitio web lo hace con el objetivo de demostrar supuestas violaciones de los estándares internacionales de derechos humanos, no estaría infringiendo el Derecho Internacional por lo establecido en pactos internacionales respecto del acceso y divulgación de información confidencial pública.

Finalmente, una persona no puede ser judicializada por delitos asociados a revelar información confidencial pública, si demuestra que la información que divulgó contiene vulneración de Derechos Humanos por parte del Estado o una entidad pública.

Bibliografía

CONGRESO DE COLOMBIA. (2011). *LEY 1437 DE 2011 Código de Procedimiento Administrativo y de lo.*

Congreso de la Republica,. (2000). Codigo Penal Ley 599 del 2000. Colombia.

Congreso de la Republica de Colombia. (2014). *LEY 1712 DE 2014 Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional* .

Constitución Política de Colombia. (1991).

Demanda de inconstitucionalidad , Expediente D-8295 (Corte Constitucional 25 de Mayo de 2011).

Lombana, J. (2006). *Injuria, calumnia y medios de comunicación.* Bogota: Universidad del Rosario ; Biblioteca Jurídica Dike.

Los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información ARTÍCULO 19. (Noviembre de 1996). (español 2005).

Ministerio de Defensa Nacional. (2018). *Contestación de Derecho de Petición No. OFI18-61218 MDN-DVPAIDSPI-GRECC.* Villavicencio.

Ministerio de Tecnologías de la Información y las comunicaciones. (2018). *Respues Radicado 911376 - Derecho de Peticón.* Bogota.

Normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras dispocisiones. (2013). Bogota.

Unidas, T. A. (1948). Humanos, Declaración Universal de Derechos. Paris.

Wikileaks. (s.f.). Recuperado el 2017, de http://wikileaks.info/

LOS PRESTADORES DE SERVICIOS DE CONFIANZA: IDENTIFICACION ELECTRÓNICA Y FIRMA ELECTRÓNICA CON CONTROL CENTRALIZADO

Por: ***María José Viega Rodríguez***
Uruguay

1. INTRODUCCIÓN

Por el artículo 28 de la Ley N° 19.535 de 25 de setiembre de 2017, se incorporaron los artículos 31 a 33 a la Ley N° 18.600 de 21 de setiembre de 2009, que regula a los prestadores de servicios de confianza, concretamente los de identificación digital y firma electrónica avanzada con custodia centralizada. El 19 de marzo de 2018 el Poder Ejecutivo aprobó el Decreto N° 70/018 reglamentario de los mencionados artículos.

La Ley N° 18.600 ha permitido el uso generalizado de la firma electrónica en nuestro país, conteniendo nuestro documento de identidad una firma electrónica avanzada. De acuerdo con la normativa, es necesario que la persona cuente con un dispositivo físico que contenga el certificado electrónico (como por ejemplo: token, tarjeta o cédula de identidad electrónica), así como, la utilización de una computadora o lector que pueda leer dicha firma.

Las firmas electrónicas con custodia centralizada (custodia de los certificados en servidores accesibles vía Internet, conocidas como firma electrónica en la nube) supone que los certificados de firma electrónica se alojan en un tercero que tiene su custodia.

Esto permite implementar soluciones de firma electrónica avanzada en dispositivos de uso masivo, como pueden ser Smartphones o tablets, lo que permite la flexibilización de su uso, por ejemplo para realizar un trámite completamente en línea o consumir servicios que se brinden a través de Internet, de manera confiable.

Por otra parte, se reconoce legalmente el concepto de Identificación Electrónica y se le otorga respaldo jurídico para su equivalencia frente a la identificación presencial.

Tratándose de un tema tan reciente y práctico, nos ha parecido relevante realizar el presente trabajo, siendo conscientes que aún quedan aspectos por definir, en los cuales se viene trabajando, a los efectos de la aprobación de las respectivas políticas. Estas permitirán que el ecosistema entre en funcionamiento. Pero con este planteo inicial es posible entender cuáles son los presupuestos y requisitos y cómo funcionará el sistema una vez implementado, lo cual se cree que sucederá en los próximos meses.

2. ANTECEDENTE: LA LEY N° 18.600

Desde la aprobación de la Ley Nº 16.002 de fecha 25 de noviembre de 1988, en sus artículos 129 y 130 se encuentra regulada la autenticidad y prueba de los documentos trasmitidos a distancia por medios electrónicos entre dependencias oficiales. A partir de ese año existió en

nuestro país normativa regulando tanto el documento como la firma electrónica y digital, como se las denominaba en esa etapa.

El 21 de setiembre de 2009 se aprueba la Ley N° 18.600 que establece el régimen jurídico del documento y la firma electrónicos, regulación que reconoce, desde su artículo primero, la admisibilidad, validez y eficacia jurídica del documento y la firma electrónicos.

Desde el punto de vista estructural la Ley cuenta con 30 artículos distribuidos en seis capítulos denominados:

Capítulo I - Disposiciones Generales (arts. 1 – 10)
Capítulo II – Infraestructura Nacional de Certificación Electrónica (arts. 11 a 15)
Capítulo III – Prestadores de Servicios de Certificación Acreditados (arts. 16 a 20)
Capítulo IV - Certificados reconocidos (arts. 21 a 24)
Capítulo V - Firmante o signatario (arts. 25 a 27)
Capítulo VI - Disposiciones finales (arts. 28 a 30)

De acuerdo con la Ley N° 18.600 la firma electrónica puede consistir en usuario y contraseña, datos biométricos o criptografía asimétrica, proporcionando un concepto amplio de ésta.

Y consagra la firma electrónica avanzada, definiéndola como: "*la firma electrónica que cumple los siguientes requisitos:*

1) requerir información de exclusivo conocimiento del firmante, permitiendo su identificación unívoca;
2) ser creada por medios que el firmante pueda mantener bajo su exclusivo control;
3) ser susceptible de verificación por terceros;
4) estar vinculada a un documento electrónico de tal modo que cualquier alteración subsiguiente en el mismo sea detestable; y
5) haber sido creada utilizando un dispositivo de creación de firma técnicamente seguro y confiable y estar basada en un certificado reconocido válido al momento de la firma".

La firma electrónica avanzada refiere a criptografía asimétrica, específicamente cuando el certificado electrónico es reconocido, por lo tanto es expedido por un prestador de servicios de certificación acreditado. Cuando el prestador no se encuentra acreditado, el certificado electrónico constituye una firma electrónica común.

3. PRESTADORES DE SERVICIOS DE CONFIANZA

Como antecedente en nuestro país podemos mencionar el Proyecto de ley remitido al Parlamento por el Poder Ejecutivo con fecha 3 de agosto de 2017, regulando la firma electrónica avanzada con control centralizado, o también llamada firma en nube y a los prestadores de servicios de confianza. Este proyecto perdió interés con la aprobación del artículo 28 de la Ley N° 19.535, al que ya hemos hecho referencia.

De acuerdo al Decreto reglamentario N° 70/018, artículo 3 literal f), son servicios de confianza: "*los servicios electrónicos que permiten brindar seguridad jurídica a los hechos, actos y negocios realizados por medios electrónicos, entre ellos:*

a) servicios de firma electrónica avanzada con custodia centralizada;

b) servicios de identificación digital;
c) servicios de sellado de tiempo;
d) otros servicios establecidos por la Unidad de Certificación Electrónica".

Como surge del título del presente trabajo, el análisis corresponde a los dos primeros, en virtud a que los servicios de sellado de tiempo ya se encontraban regulados en la Ley N° 18.600 y en su decreto reglamentario, pudiendo acreditarse en este servicio los prestadores de servicios de certificación que se encuentran acreditados, lo cual no ha sucedido hasta el momento.

En base a la nueva normativa, quienes tengan interés en brindar servicios de sellado de tiempo podrían también acreditarse como prestadores de servicios de confianza, para ello será necesario el dictado de una política que establezca las condiciones de esa acreditación, en virtud a que el Decreto solamente establece la posibilidad pero no los regula.

El literal d) es residual, dejando la norma abierta a servicios que puedan surgir en el futuro y que se deseen acreditar o controlar.

3.1 El Reglamento UE 910/014 de 23 de julio de 2014

Los prestadores de servicios electrónicos de confianza se encuentran regulados en la Unión Europea en el Reglamento UE 910/014 de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS), que derogó la Directiva 1999/93/CE y entró en vigencia el 1 de julio de 2016.

Pedro Canut plantea que: "…la gran novedad de este Reglamento es el reconocimiento de los Servicios de Confianza y los Servicios Cualificados de Confianza, además de la regulación de la firma electrónica (para personas físicas) y el sello electrónico (para personas jurídicas).

Efectivamente, la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica se ocupaba exclusivamente de la regulación de la firma electrónica y los prestadores de servicios de certificación basados en certificados reconocidos, en tanto que el Reglamento eIDAS contempla y regula asimismo los servicios de confianza consistentes en la entrega electrónica certificada, la certificación de sitios web, los servicios de sellado de tiempo y los servicios relativos a los documentos electrónicos; servicios éstos que, sin sustento en la Directiva 1999/93/CE, de 13 de diciembre, ni en la legislación nacional (Ley 59/2003, de 19 de diciembre, de firma electrónica) ya contaban, en España, con la cobertura del órgano de supervisión que, con una interpretación amplia de la Ley 59/2003, de 19 de diciembre, venía admitiendo las comunicaciones realizadas por prestadores de servicios que se dedicaban a otros servicios relacionados con la firma electrónica pero distintos a la generación de certificados de firma electrónica reconocida". (CANUT, Pedro J. "El Prestador Cualificado de Servicios de Confianza – Seguridad Jurídica en Internet").

De acuerdo a lo establecido en el Reglamento podemos decir que el servicio de confianza, es el servicio electrónico prestado habitualmente a cambio de una remuneración, consistente en:

> a) la creación, verificación y validación de firmas electrónicas, sellos electrónicos o sellos de tiempo electrónicos, servicios de entrega electrónica certificada y certificados relativos a estos servicios, o
> b) la creación, verificación y validación de certificados para la autenticación de sitios web, o
> c) la preservación de firmas, sellos o certificados electrónicos relativos a estos servicios.

Una distinción relevante en orden a los efectos jurídicos de un servicio de confianza y un servicio de confianza cualificado es que sólo una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita. La firma electrónica no cualificada de acuerdo a lo dispuesto en el párrafo 1 del artículo 25, no se le denegará efectos jurídicos ni admisibilidad como prueba en juicio.

Y el artículo 35 del Reglamento dispone que a los sellos electrónicos (para persona jurídica) no se les negará efectos jurídicos ni admisibilidad de prueba en juicio, aunque solo los sellos electrónicos cualificados disfrutarán de la presunción de integridad y corrección del origen de los datos a los que el sello esté vinculado.

A partir de julio de 2016, es obligatoria la exigencia de una cualificación administrativa a quienes deseen prestar servicios de confianza cualificados, según lo establece el artículo 21.1 del Reglamento. (…) Corresponde al organismo de supervisión verificar el cumplimiento de los requisitos y decidir, sobre la base de esta verificación, si otorga o no la cualificación al prestador de servicios de confianza y a los servicios que éste prestará. (RICO CARRILLO, Mariliana. "La entrada en vigencia de la regulación europea sobre servicios de confianza y su impacto en el comercio electrónico". Actas del XX Congreso iberoamericano de Derecho e Informática. Salamanca – España, 2016. Página 421).

En el Capítulo II del Reglamento se regula la identificación electrónica y la define en el artículo 3° numeral 1) como el proceso de utilizar los datos de identificación de una persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a una persona jurídica.

Se conceptualizan los datos de identificación de la persona como el conjunto de datos que permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a una persona jurídica.

También se define autenticación como el proceso electrónico que posibilita la identificación electrónica de una persona física o jurídica, o del origen y la integridad de datos en formato electrónico.

El objetivo del Reglamento con carácter general es la confianza en las transacciones electrónicas. Si bien se han realizado esfuerzos proteccionistas, las estafas a través de Internet son una realidad.

3.2 La normativa uruguaya

En nuestro país la Ley N° 18.600 establece en el artículo 2° lit. k) como uno de los requisitos de la Firma Electrónica Avanzada: "*haber sido creada utilizando un dispositivo de creación de firma técnicamente segura y confiable*…" y en el artículo 6° lit. C) garanticen que ha sido creada usando medios que el signatario mantiene bajo su exclusivo control.

La firma en nube o firma con control centralizado es cuando los dispositivos de creación de firma se alojan en un tercero denominado proveedor de servicios de confianza, su acceso se produce mediante factores de autenticación y el proveedor custodia el par de claves en instalaciones accesibles (la nube) y controla su acceso.

La firma en la nube no cumple con los dos requisitos establecidos en la ley. Por lo tanto, fue necesaria la ampliación de la norma, para facilitar la apropiación y el uso de la firma electrónica avanzada, pudiendo en esta nueva modalidad firmar desde cualquier dispositivo móvil, no siendo necesario portar e instalar un dispositivo físico que aloje el certificado y las claves.

Con tal finalidad se aprobó el artículo 28 de la Ley N° 19.535, reglamentado por el Decreto N° 70/018 del Poder Ejecutivo, normas que analizaremos en los apartados siguientes.

4. LA FIRMA ELECTRÓNICA AVANZADA CON CUSTODIA CENTRALIZADA

El artículo 31 de la Ley N° 18.600 en la redacción dada por la Ley N° 19.535 establece la creación en la Unidad de Certificación Electrónica (UCE) el Registro de Prestadores de Servicios de Confianza. Estos prestadores podrán prestar servicios de confianza *"que brinden seguridad jurídica a los hechos, actos y negocios realizados o registrados por medios electrónicos, entre ellos, la creación, verificación y validación de firmas electrónicas avanzadas con custodia centralizada, la identificación digital y el sellado de tiempo…".*

Para ello deben cumplir con las siguientes obligaciones:

> *"A. Custodiar diligentemente la clave del firmante o signatario y asegurar los medios para su generación, protección y destrucción.*
> *B. Establecer mecanismos seguros para realizar firmas electrónicas por orden del firmante o signatario de acuerdo con lo que determine la Unidad de Certificación Electrónica.*
> *C. Disponer de mecanismos seguros para el registro y autenticación de personas para su identificación digital".*

El inciso final del artículo establece que los prestadores de servicios de confianza deberán acreditarse ante la UCE.

El artículo 32 regula específicamente la firma electrónica avanzada con custodia centralizada, estableciendo que*: "La firma electrónica avanzada con custodia centralizada, realizada a través de un Prestador de Servicios de Confianza, si cumple con todos los requisitos legales tendrá la misma validez y eficacia jurídica que la firma electrónica avanzada"*.

El uso de la firma electrónica avanzada implica que no se depende más de un dispositivo físico, tampoco es necesario un lector para la cédula. En lugar de comprar el token, se va realizar un contrato con el proveedor de confianza para que aloje el certificado, del cual van a surgir todas las obligaciones para el prestador en cuanto a la custodia y el uso que se va a hacer del certificado. El proveedor puede coincidir con el prestador de servicios de certificación, tener las dos acreditaciones, de certificación y de confianza.

A los efectos de regular este nuevo escenario se aprueba el Decreto N° 70/018 que regula únicamente a los prestadores de firma electrónica avanzada con custodia centralizada y a los de identificación electrónica o digital, tal cual lo establece el artículo 1° al referirse al ámbito de aplicación objetivo de la norma.

El artículo 3° define en el literal b) a la primera de ellas como: "*la firma electrónica avanzada en la cual la clave privada del firmante se encuentra en custodia de un prestador de servicios de confianza acreditado, que realiza la firma bajo orden expresa del firmante*".

El artículo 4° establece las competencias de la UCE: acreditar y controlar los servicios prestados por los prestadores de servicios de confianza, establecer las especificaciones técnicas, normas y procedimientos respecto a los servicios de confianza y definir nuevos servicios de confianza.

Actualmente la UCE ya aprobó la política que deben cumplir los prestadores de servicios de confianza de firma electrónica avanzada con custodia centralizada de personas físicas y se encuentra en proceso de estudio la política que regula a los prestadores de identificación electrónica.

Los servicios de confianza de firma electrónica avanzada con custodia centralizada podrán consistir en la generación, almacenamiento y firma con certificados de firma electrónica avanzada de personas físicas y jurídicas.

Por tanto, es posible distinguir las siguientes situaciones:

a) El prestador que genera el certificado, almacena y firma, para los casos de personas físicas y jurídicas.
b) El prestador que solo almacena y firma, esta hipótesis aplica solo a personas jurídicas, como por ejemplo en los casos de certificados de personas jurídicas para facturación electrónica.

El artículo 9° del decreto establece la prohibición de migrar la clave privada para la firma avanzada de persona física, entre los diferentes prestadores de servicios de confianza, ni modificar el medio de almacenamiento dentro del mismo prestador de servicios de certificación. Por tanto, aquella firmas que se hayan emitido en dispositivos seguros de almacenamiento deben permanecer en ellos y el usuario deberá adquirir una nueva firma electrónica avanzada para utilizarla desde la nube.

5. IDENTIFICACIÓN ELECTRÓNICA

La identidad digital es el conjunto de informaciones publicadas en Internet sobre una persona y que componen la imagen que los demás tienen de ésta: datos personales, imágenes, noticias, comentarios, gustos, amistades, aficiones, etc. Todos estos datos nos describen en Internet ante los demás y determinan la reputación digital, es decir, la opinión que los demás tienen en la red. Esta identidad puede construirse sin que se corresponda exactamente con la realidad. Sin embargo lo que se hace bajo esa identidad digital tiene sus consecuencias en el mundo real y viceversa.

Como se puede observar el uso de Internet cada día va en aumento, por lo que la sociedad ha evolucionado considerablemente para formar comunidades en medios intangibles que se manifiestan día con día.

En este contexto es importante la identificación de la identidad ya que la información vertida directa e indirectamente por sí o por tercera persona puede producir efectos positivos y negativos en el mundo real. Un ejemplo de esta tendencia es cuando personas y empresas navegan por las redes sociales para investigar la identidad digital de un candidato y tomar decisiones sobre él/ella. (MOLINA MARTÍNEZ. Laura. "El Reconocimiento de la identidad digital a través de la firma electrónica avanzada". Hacia una Justicia 2.0. Actas del XX Congreso Iberoamericano de Derecho e Informática. Volumen II. Página106).

Como las contraseñas son incómodas y difíciles de recordar, para su eliminación la FIDO Alliance y W3C, los consorcios que regulan los estándares en el uso de la web están trabajando en WebAuthn, el nuevo estándar que regulará la autenticación de los usuarios y eliminará las contraseñas.

Este nuevo estándar cuenta con el respaldo de Google, Mozilla y Microsoft y, en lugar de la contraseña, apuesta por sistemas de identificación biométricos a los que los usuarios de móviles de última generación están más habituados. El nuevo estándar va a permitir que un usuario pueda identificarse de forma inequívoca en un sistema o navegador empleando la huella digital o su propio rostro, o bien confiar su identidad a un segundo dispositivo (un móvil, tableta o pendrive USB).

En materia de identificación electrónica el Reglamento de la UE parte de la importancia de asegurar la interoperabilidad transfronteriza en el seno de la UE, de las identificaciones nacionales, así como el reconocimiento y aceptación mutuos entre los Estados Miembros de los medios de identificación electrónica. Objetivo básico del Reglamento es garantizar la identificación y la autenticación electrónicas seguras para el acceso a los servicios transfronterizos en línea ofrecidos por los Estados miembros, pero preservando la libertad de los Estados respecto a la gestión de la identificación electrónica y las infraestructuras conexas. (DE MIGUEL ASENCIO, Pedro. "Unificación en la UE del régimen de los servicios de confianza para las transacciones electrónicas").

El artículo 33 de la Ley N° 18.600 en la redacción dada por la Ley N° 19.535 establece la equivalencia funcional de la identificación digital. *"La Unidad de Certificación Electrónica*

definirá los niveles de seguridad que proporcionen a la identificación digital el mismo valor y efecto jurídicos que la identificación presencial."

Por su parte, el Decreto N° 70/018 define en el artículo 3°, en el literal A) la autenticación electrónica como el proceso de identificar a una persona a través de un sistema informático mediante uno o más medios de identificación digital. En el literal C) establece los medios de identificación electrónica o digital como: "*la unidad material o inmaterial, procesable por un sistema informático, con una parte en control del sistema y otra en exclusivo control de la persona, ya sea mediante: su conocimiento; un dispositivo físico o lógico; algún rasgo físico o comportamental*".

Define además en el literal E) el Registro de identificación digital y en G) los servicios de identificación digital, como aquellos que realizan registros de autenticación electrónica de personas para su verificación por terceros.

En el Capítulo III del Decreto se encuentran regulados los servicios de identificación digital. Estableciendo el artículo 5° que éstos pueden contar con diversos niveles de seguridad, otorgándole competencias a la UCE para definir las condiciones para determinarlos, debiendo considerar el procedimiento de registro de identificación, los medios de identificación digital y el proceso de autenticación. Y siendo este organismo quien definirá los niveles de seguridad que proporcionen a la identificación digital el mismo valor y efectos jurídicos que la identificación presencial. Para que exista esta equivalencia, los prestadores de servicios de confianza que brinden este servicio deberán estar acreditados.

El artículo 7° establece que es responsabilidad de quien utiliza el servicio de identificación digital definir cuál es el nivel de seguridad que necesita, obviamente en virtud del servicio que se está brindando.

La UCE se encuentra trabajando en la política de Identificación digital para la cual se han tomado como referencia los lineamientos de identidad digital establecidos por el NIST y el marco que establece el eIDAS.

En el proceso de identificación digital tenemos que tener en cuenta el nivel de registro de la identificación digital, los medios de identificación digital y el nivel de autenticación electrónica.

Para el caso del Registro, podemos encontrar la existencia de 3 o 4 niveles, que van desde niveles muy bajos de seguridad hasta el nivel equivalente al presencial. Sin lugar a dudas, en nuestro país un alto nivel de identificación y por tanto equivalente al presencial requerirá al momento del registro la instancia presencial, pudiendo el proceso comenzar en línea, pero siendo necesaria la presencia física de la persona que solicita la acreditación de su identidad física a los efectos de vincularla con medios digitales y será necesaria la captura de datos biométricos del suscriptor y el tipo de medio digital asociado al solicitante es un certificado de firma electrónica avanzada otorgado dentro de la infraestructura de certificación electrónica de Uruguay.

Los medios de identificación electrónica digital que pueden ser considerados durante la etapa de autenticación son los siguientes:

a) Nombre de usuario y contraseña.

b) Lista de contraseñas, en soporte papel que posee el reclamante. Consiste en una lista de códigos a menudo en combinación con una contraseña estática o PIN dentro del sistema de autenticación.

c) Dispositivo de contraseña de un solo uso: es un dispositivo de hardware personal que genera una contraseña de "una sola vez", el cual es válido para una sola sesión de autenticación.

d) Certificado en software: es una clave criptográfica que normalmente se almacena en un disco, dispositivo USB u otro medio de dispositivo de comunicación. La autenticación se realiza probando la posesión y el control de la clave.

e) Certificado en hardware: es una tarjeta inteligente o medio similar que contiene una clave criptográfica protegida. La autenticación se realiza probando la posesión del dispositivo y el control de la clave.

d) Certificado electrónico reconocido de persona física: certificado de firma electrónica avanzada emitido por un prestador de servicios de certificación acreditado ante la UCE.

El tercer paso del proceso, la autenticación electrónica, como ya hicimos referencia, se encuentra definida en el artículo 3° literal A) del Decreto como "*el proceso de identificar a una persona a través de un sistema informático mediante uno o más medios de identificación digital"*.

El nivel de confianza que se puede plantear en un mecanismo de autenticación remota depende del nivel de seguridad que posea, los cuales están muy relacionados con los tipos de ataques y el medio de identificación digital utilizado durante el proceso de autenticación.

Las amenazas dentro de los procesos de autenticación pueden ser:

a) Fuerza bruta: es un ataque donde se intenta adivinar el secreto de la comunicación, por ejemplo una clave.
b) Eavesdropping: consiste en una escucha secreta o sigilosa. En la red, consiste en observar los mensajes que pasan por un canal de comunicación. Esos mensajes se almacenan para realizar un análisis fuera de línea de la información, obteniendo por ejemplo metadatos, que son utilizados para lanzar ataques sucesivos.

c) El secuestro: es un ataque que consiste en hacerse cargo de una sesión ya autenticada por un atacante y para aprender información sensible.

d) Retransmisión**:** es una forma de ataque donde una entidad maliciosa repite o retrasa previamente mensajes interceptados para obtener acceso a información confidencial.

e) *Man-in-the-middle*: es una forma de espionaje activo consiste en introducirse en la comunicación entre dos equipos para que todo el tráfico pase por él y poder así desencriptar sus datos, contraseñas, etc.

El nivel de seguridad del protocolo de autenticación lo hace o no susceptible de determinados ataques, por tanto el nivel de seguridad dependerá de a qué tipo de riesgos se encuentra expuesto.

De acuerdo a los niveles definidos durante el procedimiento es que se definen los niveles de seguridad de la identificación digital.

6. PRESTADORES DE SERVICIOS DE CONFIANZA

El capítulo V del Decreto N° 70/018 regula a los prestadores de servicios de confianza, estableciendo en el artículo 10 los requisitos para ser considerados tales, en el artículo 11 sus obligaciones, el artículo 12 establece los requerimientos técnicos y de gestión y el artículo 13 remite, en cuanto a la responsabilidad, a lo previsto en el artículo 20 de la Ley N° 18.600 respecto a los prestadores de servicios de certificación.
En el capítulo VI se establece cual es el procedimiento de acreditación de los prestadores de servicios de confianza. El artículo 14 establece los tres tipos de servicios de confianza que pueden brindarse, ellos son:

a) Generación, almacenamiento de certificados y firma de personas físicas y jurídicas.
b) Almacenamiento de certificados de personas físicas o jurídicas.
c) Identificación digital de personas físicas con niveles de seguridad equivalentes a la identificación presencial.

En el segundo caso de almacenamiento y firma será necesaria la existencia de un contrato que vincule al prestador de servicios de certificación con el prestador de servicios de confianza que proporcionará el servicio de almacenamiento.

Los requisitos para cada uno de ellos se encuentran regulados en los artículos 15 y 16 respectivamente.

El artículo 15, para los casos de prestadores de generación, almacenamiento y firma, remite a lo establecido en la Ley N° 18.600 y su Decreto reglamentario N° 436/011.

Para el caso de los prestadores que solo den servicio de almacenamiento y firma, el artículo 16 establece que no será necesario que se acrediten, teniendo la UCE facultades para controlar en cualquier momento la regularidad de los servicios prestados. Sí establece la obligación de que cuenten con procedimientos de acceso y resguardo de certificados, cláusulas contractuales y todo lo que establezca la UCE en las políticas específicas.

Al igual que para los prestadores de servicios de certificación se exige una garantía de solvencia económica, mediante la constitución de un seguro de responsabilidad por daños y perjuicios que pudiera ocasionar la prestación del servicio.

La resolución de acreditación tiene los siguientes efectos: la incorporar del prestador en el Registro de prestadores de servicios de confianza acreditados y la habilitación para prestar el servicio en el cual se acredite.

Los artículos 23 al 27 regulan la suspensión y revocación de la acreditación de los prestadores de servicios de confianza, tanto de los prestadores de firma electrónica avanzada con custodia centralizada como para los prestadores de identificación digital, así como el cese de las actividades de éstos.

En el capítulo VII se regula el control y supervisión de los prestadores de servicios de confianza acreditados, remitiendo al artículo 14 numeral 5° de la Ley N° 18.600 referente a las potestades sancionatorias de la UCE.

El artículo 30 establece el deber de colaboración en los siguientes términos: "*Los prestadores de servicios de confianza tienen la obligación de facilitar a la UCE toda la información y elementos necesarios para el ejercicio de sus funciones, así como la de permitir al personal inspector el acceso a sus instalaciones y la consulta de toda la documentación relevante*".

En forma complementaria a lo establecido en el artículo 30, el artículo 31 prevé el relacionamiento entre prestadores de servicios de certificación y prestadores de servicios de confianza, estableciendo que los primeros deberán informar a la UCE la existencia de acuerdos y convenios que suscriban con prestadores de servicios de confianza para la prestación de los servicios que se regulan.

Finaliza el artículo haciendo la referencia a que "*Dicha obligación se considerará cumplida mediante la entrega a la UCE del listado de los prestadores participantes. La UCE garantizará la confidencialidad de la información entregada*".

El artículo 31 le permite a la UCE conocer quiénes son los prestadores que brindan servicios de almacenamiento y firma, que si bien no están acreditados, posee el cometido de controlarlos.

7. CONCLUSIONES

La aprobación de las normas analizadas ha proporcionado a Uruguay un marco jurídico completo y garantista a los efectos de la utilización de la firma electrónica avanzada con custodia centralizada y la identificación digital.

El objetivo de la normativa es asegurar que el dispositivo de creación y almacenamiento de firmas electrónicas sea confiable y que el firmante tenga el acceso exclusivo a su clave de firma electrónica avanzada de persona física con una custodia centralizada, con un alto grado de confianza.

Como se mencionó en la introducción, los servicios permitirán firmar documentos evitando utilizar dispositivos adicionales para la firma como los token o los lectores de cédula de identidad, facilitando el proceso a los usuarios.

El otorgar la equivalencia de la firma en nube con la firma electrónica avanzada y de la identidad digital con la identidad electrónica constituye, sin lugar a dudas, dos herramientas poderosísimas para el avance de los proyectos de gobierno electrónico, especialmente el proyecto de trámites 100% en línea.

BIBLIOGRAFIA

MOLINA MARTÍNEZ. Laura. "El Reconocimiento de la identidad digital a través de la firma electrónica avanzada". Hacia una Justicia 2.0. Actas del XX Congreso Iberoamericano de Derecho e Informática. Volumen II.

RICO CARRILLO, Mariliana. "La entrada en vigencia de la regulación europea sobre servicios de confianza y su impacto en el comercio electrónico". Actas del XX Congreso iberoamericano de Derecho e Informática. Salamanca – España, 2016.

VIEGA RODRIGUEZ, María José y HERNANDEZ VARELA María Jimena. "Derecho Informático e Informática Jurídica II". Fundación de Cultura Universitaria". Montevideo, marzo, 2018.

VIEGA RODRIGUEZ, María José. "Derecho Informático e Informática Jurídica I". Fundación de Cultura Universitaria". Montevideo, octubre, 2017.

VIEGA RODRIGUEZ, María José y RODRIGUEZ, Beatriz. "Documento y firma. Equivalentes funcionales en el mundo electrónico. Ley N° 18.600 – Decreto N° 436/2011". Editorial CADE, junio 2012.

Formato electrónico

Canal TIC. Educación. Tecnologías de la información y comunicación. http://canaltic.com/internetseguro/manual/3_mi_identidad_digital.html Página visitada el 17 de abril de 2018.

CANUT, Pedro J. "El Prestador Cualificado de Servicios de Confianza – Seguridad Jurídica en Internet". https://www.blogespierre.com/2015/11/27/el-prestador-cualificado-de-servicios-de-confianza-seguridad-juridica-en-internet/ Página visitada el 25 de agosto de 2017.

[1]https://www.cromo.com.uy/el-fin-las-contrasenas-esta-aqui-llega-webauthn-n1223243?utm_source=planisys&utm_medium=Cromo-Titularesdelasemana&utm_campaign=Cromo-Titularesdelasemana2018&utm_content=27&ns_campaign=Cromo-Titularesdelasemana2018&ns_source=planisys&ns_linkname=27&ns_mchannel=Cromo-Titularesdelasemana Página visitada el 16 de abril de 2018.

SHELDON, Robert. "Qué buscar en un proveedor de almacenamiento en nube". http://searchdatacenter.techtarget.com/es/consejo/Que-buscar-en-un-proveedor-de-almacenamiento-en-nube Página visitada el 25 de agosto de 2017.

VIEGA RODRIGUEZ, María José y RODRIGUEZ, Beatriz. "Documento electrónico y firma digital. Cuestiones de seguridad en las nuevas formas documentales". Libro electrónico: www.viegasociados.com Montevideo, 2005.

WINKLER, Vic (J.R.). “Informática en nube: problemas legales y reglamentarios”. https://technet.microsoft.com/es-es/library/hh994647.aspx Página visitada el 25 de agosto de 2017.

“Prestadores de servicios electrónicos de confianza”. http://www.minetad.gob.es/telecomunicaciones/es-es/servicios/firmaelectronica/paginas/prestadores.aspx Página visitada el 25 de agosto de 2017.

LOS DERECHOS HUMANOS Y LA DEMOCRACIA MEXICANA EN LA ERA DIGITAL

Por: ***Ramón Gil Carreón Gallegos***
México

El progreso es imposible sin cambio, y aquellos que no pueden cambiar sus mentes no pueden cambiar nada.
George Bernard Shaw

El pasado proceso electoral mexicano del mes de julio en el que se eligió a presidente de la república, a las dos cámaras del parlamento federal, así como otros cargos de carácter estatal, representa un antes y un después en la historia reciente de México. El hecho de que por primera vez haya ganado la presidencia de la república un candidato de izquierda es un suceso que marca la historia del país de manera trascendental, sobre todo si se agregan varias circunstancias como el que haya sido el presidente electo con más votos en la historia del país, con 30 millones 47 mil 700 votos, que representa un 53.17% del total de los votos emitidos[1]; asimismo, según los resultados de la elección, en 31 de las 32 entidades del país, el partido de izquierda del candidato a la presidencia obtuvo la preferencia de los electores, lo que se tradujo también en una amplia mayoría en las dos cámaras del parlamento federal y en muchos parlamentos estatales[2].

Pero además de estos datos que dan cuenta de un hecho histórico para México por la trascendencia de la alternancia política, el pasado proceso electoral mexicano dio cuenta del auge inédito de las redes sociales y su importante influencia en el ánimo de los electores. De hecho, en su primer discurso como ganador, el candidato Andrés Manuel López Obrador agradeció a las "benditas redes sociales", lo que sin duda refleja el enorme impacto que tuvieron en la elección, frente al modelo tradicional de interacción a través de los tradicionales medios de comunicación que no lograron tener la influencia de otros procesos electorales pasados[3].

Los medios de comunicación impresa en su momento perdieron el monopolio ante la llegada de la televisión y ésta modificó sustancialmente la forma de interactuar con el conocimiento y con la realidad, prevaleciendo el hecho de ver sobre el de hablar, *"…el telespectador es más un animal vidente que un animal simbólico. Para él las cosas representadas en imágenes cuentan y pesan más que las cosas dichas con palabras…"*[4]. Sin embargo, con el paso del

[1] Tuvo AMLO 30 millones 47 mil votos, según cómputos distritales (en línea) México: El Universal. (Consulta: 12-07-2018). Disponible en: http://www.eluniversal.com.mx/elecciones-2018/computos-distritales-del-ine-dan-53-de-la-votacion-amlo

[2] México se tiñe de guinda; Morena conquista congresos, gubernaturas y alcaldías (en línea) México: Excelsior. (Consulta: 12-07-2018). Disponible en: https://www.excelsior.com.mx/nacional/mexico-se-tine-de-guinda-morena-conquista-congresos-gubernaturas-y-alcaldias/1249811

[3] Benditas redes sociales (en línea) México: El financiero. (Consulta: 13-07-2018). Disponible en: http://www.elfinanciero.com.mx/opinion/macario-schettino/benditas-redes-sociales

[4] SARTORI, Giovanni, *Homo Videns. La sociedad teledirigida*, Editorial Taurus, Argentina, 1998, p.26.

tiempo y el avance de la tecnología, hemos pasado a una "edad multimedia", desbancando a la televisión como la reina de esa "multimedialidad"[5], ya que no sólo unificó la palabra, el sonido y las imágenes, sino que como sostiene Sartori, introdujo realidades virtuales o simuladas[6].

Al día de hoy las TIC's (tecnologías de la información y la comunicación) se han convertido en un auténtico eje de la vida social, política y cultural, con la particularidad que supone un espacio democrático y plural en el que prácticamente cualquier persona puede no sólo acceder a un cúmulo enorme de información, sino que además puede difundir contenidos e interactuar con otras personas en un contexto de libertad muy amplia.

Según un estudio de la Asociación de Internet.MX sobre los hábitos de internet en México en el año 2018, creció un 12% los millones de personas con acceso a internet del año 2016 a 2017, alcanzando un total de 79.1 millones. Los datos reflejan además la edad cada vez más temprana a la que los niños tienen acceso a internet pues el país alcanza un 67% de penetración entre la población de personas mayores de 6 años[7].

El estudio revela que el del 66% de la población encuestada, tiene una madurez de uso del Internet de 8 años, mientras que el promedio total es de 7.1 años de navegación en la red. Asimismo, los datos reflejan el gran aumento del impacto de Internet y el desplazamiento de los medios de otros medios de comunicación tradicionales, ya que el tiempo promedio de uso total del Internet por cada internauta es de 8 horas con 12 minutos, mientras que el uso de televisión sin internet es de 3 horas y de radio sin internet es de 1 hora con 45 minutos[8].

Por otro lado, la información da cuenta que la comunicación a través de internet se da más a través de los Smartphones ya que ha experimentado un crecimiento del 76% en relación años anteriores, mientras que las laptop se usan un 66%, las Tablet un 51% y las PC un 39%.

El mayor uso que se le está dando al Internet es para lo relativo a redes sociales, como también para la gestión de correos electrónicos o mensajes instantáneos y en menor medida para asuntos relacionados con el gobierno, lo que da cuenta del déficit que aún existe en la interacción y el vínculo entre gobierno y ciudadanos a través de internet. El uso más frecuente que se le da al internet es para acceder a redes sociales con un 89%, para enviar o recibir mails un 84%, para enviar o recibir mensajes instantáneos (Chats) un 83%, para buscar información un 82%, para utilizar mapas un 73%, para escuchar música un 68%, para leer, ver o escuchar contenidos relevantes un 65%, para gestiones con gobierno solo un 29%.

Según los mismos datos del estudio, la red social más utilizada en México continúa siendo Facebook, además de que en promedio cada usuario pertenece al menos a 5 redes sociales.

---

[5] Sartori define a la multimedialidad como la unificación en un solo medio de la palabra escrita y hablada además del sonido y la imagen. *Ibídem,* p. 32.

[6] *Ídem*.

[7] Hábitos de Usuarios de Internet en México 2018. Estudio de la Asociación de Internet .MX (en línea) México: El financiero. (Consulta: 13-07-2018). Disponible en: https://webmarketingtips.mx/local/habitos-usuarios-internet-en-mexico-2018-7-417/

[8] *Ídem.*

Así Facebook tiene el 98% de uso por parte de los internautas, le sigue WhatsApp con un 91%, YouTube con un 82%, Instagram con un 57%, Twitter con un 49%[9].

Estos datos sobre el acceso a internet en México y sobre el uso masivo y creciente de las TIC's le dan sentido a la expresión del candidato presidencial ganador de agradecer a las "benditas redes sociales", porque sin lugar a duda el vínculo y la interacción que hoy en día tienen los ciudadanos con las redes contextualiza todos los aspectos de la vida social, política y cultural. De tal suerte que la propia vigencia de los derechos humanos y la consolidación democrática del país no pueden estar exentos de las TIC's.

La reciente elección dio muestra como nunca de la enorme influencia de las redes sociales en el ánimo de los ciudadanos a la hora de generar preferencias sobre tal o cual opción política, pero el proceso electoral también recordó la grave crisis que los derechos humanos atraviesan en México, pues al margen de los problemas añejos de desigualdad social, desempleo, falta de calidad en la educación y otros tantos, la violencia e inseguridad pública salieron a relucir en las elecciones como muestra de la crueldad del problema que vive el país desde hace algunos años. Solo por citar algunos datos, más de 25 mil homicidios dolosos registrados en el año de 2017 que significa una media de casi 70 muertes por día, las más de 200 mil muertes violentas registradas desde el 2006 en que se dio inicio a la guerra contra el narco, o los más de 120 políticos asesinados durante el proceso electoral de 2018, que al parecer representa un aumento del 470% respecto al proceso electoral del 2015[10].

Este contexto que vive México hace necesario reflexionar sobre la grave crisis que viven los derechos humanos y su nexo con la democracia en un escenario en donde las TIC's adquieren cada vez mayor relevancia e impacto en la toma de decisiones y en la consolidación de una determinada cultura política y jurídica.

El binomio de los derechos humanos y la democracia representa una de las conquistas mas importantes del liberalismo político ilustrado, y aunque la relación entre ambas ideas tiene nexos conceptuales sustanciales, la relación entre ambas no deja de tener tensiones importantes[11]. Esta tensión entre ambos conceptos adquiere además matices importantes si se asume que desde hace algún tiempo los espacios a través de los cuales las personas interactuamos con el conocimiento, con la cultura y con otras personas se han ido diversificando.

En ese escenario los derechos humanos y la democracia adquieren matices y tensiones importantes pues la solución de los problemas actuales necesariamente pasa por las nuevas tecnologías de la información y la comunicación.

Parece acertado afirmar que la medida de las tensiones entre derechos humanos y democracia se traduce en la visión que se tenga sobre los derechos humanos y sobre la democracia misma.

---

[9] *Ídem.*

[10] México: ¿por qué no hay más indignación internacional ante los miles de muertos y desaparecidos? (en línea) México: BBC. (Consulta: 14-07-2018). Disponible en: https://www.bbc.com/mundo/noticias-america-latina-44434406

[11] Sobre la relación entre derechos humanos y democracia *Vid.* VILLASEÑOR ALONSO, Isabel, La democracia y los derechos humanos: una relación compleja, *Foro Internacional,* No. 222, LV, 2015 (4), pp. 115-1138.

Por su contenido, los derechos humanos pueden ser concebidos desde una concepción liberal en el sentido de visualizar a aquellos como el producto de la aportación propiamente liberal, sustancialmente como derechos con una función negativa, como límites al poder público. En ese contexto, los derechos fundamentales serías los llamados derechos de libertad, los que permiten garantizar la independencia de las personas y un espacio de autonomía libre de injerencias indebidas, sobre todo del poder político.

Por otro lado, una concepción amplia de los derechos humanos supone considerarlos como derivados no sólo de la aportación liberal, sino, además, de la democrática y socialista y a las nuevas aportaciones de los llamados derechos de tercera y cuarta generación. En esa visión, no solo los derechos de libertad clásicos como la libertad de expresión, de imprenta, de circulación o de creencia deberían ser considerados derechos fundamentales, sino, además, con la misma jerarquía normativa e importancia moral son derechos fundamentales los derechos que contribuyen a la formación de las decisiones colectivas y los que permiten acceder a bienes y servicios de carácter social. Es decir, son también derechos fundamentales los derechos políticos como el derecho al voto y a ser votado, así como los derechos económicos, sociales y culturales como la educación pública, la vivienda, el trabajo, la seguridad social, la salud o la cultura. Esta visión de los derechos fundamentales supone concebir a la libertad en un sentido igualitario o material, no solo como igualdad de trato ante la ley o formal si se quiere. La libertad de las personas no solo implicaría un espacio de autonomía exenta de injerencias ajenas, pues además de esto, es necesario una actividad positiva del Estado, con el fin de remover los obstáculos que de hecho impidan el ejercicio efectivo de aquella libertad, no es una libertad puramente formal sino sobre todo material; en pocas palabras, no se trata de una concepción negativa de la libertad (aunque la supone) sino de una libertad real o igualitaria.

Una visión básica de la democracia es que se refiere a un sistema de gobierno en el que los ciudadanos eligen a sus representantes y gobernantes a través de elecciones limpias y transparentes, dentro de un sistema que los incluye en la toma pública de decisiones. Por si misma la democracia no es la solución de los problemas de una sociedad, sobre todo, resulta medular establecer el tipo de concepción de la democracia que se asuma, pues al igual que los derechos fundamentales, existen distintas concepciones sobre lo que puede significar democracia. Pero sea que se asuma una u otra concepción sobre lo que ha de ser una sociedad democrática, existen condiciones mínimas que deben estar presentes para que podamos hablar de una democracia política moderna, según Robert Dahl serían las siguientes:

a) El control de las decisiones del gobierno sobre política está constitucionalmente investido en los funcionarios electos.

b) Los funcionarios electos son elegidos en elecciones frecuentes y conducidas con limpieza en las que la coerción es relativamente poco común.

c) Prácticamente todos los adultos tienen derecho a votar en la elección de los funcionarios.

d) Prácticamente todos los adultos tienen derecho a presentarse como candidatos para cargos electivos en el gobierno.

e) Los ciudadanos tienen derecho a expresarse sin el peligro de un castigo severo, sobre asuntos políticos definidos ampliamente.

f) Los ciudadanos tienen derecho a buscar fuentes alternativas de información, las cuales están protegidas por la ley.

g) Los ciudadanos también tienen derecho a formar asociaciones u organizaciones relativamente independientes, incluidos partidos políticos y grupos de interés que sean independientes[12].

En el caso mexicano, pese a que el país tiene un sistema electoral formalmente eficiente que garantiza procesos electorales más o menos confiables desde una óptica procedimental, difícilmente se puede sostener que los ciudadanos tengan derecho a expresarse sin el peligro de un castigo severo si se toma en cuenta la grave crisis de violencia e inseguridad que se vive en el país.

Pero además de las características de la democracia procedimental antes apuntadas, autores como Philippe C. Schmitter y Terry Lynn Karl, agregan dos más, a saber:

a) Los funcionarios de elección popular deben ser capaces de ejercer sus poderes constitucionales sin estar sometidos a una oposición avasalladora de los funcionarios no electos. La democracia está en riesgo si oficiales militares, funcionarios públicos arraigados o administradores estatales conservan la capacidad de actuar independientemente de los civiles electos o incluso de las decisiones de veto tomadas por los representantes del pueblo.

b) La organización política debe ser autogobernada: ser capaz de actuar independientemente de constreñimientos impuestos por algún otro sistema que abarque demasiado[13].

Esta visión procedimental de la democracia es elemental para entender las funciones básicas del Estado liberal moderno en el que la soberanía popular es una condición esencial, de ahí que a lo largo de los años la democracia haya sido considerada como una forma de vida, como un sistema político que depende del consenso permanente y voluntario de los ciudadanos. En esa visión, la democracia como sistema político y como forma de vida sólo es posible y eficiente si tiene como resultados de su aplicación: la identidad cultural, la estabilidad económica, la justicia social y el consenso político, y por supuesto, un Estado de Derecho eficaz[14].

---

[12] SCHMITTER, PHILIPPE C., y TERRY LYNN K., Qué es… y qué no es la democracia, en *El Resurgimiento Global de la Democracia*, Instituto de Investigaciones Sociales, UNAM, 1996, p. 47.

[13] *Ídem.*

[14] THESING, Josef, *Estado de Derecho y Democracia.* Argentina: Fundación Konrad Adenauer- Stiftung-CIEDLA, Argentina, 1999, p. 15.

En cualquier caso, la visión procedimental de la democracia no se agota con la participación de los ciudadanos en los procesos electorales, pues la construcción de la voluntad general a partir del vínculo jurídico y político entre el Estado y sus ciudadanos es permanente. Si bien la lógica de las democracias representativas es que los representantes de los ciudadanos tienen una función delegada por los ciudadanos, lo cierto es que la voluntad social debe renovarse constantemente no sólo a través de los comicios, sino a través de otros espacios de comunicación. En tales circunstancias, una sociedad que se precie de ser democrática necesita forzosamente que sus integrantes participen activamente en sus decisiones[15]. Por ello, en los últimos años se ha detectado la necesidad de que los Estados generen mecanismos que acerquen a los ciudadanos al proceso político de toma de decisiones y que los aleje de la idea de que solo se participa de la democracia cada 3 o 6 años al ir a votar.

Así pues, la democracia exige participación y deliberación desde una óptica procedimental, pero como se expresó antes, la democracia parece hacer referencia además a otros aspectos que no son formales y que tienen que ver con las expectativas que giran en torno a la idea democrática.

Cuando se hace referencia al ideal democrático como aspiración de las sociedades modernas puede estarse haciendo referencia al menos a dos sentidos, por una parte, a una visión procedimental o formal de la democracia, que como ya se vio antes debe contener ciertos aspectos básicos, pero por la otra, puede tenerse una concepción material o sustancial de la democracia que supone o asume los contenidos formales y procedimentales pero que además requiere de otros parámetros para darle contenido.

Para el jurista y filósofo italiano Norberto Bobbio la democracia tiene un carácter predominantemente procedimental o formal, para él la democracia *"…en cuanto contrapuesta a todas las formas de gobierno…* (se caracteriza) *por un conjunto de reglas (…) que establecen quién está autorizado para tomar las decisiones colectivas y bajo qué procedimientos"* [16].

Esta visión formal o procedimental de la democracia es el núcleo duro de los Estados liberales clásicos producto de la ilustración en el que el respeto a los derechos individuales y la participación política resultan claves. Esta visión precisa de la existencia de instituciones electorales sólidas que garanticen la libre participación de los ciudadanos, la competencia equitativa entre las distintitas opciones políticas y sin duda, la protección y garantía de derechos fundamentales como la libertad de opinión, la libertad de expresión, la libertad de reunión y todas aquellas expresiones propias del liberalismo político.

15 BOREA ODRIA, Alberto, *Democracia*, en *Diccionario Electoral. Tomo I*., Instituto Interamericano de Derechos Humanos-IFE, México, 2003, p. 365.
16 BOBBIO, Norberto, *El futuro de la democracia,* Fondo de Cultura Económica, México, p. 14.

Para Ferrajoli esta visión de la democracia es precisamente procedimental pues se traduce únicamente en un método, en la forma en que se materializan las decisiones colectivas de la sociedad[17].
Con esta visión de la democracia se podría afirmar que muchas sociedades o regímenes de gobierno son democráticas pues como en el caso mexicano, tienen un sistema electoral confiable soportado por un conjunto de instituciones con cierta solidez que garantizan que se protejan los derechos a votar y a ser votado. Aunque como se ha dicho, esta aseveración debe ser matizada por el grave problema de inseguridad pública y violencia que vive México y que se ha manifestado en las altas cifras de políticos asesinados en el reciente proceso electoral, incluidos candidatos a puestos de elección popular.

Sin embargo, la visión formal de la democracia permite garantizar el cómo todos los ciudadanos eligen a sus representantes, pero no resuelve los problemas actuales sobre *qué* es lo que se debe decidir, es decir, cuál debe ser el contenido de las decisiones colectivas. De ahí que autores como Ferrajoli asuman que además del contenido formal o procedimental de la democracia, existe un contenido material que estaría integrado por una visión amplia de los derechos fundamentales y no sólo por los derechos de liberta y los derechos políticos, así, para una auténtica democracia sustancial sería necesario proteger además a los derechos patrimoniales[18]. En esta visión sustancial o material de la democracia que bien podría calificarse como política, liberal, civil y social[19], se asume que una sociedad democrática no sólo es aquella que tiene reglas e instituciones que garanticen el procedimiento para la toma de decisiones colectivas, sino que además se precisa de un sistema de instituciones que garantice la protección de los derechos económicos, sociales y culturales.

En esas condiciones la democracia vista desde una concepción amplia o sustancial que supone la protección y garantía de los derechos fundamentales desde una perspectiva integral, permite considerar otros factores que inciden directamente sobre el bienestar de la sociedad a fin de evaluar la calidad de la democracia en una sociedad determinada.

Para evaluar el desarrollo democrático de los países de América Latina desde el año 2002 la fundación Konrad Adenauer, junto a otras instituciones elabora un informe sobre el cumplimiento de los aspectos básicos de la democracia procedimental, pero además se evalúan otros indicadores que reflejan el avance, estancamiento o retroceso de la marginación o exclusión social, pero también de los aspectos básicos que permiten una auténtica participación de la ciudadanía en la toma de decisiones colectivas. Es decir, se evalúan aspectos que tienen que ver con el bienestar de la sociedad que de manera directa o indirecta hacen posible no sólo el cumplimiento de la formula democrática en su vertiente formal o procedimental, sino además en el cumplimiento de los derechos fundamentales de carácter prestacional que permiten mejorar la formula democrática en su aspecto sustancial o material.

[17] FERRAJOLI, Luigi, Sobre la definición de 'democracia'. Una discusión con Michelanagelo Bovero en *Isonomía* número 19, 2003, p. 227.
[18] *Ídem*
[19] *Ibídem,* p. 209.

Para el informe del año 2017 sobre el índice de desarrollo democrático en México, la fundación Konrad Adenauer contó con la colaboración de la Unión Social de Empresarios de México (USEM), el Centro de Estudios Políticos y Sociales (CEPOS), el Instituto Nacional Electoral (INE), así como el Colegio de México (ColMex). El índice mide cuatro dimensiones cada año, a saber: Dimensión I. Democracia de los ciudadanos, que evalúa el respeto de los derechos políticos y las libertades civiles; Dimensión II. Democracia de las Instituciones, que mide la calidad y la eficacia del sistema político; Dimensión III. Democracia social, que analiza la capacidad del sistema democrático para generar políticas que aseguren bienestar y desarrollo humano y; Dimensión IV. Democracia económica, que pondera la capacidad del sistema democrático para generar políticas que aseguren eficiencia económica[20].

Según los datos arrojados por este Índice en la Dimensión I sobre Democracia de los Ciudadanos, la percepción de los ciudadanos encuestados refleja lo siguiente:

a) Más del 60% de la población sospecha que las elecciones de gobernadores y legisladores no son ni libres ni justas;

b) casi un 90% de la población a nivel nacional cree que, en su estado, la corrupción está instalada en el gobierno;

c) el promedio del índice de percepción de derechos políticos a nivel nacional se ubica apenas por encima de los 4 puntos sobre 10 posibles, y

d) la violencia y la desigualdad aparecen como los elementos que más condicionan el ejercicio de las libertades civiles[21].

En ese contexto el índice revela que debido a la grave crisis de inseguridad que vive el país "el miedo ciudadano, la pérdida del espacio público a manos de delincuentes y crimen organizado, constituyen uno de los problemas más graves de la democracia mexicana que avanza y retrocede en este campo sin soluciones definitivas[22]."

Por lo que respecta a la Dimensión II sobre la Democracia de las Instituciones Calidad Institucional y Eficiencia Política, el índice refleja un déficit que se ha venido dando en todos los informes de cada año, alcanzando en esta ocasión el valor promedio más bajo de la serie con 3,685 puntos.

Según el informe, las causas principales de ese déficit en Democracia de las Instituciones son:

a) Participación en las decisiones públicas, que evidencia los escasos niveles de participación ciudadana en los asuntos públicos, tanto por ausencia de compromiso ciudadano como por el desaliento a la participación desde estructuras políticas y burocráticas que entienden que "a menor participación ciudadana, mayor tranquilidad para funcionarios y dirigentes".

[20] Konrad-Adenauer, *Índice de Desarrollo Democrático de México. IDD-MEX 2017*. Konrad-Adenauer, México, 2017, p. 8.
[21] *Ibídem*, p. 49
[22] *Ibídem*, p. 52 y 53.

b) Accountability que aunque tiene un promedio más alto, evidencia problemas en los mecanismos de transparencia y controles cruzados que garantizan que se vigila el uso de los fondos públicos y la toma de decisiones justas y equilibradas en la administración de los intereses de la comunidad.

c) Desestabilización, la existencia de grupos de ciudadanos que no se sienten incluidos en las políticas públicas y sus beneficios o que, simplemente, no encuentran que sus derechos estén respetados en el sistema político institucional, por lo que se autoexcluyen del sistema y actúan, muchas veces con violencia en el espacio público para hacer oír su voz.

d) Intervención Federal/Crisis de Gobierno, que evidencian la debilidad política e institucional de algunas entidades federativas para resolver el control de su espacio público y la plena vigencia de las leyes[23].

La Dimensión III sobre Democracia Social – Capacidad para generar políticas que aseguren bienestar, se registró un ligero avance general de poco más del 3%. Quince estados mejoraron sus posiciones relativas en comparación con el 2015 y otras 16 descendieron.

Por último, la Dimensión IV sobre la Democracia Económica – Capacidad para generar políticas que aseguren eficiencia económica, es destacable que, según el informe, "hubo buenos niveles de consumo, de crédito, ayudaron las remesas, algunos aumentos en los salarios, algo de empleo. En general el sector terciario se ha manejado bastante optimista y es lo que ha mantenido a la economía creciendo por arriba del 2%.", sin embargo, por otro lado, un aspecto negativo fue el bajo crecimiento económico del país, ya que creció apenas por encima del 2%, mientras que en el 2015 creció 2.5%. Asimismo, si bien el desempleo bajó al 4.1%, el sector informal emplea a casi el 60% de la población económicamente activa. Y sin duda, un dato que sigue trastocando el bienestar generalizado es que más del 45% de la población vive en pobreza[24].

Teniendo en cuenta las cuatro dimensiones analizadas en el Índice de Desarrollo Democrático en México en el 2017, la valoración no es positiva pues además de la percepción de los ciudadanos sobre determinados aspectos clave para una sociedad democrática como la confianza en las instituciones o en los gobernantes, existen datos ciertos que reflejan una realidad material del país que impide asegurar condiciones de bienestar para la mayoría.

Con la grave crisis de inseguridad pública y violencia que vive el país es difícil asegurar que México tiene consolidada la formula democrática desde una perspectiva procedimental, pues si bien existen instituciones electorales confiables en términos generales, por otro lado no existen la garantía plena para la libre expresión de ideas, pues la amenaza constante y real existe tanto para los ciudadanos en general como para quienes tienen la intención de participar en un proceso electoral determinado.

[23] *Ibídem,* p. 65.
[24] *Ibídem,* p. 98

El panorama se torna más complejo si se asume una concepción sustancial o material de la democracia en la que se plantea la protección y vigencia de los derechos fundamentales desde una perspectiva amplia, pues sin lugar a duda son varias las asignaturas pendientes para lograr un estado de bienestar generalizado.

Parece en todo caso que un Estado de Derecho en el que los derechos fundamentales sean realidad cotidiana, así como la consolidación de la formula democrática de una sociedad desde una perspectiva constitucional y material, precisan de cambios estructurales en el Estado mismo y en la sociedad, pero, además, se requiere de una mediana confianza en las instituciones y un mediano interés en los asuntos públicos del país.

Ante un escenario donde los canales de comunicación e interacción con el conocimiento y entre personas mismas han cambiado, el vínculo entre ciudadanos y gobierno debe transformarse y adaptarse a la nueva realidad. El flujo de información en internet y en el caso concreto de las redes sociales se da en un marco democrático y plural, sobre todo porque prácticamente cualquier persona tiene la facilidad de acceder, reproducir y difundir información sobre cualquier tema o personas, en un marco de libertad de expresión que es una de las piedras angulares de una sociedad informada y de un régimen democrático de Derecho. El internet y las redes sociales han potenciado la libre expresión de ideas debido al gran alcance que tienen aquellas y a su vocación democrática. El internet, permite que cada individuo se convierta en un medio de comunicación por sí mismo, al expresar sus opiniones, y difundir información.

La reciente elección presidencial en México ha dado cuenta del gran impacto e influencia que tienen las TIC's y en concreto las redes sociales. De ahí que resulte necesario replantear las políticas públicas de comunicación social tradicional, pues hoy en día es al menos cuestionable la eficacia de los medios tradicionales como la prensa escrita, la radio o la televisión como medios para difundir las obras y programas sociales, así como para servir de vínculo con los ciudadanos con el gobierno.

Es indiscutible el enorme potencial de las TIC's y las redes sociales en concreto, debido en gran medida a la rapidez, pluralidad y apertura que las caracteriza. Sin duda alguna, hasta ahora ese gran potencial se ha manifestado sobre todo para la crítica permanente y ciertamente hasta para desinformar a través de las llamadas *Fake news*; habría que promover desde los gobiernos, la academia y todos los sectores que las "benditas redes sociales" construyan y promuevan la cultura y los hábitos tan necesarios para consolidar una democracia constitucional en la que los derechos fundamentales sean la política de Estado y la base cultural de la sociedad.

REFERENCIAS BIBLIOGRAFICAS Y RECURSOS DE INFORMACIÓN

BOBBIO, Norberto, *El futuro de la democracia*, Fondo de Cultura Económica, México, 1986.

BOREA ODRIA, Alberto, *Democracia*, en *Diccionario Electoral. Tomo I.*, Instituto Interamericano de Derechos Humanos-IFE, México, 2003.

Benditas redes sociales (en línea) México: El financiero. (Consulta: 13-07-2018). Disponible en: http://www.elfinanciero.com.mx/opinion/macario-schettino/benditas-redes-sociales
FERRAJOLI, Luigi, Sobre la definición de 'democracia'. Una discusión con Michelanagelo Bovero en *Isonomía* número 19, 2003. p. 227.
Hábitos de Usuarios de Internet en México 2018. Estudio de la Asociación de Internet .MX (en línea) México: El financiero. (Consulta: 13-07-2018). Disponible en: https://webmarketingtips.mx/local/habitos-usuarios-internet-en-mexico-2018-7-417/
Konrad-Adenauer, *Índice de Desarrollo Democrático de México. IDD-MEX 2017.* Konrad-Adenauer, México, 2017.
México: ¿por qué no hay más indignación internacional ante los miles de muertos y desaparecidos? (en línea) México: BBC. (Consulta: 14-07-2018). Disponible en: https://www.bbc.com/mundo/noticias-america-latina-44434406
México se tiñe de guinda; Morena conquista congresos, gubernaturas y alcaldías (en línea) México: Excelsior. (Consulta: 12-07-2018). Disponible en: https://www.excelsior.com.mx/nacional/mexico-se-tine-de-guinda-morena-conquista-congresos-gubernaturas-y-alcaldias/1249811
SARTORI, Giovanni, *Homo Videns. La sociedad teledirigida*, Editorial Taurus, Argentina, 1998.

SCHMITTER, PHILIPPE C., y TERRY LYNN K., Qué es… y qué no es la democracia, en *El Resurgimiento Global de la Democracia*, Instituto de Investigaciones Sociales, UNAM, 1996.
THESING, Josef, *Estado de Derecho y Democracia.* Argentina: Fundación Konrad Adenauer- Stiftung-CIEDLA, Argentina, 1999.

Tuvo AMLO 30 millones 47 mil votos, según cómputos distritales (en línea) México: El Universal. (Consulta: 12-07-2018). Disponible en: http://www.eluniversal.com.mx/elecciones-2018/computos-distritales-del-ine-dan-53-de-la-votacion-amlo
VILLASEÑOR ALONSO, Isabel, La democracia y los derechos humanos: una relación compleja, *Foro Internacional*, No. 222, LV, 2015 (4), pp. 115-1138.

"REGULACIÓN JURÍDICA DE LOS DEEPFAKES"

Por: ***Julio Alejandro Téllez Valdés***
México

a) Introducción

Actualmente la *Inteligencia Artificial (IA)* por sus siglas, es uno de los temas que mayor impacto está teniendo en el sector de las TIC. Es evidente que vivimos en un mundo cada vez más conectado e inteligente, pues a través de los años las nuevas tecnologías se han convertido en herramientas que sin duda, han facilitado las tareas del hombre de manera considerable.

La inteligencia artificial tiene muchos usos, anteriormente se pensaba que el crear videos realistas generados por computadora, solo estaba disponible para producciones hollywoodenses con grandes presupuestos, ahora aplicaciones como *Snapchat* incluyen algunas tecnologías rudimentarias para transformar el rostro sin tener que recurrir a los grandes recursos del cine.

Hoy en día es fácil crear un algoritmo que pueda emular actividades propias del ser humano y que incluso puede ser capaz de analizar datos en grandes cantidades *(big data),* identificar patrones y tendencias y, por lo tanto, formular predicciones de forma automática, con rapidez y precisión, este es uno de los usos favorables de la inteligencia artificial aplicada.

Sin embargo, en los últimos meses han surgido herramientas mucho más poderosas para hacer posible el "*face swapping"* o intercambio de rostros, siendo esta herramienta una aplicación que permite animar, a partir de fotografías, el rostro de una persona, luego genera una versión digital que puede sobreponerse en cualquier video, con esto se desata un fenómeno llamado *Deepfakes,* el cual es un acrónimo que une las palabras *"Deep learning"* (aprendizaje profundo) y *"Fake"* (falso).

Esta tecnología consiste en sintetizar imágenes a través de un algoritmo de inteligencia artificial sobre videos existentes y hacerlas pasar por verdaderas. En otras palabras, los *deepfakes* hacen que sea relativamente fácil crear transformaciones faciales realistas y dejar pocos rastros de manipulación, así poner el rostro de cualquier persona en situaciones poco deseables.

La principal diferencia entre estos dos fenómenos es que mientras el *face swapping* es el nombre que se le da al hecho de crear imágenes sobreponiendo un rostro en un cuerpo diferente por medio de una aplicación o software, los *Deepfakes* son como tal el uso malicioso o ilegal que se le da a este tipo de herramientas creando una identidad falsa, lo que a su vez origina que se actualicen disposiciones legales desde el punto de vista penal como delitos de suplantación de identidad o difamación y desde un punto de vista civil como daño moral, que de acuerdo con Volochinsky consiste: *"en el dolor, la aflicción y/o el pesar que causa a la víctima el hecho ilícito. En este sentido no afecta al patrimonio sino a los*

sentimientos, afectos o creencias."[1] Esto a causa de que su identidad ha sido suplantada y puesta en situaciones poco agradables.

Los *Deepfakes* son una de las formas más nuevas de manipulación digital nociva, no es difícil imaginar que esta tecnología se utilice para desacreditar a políticos, artistas, deportistas y personalidades públicas o incluso tender trampas a cualquier persona para inculparla de algún delito o simplemente usar su imagen y ponerla en situaciones comprometedoras no consentidas o realizadas.

Además de la propagación de noticias falsas *(Fake news)*, las redes sociales se enfrentan a un nuevo reto: evitar este tipo de contenidos en el que se utilicen algoritmos para realizar *Deepfakes*, circulen por sus plataformas libremente.

Principalmente los *deepfakes* se han creado para la obtención de la identidad personal de una persona, con el fin de tener acceso a sistemas o plataformas electrónicas ya sean bancarias o del lugar de trabajo de la persona con el fin de acceder a los datos personales de ésta y generar un daño directo en su persona suplantando su identidad y/o desfalcando sus cuentas bancarias realizando transacciones que el titular no consintió, entre otros hechos ilícitos que se pueden realizar.

Este fenómeno de los *deepfakes* ha surgido a través del mal uso que se ha dado a dado a herramientas como la *Realidad Aumentada (AR)* por sus siglas en inglés, o las *Computer-Generated Imagery (CGI)* o lo que es lo mismo, Imágenes Generadas por Computadora, tecnologías que han sido una de las técnicas más utilizadas en el cine de la ciencia ficción, permitiendo que esta tecnología haga parecer la ficción lo más real posible. No obstante estos hechos ilícitos atentan contra derechos fundamentales de las personas como la privacidad, la intimidad, la dignidad, entre otros. Por lo que es necesario conocer el alcance que fenómenos como los *deepfakes y face swapping* han tenido alrededor del mundo, la forma en la que se operan y las medidas que se han tomado para prevenir el incremento de incidentes por el uso de tecnologías de inteligencia artificial y la manera en que se han pronunciado algunos de los países afectados considerando las consecuencias legales y alcance que fenómenos producidos por el uso erróneo de estas herramientas podrían llegar a alcanzar, así como los riesgos y amenazas que se generan en el ámbito jurídico.

Es por ello que a continuación se abordaran algunas de las tecnologías de inteligencia artificial que permiten crear este tipo de diseños realistas y que, si bien tienen relación con las herramientas que producen los *deepfakes*, es necesario identificar cada una para analizar su diferente aplicación y alcance, así como la forma en que se ha tergiversado su aplicación para fines maliciosos.

b) Realidad Aumentada: *Augmented Reality (AR)*

Anteriormente se mencionó a la aplicación de *Snapchat*, como una plataforma rudimentaria y de uso masificado para realizar modificaciones en el rostro por medio de filtros de realidad

[1] VOLOCHINSKY, Bracey Wilson, 226 preguntas en derecho civil. Contratos y responsabilidad extracontractual, Santiago, Editorial Jurídica La Ley, 2002, p. 177.

aumentada, la cual aunque tiene cierta relación con la tecnología que crea *deepfakes,* aquella combina elementos del mundo real con la información disponible en el mundo digital, generalmente representada en forma de imágenes, animaciones, etc. Estos datos virtuales interactúan con la imagen de un objeto real capturado por la cámara de un dispositivo electrónico: *Smartphone,* tableta o gafas conectadas a Internet a los cuales se les instala un *software* tipo *app* para poder operar.

En este sentido, las aplicaciones como *Snapchat* pueden no representar mayor conflicto, debido a que los elementos que implanta en el rostro por medio de la realidad aumentada no representan una amenaza para la identidad de una persona, debido a que normalmente en el uso de este tipo de aplicaciones el usuario lo realiza de manera voluntaria y la aplicación lo emula de manera sobrepuesta al rostro. No obstante, esto es un parámetro para considerar el avance que ha tenido la tecnología y su alcance para cualquiera que disponga de un teléfono inteligente, incluyendo los usos que le puede dar a la misma.

El uso de la realidad aumentada aunque puede generar un engaño en cuanto a una identidad falsa frente a terceros, no es complicado poder identificar cuando se está utilizando alguna de estas herramientas, debido a los elementos que se implantan en la realidad son únicamente perceptibles por medio de otro dispositivo con la capacidad de identificar los objetos a través de un *software.*

Las aplicaciones de realidad aumentada no presentan mayor peligro al detectar la sobreposición de una imagen en el rostro, o entorno de la persona, pues es simple detectar la "falsedad" del filtro, sin embargo, no se descarta a futuro sean perfeccionadas las apps al alcance de todos mediante cualquier tienda de aplicaciones de nuestros dispositivos y estás sean mucho más estructuradas para crear un filtro más idóneo y adaptable a los rostros humanos.

c) Imágenes Generadas por Computadora: *Computer-Generated Imagery (CGI)*

Sin duda las *CGI* fueron una de las innovaciones tecnológicas más importantes del siglo anterior, específicamente para la industria del cine, debido a la enorme complejidad que representaba en ese entonces comprender que una computadora pudiera crear modelos impresionantemente parecidos a los reales o bien crear diseños desde cero de algún objeto o sujeto en particular.

Las Imágenes Generadas por Computadora se mostraron por primera vez en el año de 1973 en la película *Westworld* para crear un modelo de robot. No obstante, cabe mencionar que el costo que generaba el uso de estas tecnologías era sumamente considerable, debido a las especificaciones técnicas de las computadoras, además de que quienes operaban éstas debían tener la capacidad de conocer cómo se ejecutaba el software para crear los diseños.

Para el funcionamiento de esta tecnología los protagonistas deben llevar un traje con numerosos puntos de referencia. Estos reflejan luz infrarroja, que es emitida y recibida por un sistema de cámaras especial. Los actores deben moverse en una rejilla de coordenadas que acaba en la computadora. Finalmente, un software transfiere los movimientos al modelo digital.

La función principal de esta tecnología es crear un diseño casi idéntico de una persona, para lo cual es necesario un modelo para realizar movimientos y posteriormente son adecuados a los de la persona original, con el fin de hacer parecer que el modelo principal está actuando por sí. Además, es posible también crear seres vivos completamente desde cero a través de las *CGI,* lo que evidentemente disminuye la costosa inversión que debería hacerse en efectos especiales.

Es cierto que en un principio esta tecnología fue diseñada para ofrecer una herramienta que creara efectos fantásticos en las filmaciones y a su vez, que facilitara el trabajo de los actores, ya que en ocasiones algunos movimientos eran riesgosos, complicadas de realizar o en el peor de los casos, uno de los protagonistas fallecía dejando inconcluso el rodaje del filme.

La evolución de la tecnología en la industria del cine ha llevado a los CGI a una amplia gama de variedades, sin olvidar la esencia, como la recreación hoy en día de paisajes asombrosos con características del mundo real, así como los filtros en tercera dimensión para dar vida a los superhéroes en la pantalla grande, e incluso el resucitar actores fallecidos propiciando un avance considerable para el mundo tecnológico.

En unos años seguro estaremos viendo en pantalla grande hologramas casi palpables emulando e interactuando con otros actores para recrear y dar vida nuevamente.

d) Deepfakes y Face Swapping

Anteriormente se mencionó que el término de *deepfakes y face swapping* aluden a los hechos ilícitos realizado por medio de tecnologías de inteligencia artificial y el mal uso que se le ha dado a estas herramientas. Sin embargo, es necesario precisar la diferencia entre estos dos términos.

Los *deepfakes* es una recopilación de diferentes fotografías para crear videos manipulados utilizando tecnología de intercambio de caras a través de la inteligencia artificial, permitiendo de esta manera que el rostro del protagonista sea reemplazado por la de otra persona, incluyendo movimiento y expresiones faciales que parecen auténticas. Esta tecnología está enfocada a la creación de videos.

Por su parte el *face swapping* tiene un funcionamiento sencillo, siendo una tecnología que permite elegir la fotografía de una persona y reemplazar el rostro de ésta con el del usuario.

El uso de tecnologías que permiten hacer intercambio de rostros es cada vez más habitual, debido al fácil manejo y uso que representa para los usuarios. No es necesario tener una computadora con una GPU, de gran potencia para realizar estas fotografías a diferencia de otras tecnologías, aunque es importante destacar que para realizar *face swapping* únicamente podrán obtenerse resultados positivos al realizar imágenes y no videos como sí lo permiten otras tecnologías de inteligencia artificial.

En el procesamiento para generar *deepfakes,* si bien es cierto que los resultados pueden parecer fascinantes, existen claras limitaciones de lo que se puede lograr con esta tecnología hoy en día, entre ellas se encuentran:

1. Solo funciona si hay muchas imágenes del objetivo: Para poner a una persona en un video, se necesitan del orden de 300 a 2000 imágenes de su rostro para que el software pueda aprender a recrearlo. El número depende de cuán variados sean los rostros y qué tan cercanos coincidan con el video original.

2. El algoritmo puede ser deficiente al generar imágenes de un ángulo de perfil: debido a que en general, las imágenes recopiladas de una persona están orientadas hacia el frente (por ejemplo, *selfies*) es por ello que sí se está creando un *face swapping* puede verse limitados las expresiones que el algoritmo logre generar.

3. La construcción de modelos puede ser costosa, además de necesitar por lo menos un modelo para cada par de personas. Este alto costo de creación del modelo hace que sea difícil crear una aplicación gratuita o barata con la esperanza de que se vuelva viral. Por supuesto, no es un problema si los clientes están dispuestos a pagar para generar modelos.

4. La ejecución de modelos es bastante económica, el tiempo estimado de procesamiento ronda entre 5 y 20 veces la duración de un video para crear un intercambio cuando se ejecuta en una GPU, por ejemplo, un video de 1 minuto a una resolución de 1080p demora alrededor de 18 minutos en generarse. Es por ello que para obtener resultados más impresionantes se necesita una GPU, la cual tiene mayor potencia para procesar que un *Smartphone.*

No obstante, es importante mencionar qué aunque existen algunas limitantes para la generación de *deepfakes* es claro que sólo es cuestión de tiempo para que estas limitaciones sean superadas por la inteligencia artificial en algunos años.

Fuente de la imagen: https://www.xlsemanal.com/conocer/tecnologia/20180713/noticias-falsas-creadas-con-videos-falsos-inteligencia-artificial.html#ns_campaign=rrss&ns_mchannel=xlsemanal&ns_source=tw&ns_fee=0&ns_linkname=sem28-conocer-mentira

e) Regulación Jurídica Internacional: *Datos Biométricos*

El fenómeno de los *deepfakes* y *face swapping* han representado riesgos y amenazas en los últimos años a nivel internacional. Sin embargo el alcance de esta situación pasaba desapercibida debido a que no se consideraba cómo aplicaciones o programas que en principio se desarrollaron para fines de uso profesional e inclusive con la evolución de los nuevos *Smartphones* en los cuales la inteligencia artificial se ha integrado en el software como parte esencial de estos dispositivos, permitiendo de esta manera que cualquier persona pueda tener acceso a estas tecnologías, para hacer un uso menos profesional pero asimismo más económico. Es por ello que respecto a las nuevas amenazas e incidentes registrados en los últimos meses, diversos países se han pronunciado respecto a estos fenómenos para proteger los datos personales de los usuarios. Entre ellos se encuentran los países miembros de la Unión Europea.

El término de *datos personales* se ha ido modernizando a través de los años. Anteriormente se consideraban a esta información como datos que permitían identificar a una persona por su nombre, edad, domicilio, formación académica y profesional, entre otros. No obstante, las nuevas tecnologías han ampliado aspectos de la persona en cada individuo permitiendo de esta manera resguardar su privacidad e intimidad. Es por ello que los *datos biométricos* son una parte fundamental del ser humano relativas a las características físicas y fisiológicas lo que permite hacer una identificación más sustancial.

Los Datos Biométricos según el Reglamento General de Protección de Datos (GDPR) por sus siglas en inglés son definidos como: *"datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos."*[2] Es importante sabes que mientras que los datos biométricos de una persona pueden suprimirse o alterarse, la fuente de la que se han extraído en general no puede ser modificada ni suprimida.

Ahora bien, entre los datos biométricos que refieren a características físicas y fisiológicas se encuentran:

- *La huella digital.*
- *El reconocimiento facial.*
- *La retina.*
- *El iris.*
- *La geometría de la mano o de los dedos.*
- *El ADN.*

En este sentido, las características principales de los datos biométricos son las siguientes:

- *Universales:* Debido a que son datos con los que contamos todas las personas.

[2] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, Reglamento General de Protección de Datos (GDPR), consultado el: 12 de junio de 2018, recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

- *Únicos:* Ya que no existen datos biométricos con las mismas características y de esta manera nos distinguimos de otras personas.
- *Permanentes:* Esto debido a que en la mayoría de los casos, se mantienen a lo largo del tiempo en cada persona.
- *Medibles:* Esto es de manera cuantitativa.

El objeto principal de un sistema biométrico es reconocer a las personas, es decir, volver a conocer a una persona que ya ha sido identificada y registrada previamente. En otras palabras la identificación puede realizarse de manera manual o automatizada, comparando datos biométricos de una persona con una plantilla previamente registrada en el sistema y que a su vez está relacionada con una identidad específica.

Por otra parte, como se mencionó anteriormente una de las disposiciones legales más nuevas relativo a la protección de datos personales es el Reglamento General de Protección de Datos. El cual fue una iniciativa de los países miembros de la Unión Europea.

Dicho reglamento es de carácter obligatorio y se aplicará a responsables o encargados de tratamiento de datos establecidos en la Unión Europea, pero también se amplía a aquellos fuera de ésta**,** siempre que lleven a cabo tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento.

El Reglamento General de Protección de Datos (GDPR) que entró en vigor el 25 de mayo de 2018 indica que el consentimiento debe ser libre, informado, específico e inequívoco. En este sentido es necesario que los interesados manifiesten su consentimiento para que sus datos puedan ser recolectados, los fines para los que lo hacen, cesiones a terceros, duración del tiempo en que se conservaran los datos, entre otros aspectos. Otorgando nuevas facultades y nuevos derechos para los usuarios, además de garantizar una gestión de los datos más clara y transparente.

De acuerdo a lo anterior, el nuevo reglamento obliga a un gran número de aplicaciones a actualizar sus políticas de privacidad, todo esto debido a que ahora deben apegarse a lo establecido en el GDPR y evitar sanciones relativas a un uso incorrecto de los datos personales de los usuarios, las cuales podrían alcanzar hasta el 4% de la facturación mundial o multas hasta por veinte millones de euros.

No obstante, es importante señalar que a nivel internacional se ha tratado de regular también el delito de fraude, tal es el caso de la Organización de las Naciones Unidas, institución que emitió el "Manual sobre los delitos relacionados con la identidad", mismo que fue elaborado tras la publicación del estudio de la Naciones Unidas sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos en el año 2007, solicitado por la Oficina de Naciones Unidas contra la Droga y el Delito.

Dicho estudio contribuyó en dos importantes temas:[3]

[3] UNODC, "Manual Sobre los Delitos Relacionados con la Identidad", disponible en: https://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf, consultado el: 12 de junio de 2018.

"En primer lugar, adoptó un enfoque amplio del concepto de "delito relacionado con la identidad" y lo concibió de manera que abarcara todas las conductas ilícitas relativas a la identidad, incluidos los delitos frecuentemente denominados "fraude de identidad" y "hurto de identidad". En segundo lugar, abordó los problemas planteados por el delito relacionado con la identidad desde una perspectiva nueva de derecho penal, así como el uso indebido de la identidad como una forma particular del delito, por oposición al criterio tradicional de tipificar otros actos delictivos cometidos con identidades falsas. El estudio también abordó las diferencias y las contradicciones en los conceptos y las definiciones, en los distintos contextos nacionales, relativos al fraude y la falsificación de la identidad y su uso indebido con fines delictivos, y esclareció varios aspectos que revelan el carácter multifacético y complejo del problema."

En este sentido es importante saber que en la normativa internacional existe un gran acervo de legislación que prevé asienta las bases y disposiciones relativas para garantizar la protección de datos personales, la prevención de delitos que atenten contra la identidad y sus sanciones. Lo cual es un precedente para cada país en el cual exista algún vacío legal a causa de los nuevos ilícitos realizados a través de las nuevas tecnologías de *Inteligencia Artificial*.

f) Regulación Jurídica Mexicana: *Datos Biométricos*

Por su parte, en México, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), emitió una Guía para el Tratamiento de Datos Biométricos[4] el pasado mes de marzo de 2018, en donde se establecen las bases relativas a los datos biométricos, sus implicaciones, principales características, principios, deberes y prerrogativas relativas a la protección de datos personales, obligaciones y recomendaciones en torno a su cumplimiento, entre otros aspectos. Además, advierte a los particulares sobre los riesgos que implica entregar a esas personas sus datos, por lo que se busca un equilibrio entre los sistemas de seguridad y la protección de los derechos individuales.

Algunas de las recomendaciones consisten en informar expresamente en el aviso de privacidad, sobre qué datos biométricos se recabarán; describir para qué serán utilizados; recolectar y tratar el mínimo de datos, para los fines deseados. También se recomienda garantizar que los datos sean exactos, completos y pertinentes y borrarlos a la brevedad, una vez cumplido su objetivo; atender el riesgo en la implementación de nuevas tecnologías. Se recomienda también implementar medidas de seguridad para evitar el mal uso de los datos; no difundirlos sin consentimiento expreso de su titular y definir claramente al personal que los usará.

De la misma forma, se sugiere evitar vínculos innecesarios entre los datos biométricos y otros sistemas que puedan dar lugar a transferencias no autorizadas y organizarlos de forma que se puedan atender las solicitudes de derechos de acceso, rectificación, cancelación y oposición o también conocidos como derechos ARCO.

[4] INAI, Guía para el Tratamiento de Datos Biométricos, recuperado de: http://inicio.inai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf, consultado el: 12 de junio de 2018.

Todo esto se realizó con el objeto de que el tratamiento de realice de conformidad con los principios, deberes y obligaciones establecidas en la Ley Federal de Protección de Datos Personales en Posesión de los Particulares[5] (LFPDPPP) y en la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[6] (LGPDPPSO), así como en la normativa internacional aplicable a la materia.

No obstante que en 2016 la Cámara de Diputados en México, aprobó tipificar el delito de *Usurpación de Identidad* y establecer sus sanciones de hasta nueve años de prisión y 600 días multa mediante la adición al artículo 430 del Código Penal Federal el rubro de "Delitos Contra la Identidad de las Personas", con un capitulo único llamado "*Usurpación de Identidad "* que establece que: *"se considerará delito de usurpación de identidad al que por sí o por interpósita persona, use cualquier medio licito o ilícito, se apodere, se apropie, transfiera, utilice o disponga de datos personales sin autorización de su titular o bien suplante la identidad de una persona, con la finalidad de cometer un ilícito o favorecer su comisión."*[7], dicha propuesta aún no ha sido aprobada en el Senado de la República y por lo tanto no ha entrado en vigor, sin embargo, éste delito si está tipificado en algunas entidades federativas en México, por lo que por el momento no es un delito federal sino sólo local.

La usurpación de identidad es una práctica que se ha ido expandiendo de manera exponencial en México y a nivel internacional, por lo cual es imperativo su adecuada regulación jurídica.

g) Reconocimiento Facial

El rostro, al igual que las huellas dactilares ha sido ampliamente utilizado como fuente de datos biométricos durante años. Más recientemente, no solo la identidad puede determinarse a partir de un rostro sino también características fisiológicas y psicológicas tales como el origen étnico, emociones y bienestar. La capacidad para extraer este volumen de datos de una imagen y el hecho de que una fotografía puede tomarse a distancia sin conocimiento del interesado demuestra la cantidad de problemas de protección de datos que pueden derivarse de estas tecnologías.

En este sentido el reconocimiento facial ha sido vulnerado a causa de los *deepfakes* y *face swapping* debido a la increíble capacidad de los algoritmos de Inteligencia Artificial para burlar sistemas de seguridad basados en la detección y reconocimiento del rostro para crear identidades falsas increíblemente realistas.

Estos sistemas de reconocimiento facial han sido implementados en los últimos años aunque cada vez con más frecuencia. En el plano social se ha mostrado que en grandes ciudades se ha implementado la utilización de sistemas de seguridad basados en el reconocimiento facial, lo cual facilita a determinados usuarios acceder a un sitio u obtener algún servicio a través

[5] Ley Federal de Protección de Datos Personales en Posesión de los Particulares, consultable en: http://inicio.ifai.org.mx/LFPDPPP/LFPDPPP.pdf
[6] Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, consultable en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017
[7] Minuta Proyecto de Decreto, consultado el: 12 de junio de 2018, recuperado de: http://www.senado.gob.mx/sgsp/gaceta/63/2/2016-12-06-1/assets/documentos/Minuta_art_430_CPF.pdf

de este sistema, e incluso se trabaja en materia de prevención del delito con este tipo de sistemas biométricos, principalmente implementados en aeropuertos con el fin de erradicar labores terroristas.

La tecnología de reconocimiento fácil la podemos encontrar también en nuestros teléfonos inteligentes, con el fin de evitar tener que recodar contraseñas en texto plano, claves de seguridad e incluso tarjetas de identificación, nos podemos valer del rostro. De igual forma una gran variedad de *smartphones*, han optado por integrar funciones de reconocimiento facial para brindar mayor seguridad a los usuarios en el ámbito bancario.

Uno de los dispositivos que más ha destacado en el uso de tecnologías de reconocimiento facial, es sin duda el último *Smartphone* de *Apple* el cual de acuerdo con datos oficiales de su sitio web: *"La probabilidad de que una persona aleatoria pueda acceder al contenido de tu teléfono y desbloquearlo es de aproximadamente 1 en 1 000 000. Esto debido a que el sistema de seguridad que se integra en el dispositivo funciona capturando datos faciales precisos proyectando y analizando más de 30 000 puntos invisibles a fin de crear un esquema de profundidad de un rostro; además, captura una imagen infrarroja de esta."*[8]

Sin embargo, aunque siendo una tecnología nueva y avanzada carece de completa fiabilidad, debido a que en los últimos meses se han realizado numerosas pruebas para poner a prueba este sistema de reconocimiento facial en donde determinados factores hacen que la fiabilidad de estos sistemas disminuya y que fácilmente es aprovechado por aquellas personas que se dedican a la vulneración de datos personales, todo esto con fines lucrativos o en el peor de los caos, para atentar contra la identidad y reputación de una persona.

Los riesgos para la protección de datos asociados al uso de los sistemas de reconocimiento facial pueden describirse de conformidad al Dictamen 3/2012 sobre la evolución de las tecnologías de la biometría de la manera siguiente:[9]

- **Precisión:** si la calidad de las imágenes no puede garantizarse, existe el riesgo de que la exactitud se vea comprometida. Si no se capta una cara (oscurecida por el pelo o por un sombrero) está claro que la correspondencia o categorización no podrá darse sin un alto índice de error. Las variaciones en la pose y la iluminación siguen siendo un enorme reto para el reconocimiento facial, que afecta en gran medida a la precisión.
- **Impacto:** el impacto específico en la protección de datos de un determinado sistema de reconocimiento facial dependerá de su finalidad y circunstancias particulares. Un sistema de categorización para el recuento de visitantes a una atracción, sin capacidad de registro, tendrá un impacto diferente en la protección de datos que el de un sistema utilizado para la vigilancia discreta por las autoridades con funciones coercitivas a fin de identificar a posibles alborotadores.

[8] Apple Inc., "Acerca de la tecnología avanzada de Face ID", sitio web oficial de soporte, disponible en: https://support.apple.com/es-mx/HT208108, consultado el: 12 de junio de 2018.
[9] Dictamen 3/2012 sobre la evolución de las tecnologías biométricas., *Reconocimiento Facial y Usos Combinados*., (2012), consultado el: 12 de junio de 2018, recuperado de: https://www.apda.ad/system/files/wp193_es.pdf

- **Consentimiento y transparencia:** un riesgo de protección de datos que no está presente en muchos otros tipos de tratamiento de datos biométricos es el hecho de que las imágenes pueden capturarse y tratarse desde una serie de puntos de vista, condiciones ambientales y sin el conocimiento del interesado.
- **Fin o fines ulteriores del tratamiento:** una vez capturadas, de forma legítima o ilegítima, las imágenes digitales pueden fácilmente compartirse o copiarse para su tratamiento en sistemas diferentes de aquellos para los que estaban destinadas originalmente. Esto resulta evidente en el ámbito de los medios de comunicación social, donde los usuarios cargar sus fotografías personales para compartirlas con su familia, amigos y compañeros. Una vez en la plataforma de medios sociales, las imágenes están disponibles para su reutilización por la propia plataforma para una amplia gama de fines, algunos de los cuales pueden introducirse en la plataforma incluso después de que la imagen haya sido tomada o cargada.
- **Vinculación:** un gran número de servicios en línea permiten a los usuarios cargar una imagen para vincularla con el perfil del usuario. El reconocimiento facial puede utilizarse para vincular los perfiles de diferentes servicios en línea a través de la imagen del perfil, pero también entre el mundo en línea y fuera de línea. No está fuera de lo posible tomar una fotografía de una persona en la calle y determinar su identidad en tiempo real buscando en estas imágenes de perfil público. Servicios de terceros también pueden rastrear fotografías de perfil y otras fotografías públicamente disponibles para crear grandes colecciones de imágenes a fin de asociar una identidad del mundo real con tales imágenes.
- **Seguimiento/elaboración de perfiles:** también podría utilizarse un sistema de identificación si no se conoce la identidad real de una persona. Podría utilizarse un sistema de reconocimiento facial en un centro comercial o espacio público similar para seguir las rutas y costumbres de los consumidores individuales. La finalidad podría ser una gestión eficaz de las colas o la colocación de productos con el fin de mejorar la experiencia del cliente. No obstante, junto con la capacidad para seguir o localizar a un individuo concreto está la capacidad para elaborar perfiles y enviar publicidad u otros servicios específicos.
- **Tratamiento de datos sensibles:** como ya se ha mencionado, el tratamiento de datos biométricos podría utilizarse para determinar datos sensibles, en especial aquellos con señales visuales tales como la raza, grupo étnico e incluso una enfermedad.
- **Revocabilidad:** un individuo puede cambiar fácilmente su apariencia (barba, gafas, sombrero, etc.) y burlar fácilmente los sistemas de reconocimiento facial, especialmente cuando operan en un entorno no controlado. No obstante, las principales características faciales de una persona son estables en el tiempo y los sistemas también pueden mejorar el reconocimiento recogiendo y asociando diferentes caras conocidas de una persona.
- **Protección anti-suplantación:** muchos sistemas de reconocimiento facial son fáciles de suplantar, pero los fabricantes intentan mejorar esta deficiencia con técnicas tales como la imagen en 3D o la grabación en vídeo. Sin embargo, la mayoría de los sistemas básicos utilizados en aplicaciones rudimentarias no incluyen este tipo de protección. Lo cual no garantiza seguridad.

h) Riesgos, Amenazas e Incidentes: *"Deepfakes" y "Face Swapping"*

Es evidente que el uso incorrecto de estas tecnológicas se ha convertido en un fenómeno cada vez más constante, debido a la facilidad de acceso a estas herramientas, ya no es necesario

adquirir un súper equipo de cómputo para realizar este tipo de ilícitos, basta tener, como se mencionó anteriormente, un simple teléfono inteligente al que le sea posible instalársele un *software* de inteligencia artificial que permita utilizar este tipo de *deepfakes*, pues incluso podemos encontrar a disposición y con libertad software para realizar *deepfakes* con los requerimientos mínimos de una computadora "casera".

Uno de los incidentes más recientes fue el video del expresidente estadounidense Barack Obama, el cual fue creado por *Jordan Peele* quien comentó que su intención al crear el video era advertir sobre los peligros de la desinformación digital y la propagación de las *fake news***.**

De acuerdo con un artículo de BuzzFeed News[10] el video fue realizado utilizando Adobe After Effects, una pieza de software de video disponible y FakeApp**,** una aplicación gratuita disponible en la red. Primero se acopló la boca de Peele sobre la de Obama, luego se reemplazó la mandíbula del ex presidente con una que se movía con los mismos movimientos que la boca del director, luego se usó *FakeApp* para suavizar y refinar el video. Y finalmente, el clip se procesó durante 56 horas. Aunque el tiempo estimado para generar el video fue amplio, el resultado fue impresionante, logrando captar la atención del público y de algunos medios de comunicación, los cuales no lograban discernir los rastros de manipulación en el video.

Así como este incidente, que por su objeto no se aplicó a un fin malicioso como en el caso de los *deepfakes*, lo alarmante es que hablamos de una forma de suplantación de identidad, debido a que con esta tecnología los datos biométricos pueden ser utilizados para hacerse pasar por otra persona, además la capacidad de estas herramientas les da el potencial de ser usadas para chantajes, extorsiones y otros delitos.

El uso de *FakeApp* no terminó aquí, varios sitios de contenido pornográfico para adultos se pronunciaron a principios del año, pues varios videos detectados emulaban el rostro de actrices famosas, a lo que emitieron comunicados para sus usuarios de utilizar filtros de basados en *IA* para dar de baja estos videos apócrifos, pues desprestigiaban la identidad real de la celebridad en situaciones explicitas.

[10] BuzzFeedNews, "This PSA about Fake News from Barack Obama Is Not What It Appears", disponible en: https://www.buzzfeed.com/davidmack/obama-fake-news-jordan-peele-psa-video-buzzfeed?utm_term=.ejBa79PYv#.ua0XrqWJN, consultado el: 12 de junio de 2018. Video: https://www.youtube.com/watch?time_continue=24&v=cQ54GDm1eL0

La facilidad de acceso a estas tecnologías y producción de estos videos incitan a cualquier usuario a modificar videos, ignorando las consecuencias legales que representaría incurrir en un delito de suplantación de identidad. No obstante es necesario hacer una revisión exhaustiva en la legislación actual con respecto a la regulación de datos biométricos, las implicaciones que derivan del uso de tecnologías de inteligencia artificial y las sanciones, acorde a la gravedad del delito. Y sobre todas las cosas hacer énfasis en el usuario y el correcto uso que le da a las herramientas digitales que circulan en la web, así como el no creer en todo el contenido disponible en internet, pues se podría ver inmerso en el mundo de las *fake news.*

i) Medidas de Prevención y Solución

Aunque no en todos los países del mundo se han pronunciado respecto a los incidentes que ha habido estos últimos meses relativo a estos fenómenos de *deepfakes*, la postura que debe tomar cada uno es clara; la protección de la identidad personal e intimidad de un individuo son derechos fundamentales y por ninguna situación deben ser vulnerados, al contrario, cada Estado debe fortalecer y en su caso, implementar una normativa que regule los hechos ilícitos originados a través del uso indebido de tecnologías de inteligencia Artificial. Además de garantizar que aquellos que resulten responsables de alguno de estos delitos haciendo para beneficio propio o con el fin de desprestigiar para originar un daño a otra persona, sean debidamente sancionados.

Por su parte las empresas u organizaciones que recopilan datos personales, es necesario actualizar sus sistemas en materia de ciberseguridad, debido a la increíble capacidad que tiene la inteligencia artificial siendo suficiente para generar engaños y vulnerar la identidad personal, provocando un perjuicio o afectación directa no sólo a la empresa sino también a los usuarios, causando enormes pérdidas monetarias a causa de la suplantación de identidad como se ha hecho habitual en los últimos meses. A fin de mantener la fiabilidad de un sistema biométrico y prevenir la usurpación de identidad, deben aplicarse sistemas dirigidos a determinar si los datos biométricos son auténticos y siguen estando relacionados con una persona física. Por lo que respecta al reconocimiento facial, puede resultar vital garantizar que la cara es real y no, por ejemplo, una foto unida a la cabeza del impostor.

De esta manera se busca garantizar que el número de incidentes cese y disminuya en los próximos meses, tomando medidas de prevención por parte del CEO de aquellas plataformas digitales en donde la comunicación es masiva como *Facebook, Twitter, Instagram,* etc. Para evitar la propagación de las *fake news.* Así como un apego total a la normativa internacional en las políticas de privacidad de aquellas aplicaciones o programas de uso rudimentario desarrollados para *smartphones* y computadoras. De igual forma disponer de medidas de solución, para garantizar que las consecuencias derivadas del hecho ilícito estén al alcance de la ley y ésta pueda sancionar a los responsables.

Por su parte el uso inteligente de estas herramientas será fundamental para evitar futuros problemas e incidentes relativos a la Inteligencia Artificial, teniendo en cuenta que es una tecnología que continua en desarrollo y que en un futuro se vislumbra un escenario en el que se verá involucrada en un mayor ámbito social. Es por ello que cada país debe tomar como precedente este fenómeno de d*eepfakes* y desarrollar medidas de prevención y solución para evitar futuros incidentes.

De acuerdo a un artículo de la BBC[11] la clave para identificar un *Deepfakes* de acuerdo a Yuezun Li, Ming-Ching Chang y Siwei Lyu en una investigación publicada por la Universidad de Cornell, en Nueva York, EUA, está en los movimientos oculares en cuanto al número de parpadeo de los ojos (normalmente 17 veces por minutos) ya que los algoritmos de los videos falsos aún no han podido corregir éste detalle; otros factores a considerar para identificar un video falso son: la fuente que lo publica, los lugares y fechas de la grabación, los movimientos de la boca, el tipo de mensaje que conlleva dicho video y que normalmente busca generar reacciones muy específicas y finalmente, y de ser el caso, ver el video en cámara lenta para observar más de cerca las transiciones.

Son inciertos los problemas que puedan allegarse en un futuro relativos a la tecnología, sin embargo, debemos conocer y mantenernos actualizados en estos temas de vital importancia, ya que a través de los años estas tecnologías se han hecho más presentes en la vida cotidiana y al alcance de cualquier persona. Por lo que de manera en que éstas evolucionan el Derecho debe ser también cambiante y adoptar nuevas medidas para hacer frente a los problemas futuros, auxiliándose también de tecnologías como la inteligencia artificial, la cual como se mencionó anteriormente, se creó con el fin de facilitar las tarea del ser humano y no para dañarlo o generar perjuicios en su persona, particularmente en la identidad personal de cada individuo que es el principal derecho fundamental vulnerado por los *deepfakes*..

j) A manera de corolario

Finalmente es importante comprender la importancia y complejidad de los datos biométricos como parte de la personalidad y analizar el alcance que las nuevas tecnologías tienen en la

[11] https://www.bbc.com/mundo/noticias-44482470 consultado el 13 de julio de 2018.

actualidad para poder identificar y verificar la identidad de una persona. Además de la importancia que conlleva el hacer un uso correcto de las nuevas tecnologías para su aplicación en el derecho, como una herramienta que permita la administración de justicia de manera más concreta frente a los responsables de hechos ilícitos relativos al uso negligente de las tecnologías de inteligencia artificial.

k) Fuentes de Información consultadas

- VOLOCHINSKY, Bracey Wilson, 226 preguntas en derecho civil. Contratos y responsabilidad extracontractual, Santiago, Editorial Jurídica La Ley, 2002, p. 177.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, Reglamento General de Protección de Datos (GDPR), consultado el: 12 de junio de 2018, recuperado de: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679
- UNODC, "Manual Sobre los Delitos Relacionados con la Identidad", consultado el: 12 de junio de 2018, disponible en: https://www.unodc.org/documents/organized-crime/13-83700_Ebook.pdf
- INAI, "Guía para el Tratamiento de Datos Biométricos", consultado el: 12 de junio de 2018, recuperado de: http://inicio.inai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf,
- Apple Inc., "Acerca de la tecnología avanzada de Face ID", sitio web oficial de soporte, consultado el: 12 de junio de 2018, disponible en: https://support.apple.com/es-mx/HT208108, consultado el: 12 de junio de 2018.
- Dictamen 3/2012 sobre la evolución de las tecnologías biométricas., *Reconocimiento Facial y Usos Combinados*., (2012), consultado el: 12 de junio de 2018, recuperado de: https://www.apda.ad/system/files/wp193_es.pdf
- https://www.xlsemanal.com/conocer/tecnologia/20180713/noticias-falsas-creadas-con-videos-falsos-inteligencia-artificial.html#ns_campaign=rrss&ns_mchannel=xlsemanal&ns_source=tw&ns_fee=0&ns_linkname=sem28-conocer-mentira
- Minuta Proyecto de Decreto, consultado el: 12 de junio de 2018, recuperado de: http://www.senado.gob.mx/sgsp/gaceta/63/2/2016-12-06-1/assets/documentos/Minuta_art_430_CPF.pdf
- BuzzFeedNews, "This PSA About Fake News From Barack Obama Is Not What It Appears", consultado el: 12 de junio de 2018, consultado el: 12 de junio de 2018, disponible en: https://www.buzzfeed.com/davidmack/obama-fake-news-jordan-peele-psa-video-buzzfeed?utm_term=.ejBa79PYv#.ua0XrqWJN,
- https://www.bbc.com/mundo/noticias-44482470
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares, consultable en: http://inicio.ifai.org.mx/LFPDPPP/LFPDPPP.pdf
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, consultable en: http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017

LOS MEDIOS DIGITALES Y LA DEFENSA DE LOS DERECHOS DE LA PERSONALIDAD: HONOR, INTIMIDAD Y PROPIA IMAGEN

Por: ***Ana Isabel Meráz E.***
México

INTRODUCCIÓN

Este análisis sobre los derechos de la personalidad es un breve recuento de la regulación que existe en las legislaciones de algunos países. Es un estudio comparativo de las normas reguladoras de esta materia y que son aplicadas en ciertas regiones, como México, principalmente, y con referencias merecidas y fundadas de otras entidades como España y Estados Unidos. Estos países se caracterizan por tener una normatividad avanzada, actualizada y adecuada a los tiempos actuales y cuya promulgación legislativa tiene varios años de antelación con relación a las leyes de otros países. Este enfoque está centrado en mostrar las diferencias y/o semejanzas en la regulación de estos derechos en los países antes mencionados.

Los derechos o prerrogativas de la personalidad competen a todo ciudadano y su salvaguarda es una responsabilidad inexcusable de cada persona. Sin embargo, al tomar en cuenta la inmediatez que tienen los medios electrónicos y sus acciones multiplicadoras en tiempo real para la colocación y distribución de la información, se complica preservarla y darle un efectivo tratamiento y cuidado de la misma. La colocación de datos, documentos, e imágenes en cualquier medio digital lleva un riesgo implícito que atenta contra la privacidad de su dueño o tenedor.

La privacidad, el honor, la intimidad y la propia imagen, como derechos humanos regulados en los preceptos constitucionales de varios países y de diferentes continentes, merecen un tratamiento especial al estar contextualizados normativamente en los medios digitales, siendo una temática actual que solamente puede concebirse con el uso del ciberespacio. Cada uno de estos derechos presenta características particulares y se tratan legalmente por separado, aunque tengan todos ellos el hilo conductor de ser prerrogativas de la personalidad. Es tal el impacto que tienen en esta era tecnológica que no son tratados como consecuencia de actividades meramente laborales, sino que sus efectos se derivan en gran medida de la actividad cotidiana de los ciudadanos. Esa, a veces, "inocente" ocupación que se tiene en los medios digitales, cuyas consecuencias jurídicas son inevitables, urgen a la regulación jurídica pero también previamente a una reflexión de los usuarios de Internet, sobre la exposición de sus datos e información personal que con el simple y fácil acceso digital pueden exponer situaciones personales e íntimas.

Es así, como en cualquier dispositivo electrónico transita libremente todo tipo de información qué si bien puede o no tener la categoría de sensible, como la estrictamente personal, su circulación extremadamente suelta en el ciberespacio requiere de un tratamiento especial. Ante la colocación de todo tipo de datos e imágenes que transitan libremente por el ciberespacio, surge la necesidad de preservar, regular y cuidar su distribución o publicación,

que con o sin la autorización de sus dueños puede ser utilizada para fines opuestos a los que sus titulares tuvieron al momento de entregarlas o compartirlas. Así, considerando esas diferentes razones de uso del ciberespacio surge la necesidad de tomar en cuenta la regulación existente y tener al menos un respaldo legal que permita a los usuarios del ciberespacio, de Internet o como se denomine a todo tipo de medio digital tener un medio de defensa que garantice sus derechos de la personalidad, en este caso.

LOS DERECHOS DE LA PERSONALIDAD

El precedente por antonomasia de los derechos de la personalidad se encuentra en el artículo 12 de la Declaración Universal de los Derechos Humanos de 1948 que textualmente prescribe lo siguiente: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."[1] Esta disposición es la referencia obligada en la protección de este tipo de derechos en las legislaciones nacionales de los países que los regulan.

Existen otras disposiciones de carácter internacional que también expresan la regulación de estos derechos y que son materia de consulta obligada para conocer sus alcances legales. Sin pretender abarcar la mayoría de estos ordenamientos, se puede citar a continuación un par de ellos. Por una parte, está el Pacto Internacional de Derechos Civiles y Políticos (1966), en cuyo artículo 17, señala algo parecido al artículo 12 de la Declaración Universal de los Derechos Humanos y en su artículo 19 menciona, sobre la libertad de expresión, "que el ejercicio de ese derecho entraña deberes y responsabilidades especiales por lo que podrá estar sujeto a ciertas restricciones fijadas por la ley y que sean necesarias para asegurar el respeto a los derechos o a la reputación de los demás…"[2]

Por otra parte, la Convención Americana sobre Derechos Humanos (1969), menciona en su artículo 11 que "toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad y que por tanto no deberá ser objeto de injerencias arbitrarias o abusivas en su vida privada, familia, domicilio, correspondencia, ni deberá sufrir ataques ilegales a su honra o reputación; también, establece el derecho de la persona a ser protegida por la ley contra esas injerencias o ataques."[3]

Los derechos al Honor, a la Intimidad y a la Propia Imagen pueden parecer sinónimos y a simple vista quizá sean difíciles de separar, pero cada uno tiene características propias que les permiten tener una regulación jurídica definida. La Constitución española es un buen ejemplo en la regulación de estos derechos al tener una legislación completa y efectiva en esta materia al contener una serie de disposiciones sobre los derechos fundamentales y las libertades públicas. Es conveniente mencionar su artículo 18 por contener este precepto una regulación detallada y concisa sobre las garantías de estos derechos al prescribir lo siguiente:

[1] DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS DE 1948. http://www.un.org/es/documents/udhr/
[2] DE DIENHEIM, C. El derecho a la intimidad, al honor y a la propia imagen. http://www.unla.mx/iusunla3/reflexion/derecho%20a%20la%20intimidad.htm
[3] DE DIENHEIM, C. El derecho a la intimidad, al honor y a la propia imagen. Op. Cit.

> "1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. 2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito. 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."[4]

Se parte de la Constitución Española en la definición de tales derechos por ser un ente jurídico previo a su regulación, en el caso de México. De hecho, no ha sido fácil tanto en los países pioneros como en los que han tenido una legislación tardía, el regular estos aspectos relativos a la vida privada, al honor, a la intimidad y a la propia imagen. Si se toma en cuenta que el uso de la tecnología tiene ya varias décadas, las normas no se crean a la par de ella. Esta particularidad de regular actividades de todo tipo y que se realizan a través de medios digitales es un problema derivado de un uso inapropiado de los mismos, tanto por parte de quien ejecuta las acciones, el titular de la información, como de quiénes disponen de ella, como los prestadores de servicios de Internet, de los encargados de preservar datos, de los técnicos que dan mantenimiento y deben garantizar la seguridad técnica.

En la Ciudad de México, se tiene vigente la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen en el Distrito Federal, actual CDMX, publicada en la Gaceta Oficial del Distrito Federal mediante decreto del 19 de mayo de 2006. Esta ley contiene una serie de artículos que regulan estos derechos de la personalidad y su finalidad es "regular el daño al patrimonio moral derivado del abuso del derecho de la información y de la libertad de expresión".[5] El artículo 3 señala que tiene por objeto "garantizar los siguientes Derechos de la Personalidad: el derecho a la vida privada, al honor y la propia imagen de las personas en el Distrito Federal".[6] Las normas de este ordenamiento definen conceptos particulares sobre los derechos de la personalidad como los siguientes:

Vida Privada: "Es vida privada aquella que no está dedicada a una actividad pública y, que por ende, es intrascendente y sin impacto en la sociedad de manera directa; y en donde, en principio, los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia ni les afecta."[7]

Derecho a la Intimidad: "Como parte de la vida privada se tendrá derecho a la intimidad que comprende conductas y situaciones que, por su contexto y que por desarrollarse en un ámbito estrictamente privado, no están destinados al conocimiento de terceros o a su divulgación, cuando no son de interés público o no se han difundido por el titular del derecho."[8]

---

[4] ÁLVAREZ, M. Derecho al olvido en Internet: El nuevo paradigma de la privacidad en la era digital. Ed. Reus. Madrid, 2015. P. 43.

[5] DECRETO DE LEY DE RESPONSABILIDAD CIVIL PARA LA PROTECCIÓN DEL DERECHO A LA VIDA PRIVADA, EL HONOR Y LA PROPIA IMAGEN EN EL DISTRITO FEDERAL. www.aldf.gob.mx/archivo-f1622931dc0f6677e86f68ef7b9b2270.pdf

[6] DECRETO DE LEY DE RESPONSABILIDAD CIVIL PARA LA PROTECCIÓN DEL DERECHO A LA VIDA PRIVADA, EL HONOR Y LA PROPIA IMAGEN EN EL DISTRITO FEDERAL. *Op. Cit.*

[7] Artículo 9. *Op. Cit.*

[8] Artículo 11. *Ibidem.*

Derecho al Honor: "El honor es la valoración que las personas hacen de la personalidad ético-social de un sujeto y comprende las representaciones que la persona tiene de sí misma, que se identifica con la buena reputación y la fama. El honor es el bien jurídico constituido por las proyecciones psíquicas del sentimiento de estimación que la persona tiene de sí misma, atendiendo a lo que la colectividad en que actúa considera como sentimiento estimable."[9]

Propia Imagen: "La imagen es la reproducción identificable de los rasgos físicos de una persona sobre cualquier soporte material."[10]

La regulación de los derechos de la personalidad no es una tarea sencilla cuando los puntos de vista difieren en la reconsideración de los valores de la privacidad, intimidad, honor y propia imagen. Es evidente cómo a cada concepto se le otorga importancia de acuerdo con las influencias históricas, culturales y sociales de un determinado lugar. La costumbre en la vida de las personas juega un papel relevante en la conformación de los grupos sociales, el hábito o uso reiterado de una práctica aprobada por una comunidad se puede elevar incluso a norma de carácter general y le corresponde un rol muy importante en la formación del carácter de los habitantes de una región, así como en ciertos aspectos característicos de la personalidad de sus miembros. Los grados de privacidad varían de región a región y lo que parece importante para algunos no tiene el menor interés para otros.

EL HONOR

El derecho al honor tiene una interpretación diferente en el actual contexto de las telecomunicaciones al que se tenía siglos atrás. Es un derecho clásico de la personalidad que hace referencia a "la estima que cada persona tiene de sí misma… y en el reconocimiento de los demás de nuestra dignidad…se vincula así, pues, con la fama, con la opinión social."[11] El honor parte del principio de la dignidad que todo ser humano tiene como derecho fundamental. Es el derecho a ser respetado. Es un valor en sí cuyas acepciones van de la mano de las circunstancias sociales en las que se presenta o se contextualiza y forma parte, en consecuencia, de un momento histórico determinado.[12]

La regulación jurídica del honor no tenía hasta hace poco tiempo una regulación definida, no obstante, su Constitución Política lo contempla en su artículo 6, en relación a la libertad de la manifestación de las ideas que podrían ser sujetas a un proceso judicial o administrativo si atacan a la moral o la vida privada, entre otros aspectos. También, en el artículo 7 de esta Carta Magna se hace referencia a la inviolabilidad de la libertad de "difundir opiniones,

[9] Artículo 13. *Ibídem.*
[10] Artículo 16. *Ibídem.*
[11] CONSTITUCIÓN POLÍTICA DE ESPAÑA. Artículo 18. http://www.congreso.es/consti/constitucion/indice/sinopsis/ Este ordenamiento constitucional ha sido pionero en la regulación de este derecho de la personalidad. Su acertada definición ha sido retomada por leyes de otros países de habla hispana.
[12] FIX FIERRO, M. El derecho al honor como límite a la libertad de expresión. Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México, http://historico.juridicas.unam.mx/publica/librev/rev/derhumex/cont/3/art/art6.pdf

información e ideas, a través de cualquier medio", y cuyos límites no son más que los previstos en el artículo previo antes señalado.[13]

Existen algunos textos normativos nacionales relativos a estos derechos de la personalidad, pero sería una tarea larga el intentar mencionar a cada uno de ellos. Sin embargo, vale destacar que una de las primeras leyes decretadas en esta materia, fue la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen[14], en el entonces Distrito Federal, hoy Ciudad de México, publicada el 19 de mayo de 2006 y de la cual se hará mayor referencia en páginas posteriores de este escrito. Otro caso particular, pero más reciente, es el Código Familiar del estado de Sinaloa, publicado en el Periódico Oficial el día 6 de febrero de 2013, en cuyo artículo 22 define el honor como "la valoración que las personas hacen de la personalidad ético-social de un sujeto y comprende las representaciones que la persona tiene de sí misma, que se identifica con la buena reputación y la fama. Es el bien jurídico constituido por las proyecciones psíquicas del sentimiento de estimación que la persona tiene de sí misma, atendiendo a lo que la colectividad en que actúa considera como sentimiento estimable."[15]

La Constitución Política de los Estados Unidos Mexicanos, en su reforma al artículo 1, de fecha 11 de junio de 2011, se sustituyó el vocablo "individuo" por "personas", en el contexto de preservar sus garantías individuales. El párrafo primero de este precepto señala que:

> "En los Estados Unidos Mexicanos todas las personas gozarán de los derechos humanos reconocidos en esta Constitución y en los tratados internacionales de los que el Estado Mexicano sea parte, así como de las garantías para su protección, cuyo ejercicio no podrá restringirse ni suspenderse, salvo en los casos y bajo las condiciones que esta Constitución establece."[16]

En este sentido, la anteriormente citada Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y la Propia Imagen, de la actual CDMX, contiene en su artículo 28 una excepción en relación a lo que puede considerarse como una persona y la conceptúa como "malicia efectiva", y la indica de la siguiente manera: "La malicia efectiva se configura en los casos en que el demandante sea un servidor público y se sujetará a los términos y condiciones del presente capítulo". Luego, en el artículo 29 aclara que: "Se prohíbe la reparación del daño a los servidores públicos que se encuentren contenidos en los supuestos del presente título, a no ser prueben que el acto ilícito se realizó con malicia efectiva."[17]

Con los anteriores preceptos, la Constitución Política de los Estados Unidos Mexicanos y la Ley de Responsabilidad Civil para la Protección del Derecho a la Vida Privada, el Honor y

---

[13] CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Última reforma publicada en el Diario Oficial de la Federación el 24 de febrero de 2017. http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm

[14] LEY DE RESPONSABILIDAD CIVIL PARA LA PROTECCIÓN DEL DERECHO A LA VIDA PRIVADA, EL HONOR Y LA PROPIA IMAGEN. http://www.aldf.gob.mx/archivo-f1622931dc0f6677e86f68ef7b9b2270.pdf

[15] CÓDIGO FAMILIAR DEL ESTADO DE SINALOA. Artículo 22. Última reforma publicada en el Periódico Oficial el 30 de mayo de 2016.
https://www.juridicas.unam.mx/legislacion/ordenamiento-entidad/1245-codigo-familiar-del-estado-de-sinaloa

[16] CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. *Op. Cit.*

[17] LEY DE RESPONSABILIDAD CIVIL PARA LA PROTECCIÓN DEL DERECHO A LA VIDA PRIVADA, EL HONOR Y LA PROPIA IMAGEN. *Op. Cit.*

la Propia Imagen, de la CDMX, el Poder Judicial de la Federación manifestó en una de sus Tesis resolutorias la siguiente exposición:

> "Esta Primera Sala entiende que en supuestos donde esté en juego el derecho a la vida privada de funcionarios públicos sólo debe exigirse que la información se haya difundido con la única intención de dañar, como lo establece la fracción III del artículo 30 de la ley citada; y en el caso de los particulares con proyección pública y particulares sin esa proyección, la "malicia efectiva" se reduce a la hipótesis de que la información se haya difundido con negligencia inexcusable, supuesto establecido en el artículo 32 del citado ordenamiento."[18]

Confirma la propia Suprema Corte de Justicia de la Nación, qué para efectos de los denominados Derechos de la Personalidad, este concepto de "malicia efectiva" solamente recae el derecho relativo al honor de manera literal a lo que implica una intromisión al mismo, a la vida privada de las personas, al declarar lo siguiente:

> "La "malicia efectiva" es el criterio subjetivo de imputación que se ha adoptado en el derecho mexicano para atribuir responsabilidad en casos de conflicto entre la libertad de expresión y los derechos de la personalidad. No obstante, el principal problema es que la "malicia efectiva" surgió para aplicarse en casos donde se alegaban vulneraciones al derecho al honor. En esta línea, las disposiciones sobre la "malicia efectiva" contempladas en la ley citada sólo se aplican en su literalidad a las intromisiones en el honor, por lo que la irrelevancia de la veracidad de la información en casos donde se alega la intromisión en la vida privada de una persona hace que la "malicia efectiva" como criterio subjetivo de imputación deba sufrir alguna modulación, que se traduce en dejar de considerar en todos los casos de posibles afectados (funcionarios públicos, personas con proyección pública y particulares) los elementos del estándar que presuponen la falta de veracidad."[19]

LA INTIMIDAD

Por otra parte, siguiendo el tema de los derechos de la personalidad, se encuentra el denominado derecho a la intimidad, el cual "se vincula a la esfera más reservada de las personas, al ámbito que éstas siempre preservan de las miradas ajenas, aquél que desea mantenerse oculto a los demás por pertenecer a su esfera más privada vinculada con la dignidad y el libre desarrollo de la personalidad".[20] Este derecho es una garantía fundamental que la propia legislación española reconoce, al igual que en otros países, al ciudadano y su contexto familiar, "…se reconoce incluso a las personas más expuestas al público. La intimidad, de acuerdo con el propio precepto constitucional, se reconoce no sólo al individuo aisladamente considerado, sino también al núcleo familiar".[21]

---

[18] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. Derecho a la Propia Imagen e Identidad. 24 mayo 2018. http://207.249.17.176/Transparencia/Documents/CriteriosPJF/Tesis_Tematica_Derecho_a_la_propia_imagen_e_identidad.pdf

[19] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. Derecho a la Propia Imagen e Identidad. Op. Cit.

[20] CONSTITUCIÓN POLÍTICA DE ESPAÑA. *Op. Cit.*

[21] *Ibídem.*

El derecho a la intimidad, en su terminología inglesa conocida como *The right to privacy* (derecho a la privacidad) y que se utiliza también como "intimidad de la vida privada" tiene su propio impacto cuando se emplea en los medios digitales. En el contexto de la red de redes se le conoce como "derecho a la privacidad en Internet". Esta prerrogativa, es una de las más sensibles dentro de los derechos de la personalidad, pues aquí está en juego la libre elección de abrirse al mundo a través de cualquier tipo de dispositivo electrónico que esté interconectado en el ciberespacio y ante lo cual, si se quiere tener salvaguardado este derecho en toda plenitud, no le queda otra opción al usuario que el sustraerse de estos medios digitales o tener todo tipo de cautela para preservar todo aquello en lo que nadie más pueda intervenir o entrometerse .

La misma Constitución española de 1978 en su artículo 20, sobre libertad de expresión, reconoce y protege los derechos de sus ciudadanos y en su primer inciso indica que estos tienen la prerrogativa de: "a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción; en otro de sus incisos, menciona: "d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades". Pero, en el punto 4, acota limitando específicamente ese derecho con el siguiente precepto: "Estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia."[22] Este límite a la libertad de expresión, no es otra cosa que el respeto a las prerrogativas constitucionales de los derechos de la personalidad que la misma Carta Magna española garantiza en su artículo 18 previamente comentado.

LA PROPIA IMAGEN

Respecto al derecho a la propia imagen, este se "atribuye a su titular la potestad para disponer de su imagen física impidiendo su difusión salvo que medie su propio consentimiento".[23] Este tipo de derecho "salvaguarda la proyección exterior de dicha imagen como medio de evitar injerencias no deseadas, de velar por una determinada imagen externa o de preservar nuestra imagen pública… está íntimamente condicionado por la actividad del sujeto, no sólo en el sentido de que las personas con una actividad pública verán más expuesta su imagen, sino también en el sentido de que la imagen podrá preservarse cuando se desvincule del ámbito laboral propio."[24]

El derecho a la propia imagen es exigible a particulares y a los entes públicos, es una garantía jurídica de su titular para "decidir todo lo relativo a la captación, reproducción o publicación de su imagen". Aunque su naturaleza le permite ser también un "mecanismo de protección al honor y la intimidad" tiene características muy particulares porque estas recaen directamente en lo relativo a la fisonomía reconocible de cada persona, es decir, su exclusiva y propia imagen.[25] Si bien, la fisonomía es el "aspecto particular del rostro de una

[22] *Ibídem*. Artículo 20.
[23] CARRILLO, M. *El derecho a la propia imagen*. elpais.com/diario/2003/03/15/Catalunya/1047694043_850215.html
[24] CONSTITUCIÓN POLÍTICA DE ESPAÑA. *Op. Cit.*
[25] TESIS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. México, 2009.

persona"[26] cuyas características son únicas, esto comprende también su cuerpo o algunas partes de él. Existen personajes históricos y personas en general que por su actividad son públicamente reconocidos pero cuya cara y cuerpo poseen características muy específicas que pueden servir de modelo, imitación o reproducción ilegal con fines comerciales o de diversa índole.

El derecho a la propia imagen tiene ciertas particularidades qué con el avance de la tecnología, sobre todo de los dispositivos electrónicos conectados a Internet, ha facilitado el acceso libre a todo tipo de fotografías, tanto de personas que tienen una vida profesional pública, como la de otros ciudadanos que viven al margen de este tipo de actividades. El uso de imágenes, fotografías o videos sin el consentimiento de quien aparezca en ellos, provoca en el titular o dueño todo tipo de emociones que van desde el enojo y la molestia hasta la provocación de flagrantes violaciones de sus derechos de honra y dignidad.[27]

EL USO DE LOS MEDIOS DIGITALES

En general, los derechos de la personalidad (Honor, Intimidad y Propia Imagen) son diferentes entre sí, como ya se explicó, sin embargo, esto no significa que no sean vulnerados de manera separada o bien de manera conjunta al tener rasgos comunes de proximidad. La dignidad de una persona, su privacidad y la exposición de su imagen física pueden verse afectados en un mismo tiempo por alguna intromisión externa por parte de otras personas y en donde no exista evidentemente el consentimiento del ofendido. Con el creciente uso de la tecnología y sus variados instrumentos electrónicos, la fragilidad de estos derechos es cada vez más delicada. Aunque el lugar privado por antonomasia sea el hogar de las personas, los medios digitales han propiciado que la intimidad sea vulnerada ante la escasa seguridad informática y jurídica que existe.

Con las facilidades de libre acceso que buena parte de los ciudadanos tienen a los medios electrónicos, como Internet, es muy sencillo vulnerar los espacios particulares y privados de las personas y atentar contra sus derechos de la personalidad como los antes mencionados. El honor, el buen nombre y la reputación de una persona penden de un hilo ante la cada vez más sencilla forma de acceder a sus datos personales en donde se encuentra información sobre su vida privada y conocer todo aquello relacionado con su persona, familia, domicilio, trabajo, entre otros aspectos estrictamente personales. La incipiente privacidad que existe en la actualidad ha evolucionado desde siglos pasados cuando los medios de comunicación eran principalmente papeles y que posteriormente con el uso del teléfono y de antiguas computadoras, dieron paso a las modernas tecnologías de la información y de las comunicaciones. La constante innovación de los medios electrónicos y las frecuentes actualizaciones de todo tipo de aplicaciones han traído a esta era digital una serie de supuestos legales que no tienen una regulación preventiva u oportuna ante lo vertiginoso de los cambios.

---

http://207.249.17.176/Transparencia/Documents/CriteriosPJF/Tesis_Tematica_Derecho_a_la_propia_imagen_e_identidad.pdf

[26] REAL ACADEMIA ESPAÑOLA. http://dle.rae.es/srv/search?m=30&w=fisonom%C3%ADa

[27] TESIS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. México, 2009. *Op. Cit.*

Sobre el derecho a la intimidad de las personas, en relación a sus derechos de privacidad personal y familiar, la legislación nacional en casos particulares sigue siendo parca. Sin embargo, el problema no es, algunas veces, por la ausencia de normas reguladoras sino por el desinterés de los ciudadanos que no alcanzan a medir las dimensiones de sus actos dentro del ciberespacio. Es preocupante como en países con atraso en materia de telecomunicaciones, por decir, la falta de Internet en buena parte del territorio nacional, ya sea por los altos cobros de su servicio o por la mala calidad de la señal, no se tengan cuidados extremos como se tienen en otros asuntos que vulneran la tranquilidad social. Esta sea tal vez una razón, pero lo cierto es que con la poca o mínima accesibilidad que se tiene a los medios digitales, el problema no está centrado en su uso per se, sino en el malo o incorrecto uso. Esto último es lo que incide legalmente contra terceros, pero lo preocupante del tema es que no sean los otros, sino el propio dueño de la información personal quien la divulgue o no tenga la precaución para resguardarla y cuidarla.

Los Estados Unidos son uno de los países con un mayor avance en el tema de los medios electrónicos y las telecomunicaciones y consecuentemente con menos problemas a los ya mencionados. Por ello, es pertinente comentar sobre la encuesta que realizó el Opera Software en el año de 2011 en donde los norteamericanos respondieron de manera contundente y tal vez más radicalizada que cualquier otra, en relación con preguntas sobre la seguridad y privacidad de sus datos e información en la web, que para ellos no eran "…más angustiantes las violaciones a su privacidad en la red, como los ataques terroristas, la bancarrota personal o la invasión a sus hogares".[28] Estas respuestas no son ajenas a las opiniones que los ciudadanos tendrían en otras partes del mundo, ya que si en cada país se realizaran encuestas como esta seguramente habría otro tipo de resultados, quizá muy diferentes a los expresados por los norteamericanos pero con toda certeza coincidirían asombrosamente en la parte relativa a que no es tan importante la violación de la privacidad ciberespacial de las personas como podría ser cualquier otro problema o intromisión que esté presente en el entorno social en donde habite y provoque al ciudadano una preocupación o incomodidad más allá del uso de los medios electrónicos y sus consecuentes problemas relacionados con los derechos de la personalidad.

En cuanto al derecho a la propia imagen, como se hizo referencia con antelación, también forma parte de los derechos de la personalidad pero con una característica muy particular al ser una garantía constitucional en algunos países, no con exacta regulación en el caso mexicano pero circunscrita exclusivamente en el aspecto físico de las personas, como el cuerpo y la cara, representando esta última la proyección directa de la esencia personal por ser la parte asociada directamente a la imagen de un sujeto. La fisonomía es la zona externa la que se muestra públicamente y conocen los demás y puede ser utilizada indebidamente al estar expuesta en actividades propias de los individuos, así, es el rostro el representante de la imagen personal y única del ser humano y está íntimamente relacionado con las actividades públicas que realiza y que incluso al cambiarlas o no hacerlas se pueden seguir preservando y en consecuencia utilizando para causar algún daño a su propia imagen. En todo caso, como se expresó en líneas anteriores, la propia tesis de la Suprema Corte de Justicia de la Nación, lo considera como un derecho de la personalidad que constituye en sí un escudo o protección de los otros dos derechos correlativos que son el honor y la intimidad.

[28] CRAIG, T. y LUDLOFF, M. Privacy and Big Data. Sebastopol, CA: O´Reilly, 2011, p. 2.

La publicación que se haga de la imagen de una persona sin su autorización es violatoria de un derecho humano, la protección jurídica que tiene la convierte en una garantía constitucional y su autonomía permite a su titular la exclusividad de exponerla y publicarla cuantas veces quiera y en los medios que prefiera, incluso, puede venderla o autorizar a otros para que la utilicen o exploten siempre y cuando exista el consentimiento de por medio. Para el caso de México, aunque no esté expresamente señalado en la Constitución este derecho fundamental, hay ciertas acepciones equiparadas en el artículo 16 constitucional, sobre todo con la parte relativa a la protección de datos personales y la vida privada de las personas, en donde en esta última podría considerarse en parte el honor, la intimidad y la propia imagen. Esta garantía individual inherente a todo ciudadano mexicano, menciona que "Las comunicaciones privadas son inviolables. La ley sancionará penalmente cualquier acto que atente contra la libertad y privacía de las mismas, excepto cuando sean aportadas de forma voluntaria por alguno de los particulares que participen en ellas…" Este atisbo de protección constitucional a los derechos de la personalidad se refleja en la continuidad de este mismo precepto al indicar que "El juez valorará el alcance de éstas, siempre y cuando contengan información relacionada con la comisión de un delito. En ningún caso se admitirán comunicaciones que violen el deber de confidencialidad que establezca la ley."[29]

Cuando los modos o caracteres de la personalidad de ciertos pueblos traspasan las fronteras ciberespaciales es cuando comienza la reacción ente el rechazo o la aceptación a lo que los otros muestran y manifiestan. Así, algunos de los rasgos que provocan esa disparidad o extrañeza pueden ser producto de factores típicamente complejos como los que Craig y Ludloff señalan en relación con los límites de la privacidad en estos tiempos de electrónica y tecnología, estos autores afirman que "… la edad, la etnicidad, y el sexo pueden influir en nuestra expectativa de privacidad. Aquellos que viven bajo regímenes represivos, como China, Rusia o Siria, no tienen expectativas de privacidad. Los adolescentes también no tienen expectativas de privacidad. Pero no son fuerzas externas a las que ellos tienen miedo de intrusión, sino a las frecuentes intromisiones de sus padres."[30]
Tomando en cuenta los aspectos particulares del derecho a la privacidad que se tienen en cada lugar, ciudad o país, por la propia dinámica social y cultural que predomina, sus diferencias en relación con otros lugares, contrasta cuando sin mediar presencia física alguna los medios electrónicos comienzan a hurgar y extender los usos y costumbres de los demás ante el libre acceso y traspaso de jurisdicciones de los cibernautas entre regiones. Aquí se vuelve a plantear la duda respecto hasta dónde se puede llegar a intimar, a transgredir la privacidad y la intimidad de los demás, atentar contra el honor, la dignidad y la imagen de los ciudadanos por medio del uso de la tecnología en actividades llevadas a cabo en territorios nacionales, pero con alto impacto transnacional. Es importante señalar que "El derecho a la privacidad, en cuanto especie del género de los derechos de la personalidad, es un tema tratado con un cierto romanticismo tanto en el ámbito de Internet y de la sociedad tecnocomunicacional como fuera de ella. Este derecho debe ser preservado, aunque no

[29] CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Última reforma publicada en el Diario Oficial de la Federación el 24 de febrero de 2017. http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm
[30] CRAIG, T. y LUDLOFF, M. Privacy and Big Data. *Op Cit.* p. 22.

sacralizado. Debe ser preservado por tratarse de una figura cuyos elementos esenciales son expresión de la personalidad de los individuos".[31]

El problema de la jurisdicción o territorialidad de las normas reguladoras del ciberespacio es un tema complejo que para el caso de la privacidad solamente a nivel nacional en algunos países se tiene regulado, sin embargo, el gran conflicto se presenta en los casos o situaciones que van más allá de las fronteras físicas. Estados Unidos y la Unión Europea son dos regiones que en esta materia tienen regulaciones claras y definidas aunque en cierta forma sus normas y políticas entre sí sean divergentes y cada una tenga conceptos propios en cuanto a lo que la privacidad significa y la forma en que pueda ser reforzada.[32]

El derecho y el respeto a la privacidad, en todas sus variables o especies, como el honor, la intimidad o la propia imagen, son límites externos a los que se exponen todos los ciudadanos en el ámbito de las comunicaciones electrónicas. El acceso a Internet no es una moda o una etapa en la cual se acostumbre interactuar sin graves consecuencias; esto sigue, la red de redes continuará expandiendo su telaraña de la información y la extralimitación en el entorno digital seguirá presente con los accesos digitales cada vez más sutiles y afilados en la flagrante violación a este derecho de libertad de los ciudadanos.

CONCLUSIONES

Los derechos de la personalidad, como la privacidad, la intimidad, el honor y la propia imagen, constituyen en sí un tema interesante, por el respeto que debe imperar en los medios electrónicos hacia los aspectos más reservados, particulares y personales de los seres humanos. Las fronteras invisibles que caracterizan al ciberespacio permiten a todo tipo de usuario transgredir la dignidad, imagen y honor de los demás.

Los derechos de la personalidad, Vida Privada, Honor, Intimidad y Propia Imagen, plantean otros supuestos, entre ellos la subjetividad, para poder delimitar lo que se debe estimar como espacio público y espacio privado. Ante la disparidad de criterios sociales y culturales sobre el correcto o aceptable uso del ciberespacio, la legislación marca aspectos jurídicos bastante claros en esta materia, sin embargo, queda la ambigüedad de lo que considera como privado el propio titular del derecho. Existen valores morales y éticos intrínsecamente relacionados a estos derechos jurídicos, como el respeto y la dignidad, para que a cada quien se le reconozca legalmente ese espacio privado con derecho a la intimidad, a la soledad y al anonimato elegidos. Pero, como todo aspecto moral y ético, queda a criterio del ciudadano el exponer o salvaguardar lo que considere, de manera autónoma, como estrictamente privado o personal, y con la única limitante que impone la norma jurídica que al traspasar el límite y transgredir la esfera personal e íntima de otro ciudadano puede ser legalmente sancionada.

Internet es un recurso electrónico, informático y telemático, catalogado como derecho humano y está plenamente reconocido en las esferas legales de la mayoría de los países del mundo. Su uso no se concreta solamente al goce de una garantía ciudadana que respalda su libre acceso, sino que al ser un escaparate para colocar información y exponer ideas con plena

[31] DRUMMOND, V. *Internet, Privacidad y Datos Personales, Op. Cit.* p. 149.
[32] CRAIG, T. y LUDLOFF, M. *Privacy and Big Data, Op Cit*. p. 22.

libertad, este derecho puede exceder los límites y atentar contra los derechos de privacidad protección de datos personales de los usuarios. Así, el análisis de esta temática plantea dos interrogantes clave: Hasta dónde puede existir la libertad en Internet para interactuar, intimar y acceder a la privacidad de los otros sin previo consentimiento y hasta donde llega la responsabilidad de los tenedores de datos personales de los titulares y bajo un contrato laboral a alguna corporación o empresa.

La respuesta para ambos cuestionamientos se reduce a la palabra comunicar. Una comunicación masiva, continua y sistemática, por todo tipo de medios, debe llegar al público en general para informarle y advertirle que en su estatus de empleado en lo particular existen riesgos sobre su información y documentación personal entregada con fines laborales a un patrón. Este punto es jurídicamente vulnerable para el empresario y también para sus colaboradores pues ambos requieren estar informados sobre la los derechos y obligaciones que existen en esta materia y ser cautelosos en el manejo de todo tipo de información contenida en soportes físicos o electrónicos.

REFERENCIAS

ÁLVAREZ, M. Derecho al olvido en Internet: El nuevo paradigma de la privacidad en la era digital. Ed. Reus. Madrid, 2015.

CARRILLO, M. *El derecho a la propia imagen* [en línea]. [Consulta: 20-1-2018]. Disponible en: elpais.com/diario/2003/03/15/Catalunya/1047694043_850215.html

CÓDIGO FAMILIAR DEL ESTADO DE SINALOA. Artículo 22. Última reforma publicada en el Periódico Oficial el 30 de mayo de 2016 [en línea]. [Consulta: 18-2-2018]. Disponible en: https://www.juridicas.unam.mx/legislacion/ordenamiento-entidad/1245-codigo-familiar-del-estado-de-sinaloa

CONSTITUCIÓN ESPAÑOLA DE 1978. Artículo 18 [en línea]. [Consulta: 15-1-2018]. Disponible en: http://www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=18&tipo=2

CONSTITUCIÓN POLÍTICA DE ESPAÑA. ARTÍCULO 18. [en línea]. [Consulta: 10-2-2018]. Disponible en: http://www.congreso.es/consti/constitucion/indice/sinopsis/

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS. Última reforma publicada en el Diario Oficial de la Federación el 24 de febrero de 2017 [en línea]. [Consulta: 18-3-2018]. Disponible en: http://www.diputados.gob.mx/LeyesBiblio/ref/cpeum.htm

CRAIG, T. y LUDLOFF, M. Privacy and Big Data. Sebastopol, CA: O´Reilly, 2011.

DE DIENHEIM, C. El derecho a la intimidad, al honor y a la propia imagen [en línea]. [Consulta: 24-5-2018]. Disponible en:

http://www.unla.mx/iusunla3/reflexion/derecho%20a%20la%20intimidad.htm

DECLARACIÓN UNIVERSAL DE LOS DERECHOS HUMANOS DE 1948 [en línea]. [Consulta: 20-1-2018]. Disponible en: http://www.un.org/es/documents/udhr/

DECRETO DE LEY DE RESPONSABILIDAD CIVIL PARA LA PROTECCIÓN DEL DERECHO A LA VIDA PRIVADA, EL HONOR Y LA PROPIA IMAGEN EN EL DISTRITO FEDETAL [en línea]. [Consulta: 15-1-2018]. Disponible en: www.aldf.gob.mx/archivo-f1622931dc0f6677e86f68ef7b9b2270.pdf

DRUMMOND, V. Internet, Privacidad y Datos Personales. Madrid: Reus, 2004.

FIX FIERRO, M. El derecho al honor como límite a la libertad de expresión. Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México [en línea]. [Consulta: 30-3-2018]. Disponible en: http://historico.juridicas.unam.mx/publica/librev/rev/derhumex/cont/3/art/art6.pdf

REAL ACADEMIA ESPAÑOLA [en línea]. [Consulta: 18-3-2018]. Disponible en: http://dle.rae.es/srv/search?m=30&w=fisonom%C3%ADa

TESIS DE LA SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. México, 2009. [en línea]. [Consulta: 23-5-2018]. Disponible en: http://207.249.17.176/Transparencia/Documents/CriteriosPJF/Tesis_Tematica_Derecho_a_la_propia_imagen_e_identidad.pdf

EL ADIESTRAMIENTO Y EL ADOCTRINAMIENTO DE TERRORISTAS COMO DELITOS DE PREPARACIÓN DE ACTOS TERRORISTAS

Por: María Isabel Monserrat Sánchez-Escribano
España

I. INTRODUCCIÓN

En la última década, el legislador español ha reformado dos veces el Código penal en materia de terrorismo con la finalidad de ofrecer una mejor respuesta a la que es considerada hoy una de las principales amenazas de la actualidad: el terrorismo yihadista. Aunque dicha norma contenía ya diversos preceptos dirigidos a reprimir actos terroristas, lo cierto es que tales disposiciones estaban pensadas fundamentalmente para combatir un tipo de terrorismo interno de corte nacionalista, el representado por las organizaciones ETA o GRAPO, y no eran susceptibles de ser aplicadas con igual eficacia a otro fenómeno terrorista con importantes diferencias en su estructura organizativa, repertorio de violencia, capacidad operativa y alcance transnacional.

Una de las modificaciones más relevantes de la mencionada reforma ha sido la introducción de un nuevo artículo 575, que castiga tres acciones: la recepción de adoctrinamiento para cometer actos de terrorismo, ya sea por parte de un tercero (apartado 1) o de motu proprio a través del ciberespacio (apartado 2); la recepción de adiestramiento militar o de combate en los mismos términos, y, finalmente, el fenómeno de los combatientes terroristas extranjeros, es decir, el traslado o establecimiento en territorio dominado por un grupo terrorista. Su tenor literal reza lo siguiente:

Artículo 575

1. Será castigado con la pena de prisión de dos a cinco años quien, con la finalidad de capacitarse para llevar a cabo cualquiera de los delitos tipificados en este Capítulo, reciba adoctrinamiento o adiestramiento militar o de combate, o en técnicas de desarrollo de armas químicas o biológicas, de elaboración o preparación de sustancias o aparatos explosivos, inflamables, incendiarios o asfixiantes, o específicamente destinados a facilitar la comisión de alguna de tales infracciones.
2. Con la misma pena se castigará a quien, con la misma finalidad de capacitarse para cometer alguno de los delitos tipificados en este Capítulo, lleve a cabo por sí mismo cualquiera de las actividades previstas en el apartado anterior.
Se entenderá que comete este delito quien, con tal finalidad, acceda de manera habitual a uno o varios servicios de comunicación accesibles al público en línea o contenidos accesibles a través de internet o de un servicio de comunicaciones electrónicas cuyos contenidos estén dirigidos o resulten idóneos para incitar a la incorporación a una organización o grupo terrorista, o a colaborar con cualquiera de ellos o en sus fines. Los hechos se entenderán cometidos en España cuando se acceda a los contenidos desde el territorio español.

Asimismo se entenderá que comete este delito quien, con la misma finalidad, adquiera o tenga en su poder documentos que estén dirigidos o, por su contenido, resulten idóneos para incitar a la incorporación a una organización o grupo terrorista o a colaborar con cualquiera de ellos o en sus fines.
3. La misma pena se impondrá a quien, para ese mismo fin, o para colaborar con una organización o grupo terrorista, o para cometer cualquiera de los delitos comprendidos en este Capítulo, se traslade o establezca en un territorio extranjero controlado por un grupo u organización terrorista.

Como se ve, este precepto recoge conductas de participación necesaria que son la contrapartida del artículo 577. El artículo 575 castiga la modalidad pasiva, mientras que el artículo 577 la activa . Se trata de un precepto sobre el que, aparte de unos pocos estudios, los citados en el presente texto, no existe bibliografía doctrinal que lo analice. De ahí la importancia del presente texto.

II. RAZONES POLÍTICO CRIMINALES DE LA INCRIMINACIÓN DE ESTE PRECEPTO

Las razones político-criminales que han conducido al legislador español a aprobar la Ley Orgánica 2/2015, de 30 de marzo, son dos, las que se exponen a continuación.

1. El principal motivo de la incriminación de esta conducta ha sido, según palabras del propio legislador, la insuficiencia normativa para hacer frente a una nueva faceta del fenómeno terrorista: el terrorismo individual . Ello porque las disposiciones contenidas en nuestro Código penal en materia de terrorismo, tal y como se ha adelantado, no permitían ofrecer una respuesta eficaz en estos casos debido a que estaban articuladas en torno al terrorismo protagonizado por organizaciones y grupos terroristas .
2. Aparte de su propio deseo de castigar esta nueva amenaza, el legislador acomete también con esta reforma las exigencias derivadas de compromisos de carácter supranacional. Concretamente, la Resolución 2178 (2014) del Consejo de Seguridad de Naciones Unidas, el Protocolo Adicional del Convenio del Consejo de Europa para la Prevención del Terrorismo, de 20 de octubre de 2015 y la Decisión Marco 2002/475/JAI del Consejo de la Unión Europea, de 13 de junio de 2002, sobre la lucha contra el terrorismo, modificada por la Decisión Marco 2008/919/JAI, de 28 de noviembre de 2008.

En lo que concierne al artículo 575, debe hacerse notar que parte de su contenido tiene reflejo en la normativa internacional mencionada. Así, la propuesta de tipificación de la conducta de recepción de adiestramiento está prevista en el artículo 3 del Protocolo Adicional del Convenio del Consejo de Europa para la Prevención del Terrorismo , y la de traslado o establecimiento en territorio dominado por un grupo terrorista en el apartado 6 a) de la Resolución 2178 (2014) del Consejo de Seguridad de Naciones Unidas y artículo 4 del referido Protocolo . Sin embargo, la incriminación de la acción de adoctrinamiento no ha sido prevista por ninguna de las normas internacionales y comunitarias citadas, de modo que en este caso el legislador ha ido más allá de las exigencias internacionales.

III. NATURALEZA DEL ARTÍCULO 575: CRÍTICA A LA INCRIMINACIÓN DE LA ACCIÓN DE ADOCTRINAMIENTO

Por lo que se refiere a la naturaleza de estas acciones, el denominador común de todas ellas es que se trata de actos preparatorios o pre-preparatorios individuales de acciones terroristas concretas, lo que implica —en teoría— que ninguna de ellas supone una intervención ejecutiva, directa y material, en un acto terrorista sino que simplemente tienen una naturaleza facilitadora de un hecho delictivo concreto, en el sentido de que a través de ellas el sujeto o bien crea las condiciones óptimas para cometer el delito o bien se pertrecha de los instrumentos necesarios para realizarlo .

1. Sin perjuicio de lo anterior, considero que el contenido disvalorativo de una de estas conductas es distinto al de las demás. Así, para mí, mientras las acciones de recepción de adiestramiento y de traslado a un país extranjero con este fin permiten vislumbrar un todavía dudoso atisbo de futura intención criminal, ello no ocurre en la de adoctrinamiento, que se produce en una fase muy inicial del iter criminis, lo que, en mi opinión, conduce a que resulte imposible afirmar la naturaleza facilitadora de esta actividad así como su calificación si quiera como acto preparatorio. De ahí, por ejemplo, que doctrina y jurisprudencia lo califiquen como acto pre-preparatorio o proto-preparatorio.

A ello hay que añadir los conflictos que este precepto plantea en relación con el derecho a la libertad ideológica. De la propia noción de adoctrinamiento se infiere que este se concreta en el proceso de formación en la doctrina terrorista. Así pues, se integra únicamente por la realización de actos que no son más que la manifestación de una ideología concreta, la terrorista . Teniendo en cuenta que en España la Constitución proclama lo que se conoce como indiferentismo ideológico, entendido este en el sentido de que admite la defensa de cualquier tipo de ideología, incluso las contrarias al ordenamiento constitucional , se torna cuestionable la decisión político-criminal de activar el mecanismo represivo en el que consiste el Derecho penal para reprimir la formación en la doctrina terrorista, decisión cimentada únicamente en la idea de que esta ideología es profesada por el máximo enemigo actual del Estado: el terrorista yihadista.

Desde esta perspectiva, considero que resulta muy criticable que el Código penal castigue con idéntica pena conductas de muy distinto potencial lesivo: mientras que el adiestramiento y el traslado a territorio ocupado por un grupo terrorista tienen un carácter claramente facilitador, el adoctrinamiento no lo tiene. La acción de adoctrinamiento pasivo se encuentra en un estadio tan incipiente respecto a la afectación de cualquier interés que resulta muy difícil determinar que efectivamente vaya a concretarse en un futuro en un resultado lesivo. La mencionada modalidad no es otra cosa que un nuevo adelantamiento de la barrera de protección a estadios en los que apenas se ha dado el paso de la simple ideación —cogitationem nemo patitur— a conductas de una gran equivocidad en cuanto a los objetivos perseguidos . Esta lejanía de la afectación del bien jurídico aconseja su derogación, pero, entretanto, debe abogarse por una aplicación e interpretación muy restrictiva del precepto a supuestos en los que exista una especial intensidad, sin considerarse suficiente el mero acercamiento ideológico .

2. En consecuencia, debe resaltarse que el extremado adelantamiento de la barrera punitiva en la configuración del tipo penal determina su configuración como un delito de peligro abstracto .

a) Ello con independencia de que en realidad, como he dicho, no todas las conductas que contempla lleven implícito tal peligro siquiera abstracto para el bien jurídico protegido en los delitos de terrorismo . El potencial riesgo de estas conductas se basa en una presunción iuris tantum del legislador en relación con un "posible futuro atentado terrorista". De hecho, así mismo lo reconoce en la Exposición de Motivos de la Ley cuando hace referencia a que es una conducta que simplemente "puede" derivar en un ataque terrorista .

b) Dicho esto, no cabe duda de que los demás comportamientos ilícitos incriminados en el artículo 575 CP sí que presentan un eventual grado de peligrosidad con respecto a bienes jurídicos de gran valor . Así, puede observarse un cierto contenido de injusto de carácter objetivo en las acciones de adiestramiento (y autoadiestramiento) militar y de combate (apartado 1 y 2) así como en el traslado a territorio dominado por un grupo terrorista (apartado 3). Se trata como dice CANO PAÑOS de actividades que sí suponen la creación de un riesgo para bienes jurídicos de importancia, las cuales eventualmente podrían resultar merecedoras de reproche penal a través de la correspondiente creación de un delito de peligro abstracto .

IV. UN ELEMENTO DEL TIPO COMÚN A TODAS LAS CONDUCTAS: LA TENDENCIA SUBJETIVA DEL AUTOR

En tanto delito de preparación, todas las conductas recogidas en el artículo 575 vienen acompañadas de un elemento subjetivo del injusto, que en este caso se concreta en la finalidad de cometer un delito de terrorismo. En este sentido se expresan el primer párrafo del artículo 575.2 (con la finalidad de capacitarse para llevar a cabo cualquiera de los delitos tipificados en este Capítulo), el segundo párrafo (con tal finalidad) y, finalmente, el tercero (con la misma finalidad). Varias son las cuestiones a comentar en este punto:

1. El Tribunal Supremo ha afirmado que este elemento es diverso y contiene un elemento teleológico doblemente redoblado, de forma que la realización de la acción típica de adoctrinamiento o adiestramiento debe ser con la finalidad de capacitarse, donde el logro pretendido de tal aptitud, a su vez, ha de ser para llevar a cabo cualquiera de los delitos tipificados en este Capítulo (terrorismo) .
2. Esta intención delictiva del autor es, por tanto, el único elemento de conexión entre las acciones recogidas en el artículo 575 y un "posible" futuro ataque terrorista . De hecho, al utilizar el término "posible" quiero hacer notar que el adelantamiento de la barrera punitiva va más allá no solo de la preparación de un futuro atentado sino también, muy posiblemente, de la propia adopción de la decisión de cometerlo.
3. De este modo, el elemento subjetivo del injusto se convierte, a mi modo de ver, en el elemento fundamental de la infracción penal, ya que en él descansa, tal y como indica GARCIA ALBERO, por completo la delimitación entre lo que resulta penalmente relevante por un lado y el ejercicio de derechos fundamentales básicos (a difundir y recibir información, a la libertad ideológica, a la libertad de expresión, etc.), por otro .
4. En consecuencia, toda la carga probatoria deberá dirigirse a constatar la intención de que con su conducta el sujeto desea cometer más adelante un acto terrorista, un futurible que únicamente podrá ser contrastado necesariamente a través de prueba indiciaria o carga probatoria adicional. Así, quedarán excluidas todas aquellas actividades que encajen en las acciones que el tipo penal describe pero que se realicen por mera curiosidad en el aprendizaje

de los métodos utilizados por la violencia terrorista o por vivir una experiencia espiritual asociada a su credo religioso . En cualquier caso, ya existe una resolución judicial que aplica este precepto, concretamente la Sentencia del Tribunal Supremo 661/2017, de 10 de octubre, que condena por autoadiestramiento a un sujeto que se había auto-formado en la doctrina yihadista y que en el curso de las comunicaciones telefónicas familiares manifestó su anuencia a marcharse a Siria a cubrir el puesto dejado por su hermano cuando falleciera en el acto suicida al que estaba destinado.

5. En último lugar, es necesario hacer referencia al carácter abierto de la cláusula de remisión a los delitos fin. Resulta criticable el ansia incriminadora del legislador por lo que se refiere a este aspecto, ya que cada acción podrá constituir la antesala únicamente de un número determinado de conductas que podrían quedar perfectamente delimitadas en la descripción típica. Para GARCIA ALBERO cabe incluir los delitos de la sección primera: simple integración, y por supuesto todas las de la sección segunda del Capítulo dedicado a los delitos de terrorismo, incluyendo las mismas conductas del art. 577.2 (capacitación de capacitadores)—.

V. ANÁLISIS DE LAS CONDUCTAS DEL APARTADO 1 DEL ARTÍCULO 575: ADOCTRINAMIENTO Y ADIESTRAMIENTO PASIVO DE TERRORISTAS

El adoctrinamiento y adiestramiento pasivo de terroristas vienen recogidos en el apartado 1 del artículo 575 . Estas conductas se concretan en la recepción de adoctrinamiento o adiestramiento militar o de combate, o en técnicas de desarrollo de armas químicas o biológicas, de elaboración o preparación de sustancias o aparatos explosivos, inflamables, incendiarios o asfixiantes. Se castiga, por tanto, el proceso en el que un sujeto se deja instruir por otro en una serie de conductas enumeradas en la mencionada disposición, ello con la finalidad (elemento subjetivo del injusto como se ha indicado) de capacitarse para llevar a cabo cualquiera de los delitos de terrorismo . Véanse por separado cada una ellas.

A) ADOCTRINAMIENTO PASIVO

La primera acción típica consiste en la recepción de adoctrinamiento con el fin de obtener la capacitación necesaria para cometer actos de terrorismo. El adoctrinamiento que se castiga en este precepto es, en mi opinión, el mero adoctrinamiento ideológico, que se concreta en el proceso de instrucción personal en la "doctrina terrorista", es decir, en la inculcación de ideas y creencias dirigidas a cometer un acto terrorista. Se trata, simplemente, de un proceso educativo dirigido a transmitir determinados valores (contravalores) o formas de pensar (justificación ideológica) , porque, si se vincula a la enseñanza de habilidades tácticas precisas para desarrollar un eventual plan terrorista, entonces nos encontraríamos ya ante la conducta de adiestramiento .

A mi modo de ver, esta conducta puede tener lugar tanto de forma directa o personal, es decir, asistiendo de forma presencial a lugares donde se predique la doctrina terrorista, o bien de forma indirecta o a distancia, esto es, a través del análisis y estudio de materiales recibidos ya sea por correo postal o por vía telemática. Ambas modalidades pueden, por tanto, integrar el tipo penal.

Además, no todo adoctrinamiento pasivo será típico sino que, cómo se ha adelantado previamente, sólo lo será el que lo sirve y lo recibe con la finalidad de capacitarse para cometer delitos de terrorismo. En este sentido, tal y como afirma GARCIA ALBERO, la inferencia y prueba de dicho elemento subjetivo se muestra aquí extremadamente problemática, salvo que el adoctrinamiento recibido, por sus características, esté no sólo subjetivamente sino objetivamente orientado a la integración de tal finalidad de modo indiscutible .

En cualquier caso, aunque, como se ha indicado, la extrema lejanía para la afectación del bien jurídico no se pone en peligro el bien jurídico aconsejan su derogación, por el momento, la equiparación penológica entre adoctrinamiento y adiestramiento aconsejan que esta actividad de aprehensión de credos debe tener una especial intensidad, sin que baste el mero acercamiento ideológico .

B) ADIESTRAMIENTO

La segunda conducta que castiga el artículo 575 es la recepción de adiestramiento militar o de combate, o en técnicas de desarrollo de armas químicas o biológicas, de elaboración o preparación de sustancias o aparatos explosivos, inflamables, incendiarios o asfixiantes. Esta acción constituye el reverso de la que específicamente se prevé en el apartado 2 del artículo 577 del Código Penal: el artículo 577 castiga al docente, el artículo 575, al discente. GARCÍA ALBERO considera que entre ambos preceptos se da un solapamiento, ya que el artículo 577 en su apartado 2 castiga la organización de prácticas de entrenamiento, pero también la asistencia a las mismas . Así pues, para el autor, cuando el adiestramiento se verifica en modo de asistencia a prácticas de entrenamiento, tal conducta está ya específicamente prevista en el art. 577.1 CP como acto de colaboración con actividades o grupos terroristas (o de comisión de los delitos) . En mi opinión, sin embargo, puede establecerse una la línea divisoria clara entre uno y otro precepto: el artículo 575.1 castiga la participación activa en prácticas de entrenamiento terrorista mientras que conforme al artículo 577.2 se penará la mera asistencia a tales prácticas sin tomar parte activa en ellas (la conducta del mero observador) o su organización. La diferencia entre el ámbito aplicativo de ambas normas radica, pues, en que en el primer caso se quieren cometer actos terroristas, mientras que en el segundo solo cooperar o colaborar con la organización. Piénsese, además, que el artículo 577 está penando la modalidad activa de la conducta y, el artículo 575, la pasiva.

VI. ANÁLISIS DE LAS CONDUCTAS DEL APARTADO 2 DEL ARTÍCULO 575: AUTOADOCTRINAMIENTO Y AUTOADIESTRAMIENTO

El apartado 2 del artículo 575 castiga a quien lleva a cabo por sí mismo cualquiera de las actividades enunciadas en el apartado 1 : autoadoctrinamiento y autoadiestramiento. Particularmente, esto significa que se incrimina la conducta de aquella persona que pretende capacitarse para llevar a cabo delitos de terrorismo de forma individual y aislada.

2. En este caso, el precepto establece una presunción en relación con los supuestos en los que deberá entenderse que se comete este delito: cuando se acceda telemáticamente de manera habitual a contenidos terroristas, cuando se utilicen servicios de telecomunicación

transmitiendo o recibiendo este contenido, o cuando se adquiera o posea documentos con tal contenido .

a) La literalidad del precepto se refiere a aquellas actividades ilícitas que el sujeto realice mediante el uso de Internet o de las redes sociales. Atiende, en este sentido, a la realidad criminológica actual, ya que estos medios se han convertido no sólo en un nuevo escenario de conflicto sino en el cauce más habitual que la yihad utiliza para lograr el reclutamiento y la formación de los potenciales terroristas (más del 80% según datos del subdirector general de tratamiento y gestión penitenciaria del Ministerio del Interior, Javier Nistal Burón) .

b) El precepto utiliza una única definición para determinar cuándo debe considerarse que existe delito sin distinguir en qué casos debe considerarse que existe autoadoctrinamiento y en cuáles autoadiestramiento. Aunque se trata de una mera cuestión teórica porque nos encontramos ante un tipo mixto alternativo en el que ambas conductas tienen atribuida la misma pena, entiendo que la subsunción de los hechos en una u otra dependerá del examen del contenido accedido, transmitido, adquirido o poseído. Ejemplo de esta idea constituye la Sentencia 661/2017, de 10 de octubre, que aprecia la existencia de autoadoctrinamiento en un supuesto en que el acusado utilizaba un teléfono que contenía vídeos y fotografías de las acciones y militantes de la organización DAESH-Estado Islámico en la que militaba su hermano, destinados a instruirse en su credo e incitar su integración a ella.

3. En cualquier caso, todo ello a la espera de que la concurrencia del elemento subjetivo del injusto consistente en la intención de cometer un acto terrorista pueda ser probada , una prueba que a mi juicio resultará extremadamente complicada en tanto en cuanto los principios a la presunción de inocencia e in dubio pro reo conducirán a que cualquier explicación verosímil acerca de por qué se ha accedido habitualmente o se poseen tales contenidos enerve la prueba de tal elemento.

VII. COLABORACIÓN CON ORGANIZACIONES TERRORISTAS

El tercer apartado del artículo 575 determina: La misma pena se impondrá a quien, para ese mismo fin, o para colaborar con una organización o grupo terrorista, o para cometer cualquiera de los delitos comprendidos en este Capítulo, se traslade o establezca en un territorio extranjero controlado por un grupo u organización terrorista.

Esta previsión responde a la necesidad de hacer frente al problema de los combatientes terroristas extranjeros, un fenómeno que, como señala la Resolución 2178 de las Naciones Unidas, ya citada, aumenta la intensidad, duración e insolubilidad de los conflictos armados regionales. La acción típica consiste en trasladarse a territorio extranjero controlado por grupo u organización criminal con la finalidad de capacitarse para la comisión de delitos, para cometerlos directamente, o para integrarse en grupo u organización terrorista.

1. Nuevamente debe ponerse este apartado en relación con el artículo 577, cuyo apartado 1 castiga la realización de actos de colaboración de terceros que faciliten el acogimiento o traslado de personas.
2. Coincido con GARCIA ALBERO cuando señala que en la práctica esta conducta irá en un alto porcentaje de casos precedida de la recepción de un previo adoctrinamiento . Ahora bien, en mi opinión, que difiere en este aspecto a la del autor, en un número muy reducido de

ocasiones este comportamiento irá precedido también de un previo adiestramiento militar o de combate, puesto que lo más probable es que este sea el motivo del traslado.
3. Exige por lo demás el precepto que el traslado se efectúe a territorio extranjero controlado por un grupo u organización terrorista, lo que excluye traslados a zonas donde pese a verificarse actividad terrorista por parte de organizaciones o grupos, estos no ostentan un control efectivo sobre el territorio .
4. Por último, destacar que resulta muy discutida la cuestión de si esta modalidad típica ha de entenderse como modalidad materialmente autónoma respecto de las anteriores, y si, en consecuencia, la simple búsqueda reiterada de información sobre cómo realizar el viaje es ya constitutiva de delito vía art. 575.2 CP .

VIII. CONCLUSIONES

I. El artículo 575 será una de los preceptos más controvertidos de la reforma operada por la Ley Orgánica 2/2015, de 30 de marzo, especialmente en lo que concierne a la conducta de adoctrinamiento. Con ella se pretende ofrecer una mejor respuesta penal a la que es considerada una de las principales amenazas de la actualidad: el terrorismo yihadista. No obstante, esta previsión está tensionando de forma preocupante principios hasta ahora asentados del derecho penal en un Estado democrático.

II. Este precepto castiga de forma alternativa un conjunto de tres acciones que, en principio, vienen a conformar actos preparatorios o pre-prepatarorios individuales de acciones terroristas concretas. Sin embargo, el potencial lesivo de cada una de estas acciones es muy distinto, siendo que en la acción de adoctrinamiento se encuentra en un estadio tan incipiente respecto a la afectación de cualquier interés que resulta muy difícil determinar que efectivamente vaya a concretarse en un futuro en un resultado lesivo. Esta lejanía de la afectación del bien jurídico aconseja su derogación, pero, entretanto, debe abogarse por una aplicación e interpretación muy restrictiva del precepto a supuestos en los que exista una especial intensidad, sin considerarse suficiente el mero acercamiento ideológico .

III. Dicho esto, no cabe duda de que los demás comportamientos ilícitos incriminados en el artículo 575 CP sí que presentan un eventual grado de peligrosidad con respecto a bienes jurídicos de gran valor . Así, puede observarse un cierto contenido de injusto de carácter objetivo en las acciones de adiestramiento (y autoadiestramiento) militar y de combate (apartado 1 y 2) así como en el traslado a territorio dominado por un grupo terrorista (apartado 3).

IV. En cualquier caso, el elemento determinante para afirmar la comisión de este ilícito es el elemento subjetivo del injusto, que se concreta en la finalidad de capacitarse para cometer un delito de terrorismo. El legislador hace pivotar la tipicidad sobre la presunción iuris tantum de la posible comisión por parte del sujeto de un futuro atentado terrorista, un estadio temporal incierto y nada concretizado, ubicándose el acto preparatorio en una fase de planificación precoz en lo temporal y vaga en lo material. A tal efecto, como indica CANO PAÑOS, el legislador podría haber configurado un tipo penal consistente en la simple posesión, aún el acceso, a material gráfico o audiovisual que, con inequívoca finalidad apologética o propagandista, consista en la representación de un delito de terrorismo, como ha hecho en otros ámbitos, pero no lo ha hecho. En consecuencia, no estamos ante un simple

delito de acceso o posesión calificado por la clase de contenido, sino por el objetivo que persigue el sujeto: capacitarse para cometer delitos de terrorismo.

VI. BIBLIOGRAFÍA

ALONSO RIMO, A. "¿Impunidad general de los actos preparatorios?: La expansión de los delitos de preparación", en Indret: Revista para el Análisis del Derecho, (4), 2017.

ALONSO RIMO, A. La criminalización de la preparación delictiva a través de la parte especial del Derecho penal, en Terrorismo, sistema penal y derechos fundamentales, Tirant lo Blanch, Valencia, 2018 pág. 215-260.

BAYARRI GARCÍA, C. E. Los nuevos delitos de terrorismo. Adoctrinamiento activo y pasivo vs. enaltecimiento, en Terrorismo, sistema penal y derechos fundamentales, Tirant lo Blanch, Valencia, 2018, pág. 279-298.

CANO PAÑOS, M. A. La nueva amenaza terrorista y sus (negativas) repercusiones en el ordenamiento penal y constitucional. Comentario a la sentencia de la audiencia nacional núm. 39/2016, de 30 de noviembre, en Revista Electrónica de Derecho penal y Ciencias Penales, 2017.

CAMPO MORENO, J. C. Comentarios a la Reforma del Código Penal en Materia de Terrorismo: la L.O. 2/2015, Tirant lo Blanch, Valencia, 2015.

CUERDA ARNAU, M. L. Terrorismo, en Derecho penal. Parte Especial (VIVES ANTÓN (dir.)), Tirant lo Blanch, Valencia, 2016.

FUENTES OSORIO, J.L. La preparación delictiva, Comares, Granada, 2006.

GARCIA ALBERO, R. Artículo 575, en Comentarios al Código penal español (QUINTERO OLIVARES, G. (dir.)), Aranzadi, Navarra, accesible en Thomson-Reuters ProView, 2016.

MUÑOZ CONDE, F. Derecho penal. Parte Especial, Tirant lo Blanch: Valencia, 2017.

VV.AA. Memento Penal Práctico, Ediciones Francis Lefevre, 2017.

MODA TECNOLÓGICA: HACIA UNA HIPERCONEXIÓN TOTAL

Por: ***Ana Karin Chávez V.***
Perú

INTRODUCCIÓN

Es indiscutible que la wearable technology ha evolucionado vertiginosamente y en paralelo a los diversos avances tecnológicos. La expansión de esta innovación disruptiva no solo implica la presencia de una tecnología más precisa, portátil y asequible en nuestras vidas sino que además el "diseño centrado en el ser humano" deviene en un factor esencial para su éxito

En este sentido la wearable technology ha encontrado múltiples aplicaciones en diversos sectores y viene ganando un espacio cada vez mayor. Más aún, este concepto innovador se está expandiendo vertiginosamente y está produciendo una transformación de dispositivos móviles a dispositivos wearables.

Dentro de este contexto uno de los principales desafíos aún por resolver en relación a su uso se cierne en torno a la privacidad y consecuente seguridad, no solo debido a la enorme cantidad de información que pueden reunir los wearables sino también porque pueden detectar, capturar y almacenar información sensible sobre los usuarios y sus alrededores de manera continua y discreta

Al mismo tiempo la prometedora relación moda y wearable technology dentro de la cual convergen algunos derechos clásicos de la propiedad intelectual plantea la necesidad de contar con mecanismos legales uniformes que permitan regular la creación, aplicación e implicancias derivadas de su uso lo que conllevará a un obligado análisis sobre la pertinencia de las normativas actuales y la importancia de contar con regulaciones acordes a las probables repercusiones aparejadas al inminente desarrollo de esta tecnología dentro de las diferentes áreas del derecho.

1. WEARABLE TECHNOLOGY

Años atrás hubiera parecido casi imposible considerar la posibilidad que algún objeto pudiera "seguirnos a todas partes". En los últimos años la wearable technology no sólo desbordó esta posibilidad sino que además, centrada en el ser humano, integró la tecnología con la moda acorde al estilo de vida actual y necesidades de cada persona.

La idea implícita en el término "wearable" es "que puede llevarse puesto". En este sentido, la wearable technology o tecnología ponible, es aquella diseñada para ser vestida, ya sea como complemento o como parte de algún material usado en la ropa. Los desarrolladores actualmente están considerando todo el cuerpo humano como una oportunidad para la conexión[1].

[1] Han pasado casi 20 años desde Gemperle y otros autores escribieron "Design for Wearability" y aunque gran parte de sus directrices iniciales sobre los factores humanos que rodean la capacidad de resistencia siguen en pie, los dispositivos y los casos de uso han cambiado con el tiempo; sin embargo, la tecnología portátil se ha

Cabe señalar además, que este contexto tecnológico ha dado lugar a la aparición de un nuevo concepto: el "yo cuantificado"[2] para referirse precisamente a la práctica de registrar y analizar los hábitos, pensamientos, emociones y comportamientos propios con la ayuda de dispositivos digitales, el mismo que viene suscitando críticas importantes en torno a la responsabilidad o irresponsabilidad de tratar de reducir el ser humano a números y se le viene dando denominaciones alternativas tales como: "Yo cualitativo", "Informática personal", "Auto-seguimiento", "Auto-monitoreo", "Analítica personal", "Informática personal", entre otros (Rodríguez, 2015) debido precisamente a que cada día se incrementa el número de personas que cuantifican su vida recopilando información sobre sus actividades simples y cotidianas a través de diversos dispositivos o herramientas tecnológicas cuyo número no sólo va en ascenso sino que también comprende distintas categorías de wearables[3].

Enumerar detalladamente los aspectos que abarcan cada uno de ellos se convertiría en una lista interminable; sin embargo lo que sí es innegable es que esta cuantificación crea una especie de línea temporal que es susceptible de análisis para múltiples finalidades exponiendo nuestro registro de vida digital a quienes estén interesados en darle uso a nuestra información personal.

Actualmente existen diversas conceptualizaciones sobre la wearable technology. Para Thierer (2015) las tecnologías usables son dispositivos en red que pueden recopilar datos, rastrear actividades y personalizar experiencias según las necesidades y deseos de los usuarios".

De otro lado, Langley (2015) señala que los dispositivos de consumo son capaces de monitorear información sensitiva de signos vitales, y las compañías están recolectando fácilmente una cantidad desproporcionada de datos individuales. Estos dispositivos se conocen como "vestibles" y pueden monitorear la frecuencia cardíaca, el nivel de estrés, la actividad cerebral, la respiración, la temperatura corporal, el nivel de hidratación y otra información relacionada de un individuo.

Por su parte Alsadoon, Costadopoulos, Prasad y Segura (2018) consideran que "Tecnología usable" se refiere a prendas de vestir o accesorios mejorados mediante el uso de productos electrónicos, destinados a fines informativos o de entretenimiento. Este tipo de tecnología generalmente se adjunta al cuerpo y se puede utilizar para controlar la información sobre los usuarios y su entorno.

---

extendido a los nuevos dominios de aplicación en los últimos 20 años. Los dispositivos se han vuelto más pequeños y también pueden detectar y medir más. Ahora se usan más dispositivos portátiles como sensores corporales, y ahora hay más dispositivos que aprovechan la capacidad del cuerpo humano para detectar. Nuestra comprensión de cómo percibimos e interactuamos con dispositivos portátiles también ha crecido.

[2] En el 2007 Gary Wolf y Kevin Kelly, emplearon por primera vez el término Yo Cuantificado (Quantified Self) para referirse al modo en que los individuos estaban "encontrando estrategias ingeniosas para extraer datos a partir de actividades habituales".

[3] El WebSite denominado Quantified Self. Guide to Self-tracking tools presenta una amplia gama de aplicaciones que realizan funciones de rastreo personalizado ofreciendo al internauta la opción de poder revisarlas en detalle de modo que pueda realizar una elección informada en torno a esta tecnología http://quantifiedself.com/guide/tools?sort=reviews&pg=6

El grupo de trabajo de la Comisión Europea (2014) emplea el término "computación usable" para hacer referencia a los wearables y aunque el documento elaborado analiza tres tipos distintos de bienes en relación a la protección de datos en el "Internet de las Cosas" -Internet of Things- precisa que es probable que las cosas usables se adopten rápidamente a medida que extienden la utilidad de los objetos cotidianos que le resultan familiares, sobre todo porque difícilmente pueden diferenciarse de sus semejantes desconectados y porque pueden incorporar cámaras, micrófonos y sensores que pueden registrar y transferir datos al fabricante del dispositivo.

De otro lado, como acertadamente señala Ciçek (2015) el alcance de la tecnología ponible es muy amplio y amorfo, aun así contempla una división que comprende tres categorías principales en torno a la wearable technology como son: las tecnologías portátiles de salud, tecnologías textiles portátiles y productos electrónicos de consumo portátiles.

En este sentido, refiere también Luque (2016) que existen múltiples tipos de dispositivos para ser llevados puestos entre los que pueden mencionarse: gafas, lentillas, relojes, ropa electrónica, bandas de pelo, gorras, joyas (anillos, brazaletes, colgantes, pendientes) auriculares, cascos, cinturones, zapatos, guantes, exoesqueletos, entre otros. Señalando además que, adicionalmente, se consideran también wearables a los dispositivos implantados en el organismo, bien como microchips insertados, bien como tatuajes grabados en la piel. Incluso según avance la tecnología, estarían contemplados dentro de este tipo de dispositivos aquellos que sean ingeridos para cumplir una función de recopilación y transmisión de información.

Para la multinacional americana Cognizat (2014) los Wearables se pueden agrupar en general en cinco categorías: fitness, medicina, estilo de vida, juegos e información y entretenimiento. Sin embargo y dentro de este contexto pareciera que a pesar de los reiterados intentos aún no existe un consenso tendiente a establecer cuáles serían los requisitos esenciales para que un dispositivo pudiera ser considerado ponible dentro de la perspectiva de la wearable technology lo que ha significado que desde ahora cierto tipo de tecnología ya esté excluida de este rubro; sin embargo como señalamos anteriormente creemos que esta deviene en una tarea bastante compleja dada su propia naturaleza. Adicionalmente y muy a pesar de la falta de consenso delineada en el párrafo anterior lo que sí pareciera estar más definido son las capacidades o funciones que estos wearables deberían tener.

Entre algunas de las características comunes fundamentales de esta tecnología y sus dispositivos asociados -llamados también wearable devices- se encuentran la capacidad de conectividad inalámbrica, la compatibilidad con las plataformas y herramientas estándar de la industria, la introducción de datos realizada por el usuario o el almacenamiento de información en los dispositivos, los cuales pueden también interactuar con nosotros mismos, con otros dispositivos o con el entorno, lo que le ha dado el calificativo de "tecnología inteligente".

En este sentido Ciçek (2015) señala que estas tecnologías consisten en al menos cinco funciones principales. Estas funciones son: la interfaz como medio para transferir datos entre el usuario y el dispositivo. La comunicación entendida como la transferencia de información

a través de radiofrecuencias, sistemas inalámbricos, infrarrojos, tecnología Bluetooth y red de área personal. La gestión de datos, referida al almacenamiento y procesamiento de datos. La gestión energética vinculada a la duración de las baterías y los circuitos integrados.

Por su parte Hu (2015) considera que un buen dispositivo wearable debe tener tres condiciones: en primer lugar, debe contactar razonablemente a las personas de forma lógica, es decir la intrusión no debe ser demasiado fuerte. En segundo lugar, debe poder recopilar información del usuario que sea lo suficientemente precisa. Finalmente, debe brindar soluciones al usuario, no solo para prestar atención a la información, sino también a la solución en sí misma.

Refiere asimismo, Mind Commerce Staff (2014) que la adopción de esta tecnología por parte de los usuarios depende de varios factores entre los que considera el peso de un wearable, destacando su importancia en la medida en que el dispositivo va estar conectado al cuerpo del usuario y de ser pesado no será usado; en tanto, un wearable liviano le permitirá involucrarse en actividades de tareas múltiples porque el peso no le impide realizar sus despliegues habituales. La comodidad es también considerada como otro factor crítico para su adopción ya que un dispositivo debe ser fuerte y no verse afectado por la temperatura u otros factores externos que puedan generar algún tipo de incomodidad a quien lo usa. El tamaño además debe ser el apropiado para la tarea que el dispositivo está diseñado a realizar; un tamaño pequeño puede mejorar la capacidad del dispositivo para completar sus tareas, mientras que un tamaño grande no puede ser fácil de usar y conducirá a una lenta adopción por parte del usuario final. El costo es otro elemento a considerar ya que la mayoría de los dispositivos nuevos tienden a tener un alto costo de compra para los consumidores, independientemente del costo de producción para los fabricantes.

A todo esto se suma indiscutiblemente un extenso y disímil entorno legal a nivel internacional que podría afectar la adopción de los wearables de muchas maneras debido a las múltiples normativas y enfoques en relación a la protección de los datos personales, privacidad o seguridad.

Las tendencias del mercado de los wearables muestran que se espera un aumento lento pero continuo en la demanda de esos dispositivos. Según el informe Business Insider Intelligence (2015), el mercado en este sector crecerá a una tasa del 35% entre 2014 y 2019.

2. LA NUEVA TENDENCIA DE LA MODA FUNCIONAL

No en muchos campos se evidencia lo efímero o temporal como en el sector de la moda donde es imposible no observar los cambios que se producen de una "temporada" a otra. Esta industria posee características que le son propias y en consecuencia diferenciadoras que van desde el entendimiento de los procesos productivos, pasando por los ciclos o temporadas de los productos en el mercado, la innovación, los símiles sin que necesariamente sean copias, hasta la expansión de las industrias internacionales.

Podemos afirmar que la moda es una manifestación de la cultura de una sociedad en un lugar y tiempo determinado. Por ello, con el transcurrir de los años ha pasado de cumplir un rol

únicamente utilitario (necesidad básica de vestirse) a tener una finalidad estética. Actualmente consideramos que se le ha añadido un rol funcional jamás pensado, producto del desarrollo tecnológico; esto es, la moda de la wearable technology.

Brenda Salas (2013) refiere que, a pesar de que por cientos de años la moda fue observada únicamente como la necesidad básica de vestirse, se convirtió en el lenguaje empleado por hombres y mujeres en distintos momentos de la historia. En este sentido, la industria de la moda ha sido entendida como una manera pasajera de ser o de hacer, pero largamente adoptada y valorizada en un grupo y con alcance cultural. Por lo tanto, se convierte en un concepto transversal que se extiende incluso a las maneras de pensar de una sociedad y no solamente se aplica al ámbito textil y al vestido. Al mismo tiempo, esto involucra una serie de conceptos como la creación, creatividad y novedad, términos todos que se traducen en la llamada innovación.

La moda es una de las industrias más grandes del mundo. Al mismo tiempo, es una de las más antiguas. Su protección siempre ha gravitado en torno a dos ramas de la propiedad intelectual: el Derecho de autor y la Propiedad industrial. Siendo así, en el contexto internacional se evidencia que la moda no encuentra un régimen jurídico uniforme de protección. En el Derecho anglosajón los diseñadores recurren a las figuras tradicionales de la propiedad intelectual como marcas, patentes, diseño y derecho de autor. En tanto el sistema europeo presenta un Derecho con figuras sui generis.

En el Perú, se establece que las creaciones de moda son consideradas como obra de arte aplicado, siempre y cuando cumplan con el requisito de originalidad que la ley establece para tal fin. Es decir, que la creación en cuestión exprese la personalidad del diseñador y no sólo provenga de la naturaleza de las cosas. En este sentido establece el artículo 2°, numeral 20 del Decreto Legislativo N° 822 – Ley sobre el Derecho de Autor - que una obra de arte aplicado es una creación artística con funciones utilitarias o incorporada en un artículo útil, ya sea una obra de artesanía o producida en escala industrial. Adicionalmente nuestra legislación contempla también la posibilidad de proteger las creaciones de moda mediante los Signos distintivos y el Diseño industrial.

Indiscutiblemente, entre las disciplinas señaladas se presentan zonas fronterizas que hacen posible la protección de un mismo bien intelectual dentro de cada una de ellas bajo diferentes ópticas y con distinto contenido. Debido a que a nivel internacional las soluciones que arroja el Derecho Comparado no son uniformes, se evidenció en el ADPIC un intento de lograr una armonización en relación a este tema; sin embargo la dificultad estriba en el hecho que no todos los países reconocen al derecho de autor como una alternativa eficaz para amparar este tipo de industria.

Debemos considerar que la moda contemporánea, además de comprender indumentaria (entendida tiempo atrás únicamente como prendas de vestir), a la fecha hace referencia a un universo tecnológico heterogéneo que incluye diversos segmentos como relojes, computadoras, joyas, teléfonos, gafas, artículos deportivos, productos que permiten visualizaciones en espacio 3D, entre otros. En ese orden de ideas, deviene en impostergable un análisis en torno al régimen de protección en el cual se enmarca esta industria creativa, toda vez que ella se orienta hacia dos ángulos: el estético y el funcional.

Tomar las mejores decisiones de diseño para dispositivos portátiles es un desafío debido a su género multidisciplinar, Es difícil considerar y priorizar adecuadamente las perspectivas de los usuarios y la tecnología. Tener en cuenta sus requisitos y limitaciones específicas puede llevar a muchas compensaciones. Mientras que desde la perspectiva de los usuarios, la estética y la comodidad son obligatorias; desde una perspectiva tecnológica, la funcionalidad y la duración de la batería son las prioridades. Lidiar con estas prioridades multidisciplinarias genera discusiones en el proceso de diseño. Por lo tanto, los profesionales deben analizar cuidadosamente los costos y beneficios de cada solución antes de tomar las decisiones adecuadas.

Es indiscutible que nos encontramos dentro de un sector de la moda que indiscutiblemente presenta innovaciones técnicas y tecnológicas. En este sentido compartimos parcialmente la opinión de Salas (2013) al señalar que al conjugarse las innovaciones con el carácter estético se daría lugar a otra dinámica: la de la invención y discrepamos cuando señala que a pesar que de hablar de innovación, no se hace en referencia al concepto de patentes, es decir, a la invención entendida como una solución a un problema no resuelto en el estado de la técnica tratándose más bien de una innovación desde el punto de vista estético, que deberá expresar las fantasías e innovaciones de esta naturaleza en materia de indumentaria concluyendo la autora que al hacer referencia a una creación de forma estética u ornamental, se corresponde a ese fenómeno.

El ámbito estético vinculado con la creatividad y novedad ha sido abordado desde distintos sistemas normativos; sin embargo, la moda tecnológica involucraría adicionalmente al sistema de patentes en relación a una sólida plataforma de innovaciones.

Consideramos que si la creación de la moda es calificada de innovación técnica o tecnológica, respondería a un régimen de protección no exclusivamente diferente, cual es el sistema de patentes y/o modelos de utilidad -que por su naturaleza presenta otras características y sistema de tutela- sino tal vez un sistema mixto donde confluirán diversos sistemas de protección.

Sin embargo, es innegable que el cambio constante y la vida efímera de la industria de la moda revelan la necesidad de reconocer que las actuales formas de protección contempladas por el derecho tal vez son insuficientes para subsanar algunas deficiencias y ofrecer soluciones certeras en campo de la moda convencional por lo que consideramos que la prometedora relación moda y tecnología probablemente presenten dificultades mayores debido a la propia naturaleza de la wearable technology.

En nuestro país como muchos otros aún existe ausencia legal en torno a la moda tecnológica propiamente dicha y se evidencia sin embargo que no es un tema trivial la necesidad de establecer una normativa al respecto. Nos encontramos ante el imparable avance de la moda tecnológica que aventaja de lejos a la tradicional y que por sus particulares y propias características probablemente demande la integración no sólo de los diversos sistemas de protección analizados sino que deberá buscar también consenso en espacios transdisciplinarios con miras al establecimientos de una normativa acorde y realmente eficaz, ya que la tecnología juega un papel esencial y las innovaciones tecnológicas avanzan a un

ritmo vertiginoso por lo que la regulación no deberá ser un impedimento para frenar su propio desarrollo o de alguna forma limitar la competencia dentro del mercado.

3. LOS WEARABLES Y SU RELACION CON NUESTROS DATOS

El problema de la privacidad y consecuente seguridad es uno de los principales desafíos aún por resolver en relación al uso la wearable technology. No solo debido a la enorme cantidad de información que puede reunir sino también porque también puede detectar, capturar y almacenar información sensible sobre los usuarios y sus alrededores de manera continua y discreta.

Siendo así, un punto de inflexión crítico para la categoría wearable es su capacidad para dar cuenta de los entornos ambientales y tomar datos de manera transparente, ya que eso contribuye de manera esencial a la generación de datos. A esto se suma el hecho de que por su propia naturaleza los wearables no pueden separarse de Internet of Things (IoT), ya sea local o remoto y deben interactuar con otros servicios y utilizarse junto con la nube y las correspondientes aplicaciones de Big Data por lo que las preocupaciones relacionadas con la privacidad y la seguridad crecerán a medida que estos dispositivos y servicios proliferen y se produzca una posterior hiperconexión entre ellos.

Estas preocupaciones son diversas y van desde el acceso no autorizado al dispositivo en sí mismo por parte de un tercero; el acceso a la información que el dispositivo comparte con dispositivos o sistemas cercanos a través de algún mecanismo inalámbrico hasta el acceso a la información transmitida a la nube o a cualquier sistema de almacenamiento remoto.

En este sentido Thierer (2015) considera que la mejor alternativa de regulación en torno a la tecnología ponible consiste en abordar las diversas inquietudes mediante una combinación de herramientas de empoderamiento tecnológico, normas sociales, presión pública y vigilante, mejores prácticas de la industria y autorregulación, transparencia y objetivos específicos y aplicación de estándares legales existentes, acorde a las necesidades emergentes. Más aún, sostiene que este enfoque en capas para abordar las diversas problemáticas que incorpora muchas soluciones diferentes no sofocaría de forma preventiva la experimentación tecnológica y la innovación.

Compartimos la opinión del autor al señalar que a estas consideraciones debe sumarse la gradualidad de adaptación social e individual la cual desempeñará un rol trascendental en torno a los wearables como ha sucedido con todas las otras transformaciones tecnológicas disruptivas y consideramos que no hay soluciones innovadoras que puedan resolver de forma instantánea o sencilla estos complejos problemas. Sostiene además, que esta preocupación está llevando a la repetición de un debate que ya ha ocurrido muchas veces en la economía de la información moderna: el choque entre la mentalidad de "innovación sin permiso"[4]

[4] El término se refiere a la noción de que la experimentación con nuevas tecnologías y modelos de negocios generalmente debería permitirse por defecto. A menos que se pueda argumentar convincentemente que una nueva invención causará un daño grave a las personas, se debe permitir que la innovación continúe sin interrupción, y los problemas, si se desarrollan, se pueden abordar más adelante. La innovación sin permiso no es una posición absolutista que niega cualquier rol para el gobierno. Más bien, es un objetivo ambicioso que enfatiza el beneficio de impulsar la "innovación permitida" como la mejor posición predeterminada para comenzar los debates sobre la política tecnológica. La carga de la prueba recae en aquellos

y "principio de precaución"[5].

En este orden de ideas, es innegable que nos enfrentamos dos grandes disyuntivas: Mientras que algunos autores como Popat y Sharma (2013) han declarado los peligros de los wearables afirmando que si estas tecnologías se dejan desatendidas y/o no aseguradas, la información privada sobre las personas y las empresas puede ser robada y en concordancia Ackerman (2012) afirma que la tecnología ponible podría conducir a una pérdida de control sin precedentes sobre la información personal del individuo. Sus detractores señalan que la mayoría de los problemas de privacidad se pueden resolver a través de leyes y legislaciones, firewall, antivirus, antispyware y software antimalware diseñados exclusivamente para tecnologías portátiles y que los beneficios de las tecnologías portátiles superarán los riesgos y nos traerán un futuro más seguro, fácil, más saludable, más rápido, moderno y más entretenido.

Por otro lado compartimos el criterio de García (2015) al precisar cuál es el tratamiento que vienen recibiendo los datos personales por parte de los wearables:

a) Falta de transparencia al obtener el consentimiento del usuario
En muchos casos, la recolección de datos que llevan a cabo algunos dispositivos electrónicos pasa inadvertida para el usuario. Los mecanismos clásicos para obtener el consentimiento del usuario podrían resultar difíciles de implantar en los wearables, obteniendo un consentimiento de baja calidad basado en la falta de información.

b) Uso de datos con fines distintos a aquellos para los cuales se recogieron
El incremento de la cantidad de datos procesados por los dispositivos inteligentes en combinación con las nuevas técnicas de análisis de datos y el intercambio de los mismos podría permitir un uso secundario de dichos datos, relacionado o no con la finalidad inicialmente prevista.

c) Riesgos de seguridad: ¿implica una pérdida de eficiencia del dispositivo el aumento de los requisitos de seguridad?
Los wearables adolecen de un problema de limitación de espacio y de autonomía energética evidentes y aún se desconoce cómo pretenden los fabricantes equilibrar el cumplimiento de los deberes de protección de datos con la necesidad de optimizar los recursos del dispositivo. Menos seguridad en los wearables conllevaría nuevas formas potenciales y eficaces de ataque, incluyendo datos personales robados o comprometidos que pueden perjudicar los derechos de los usuarios y menoscabar la imagen de seguridad de internet. La mayoría de los sensores que se encuentran actualmente en el mercado no son capaces de encriptar el acceso de las comunicaciones puesto que los requisitos informáticos tienen un impacto limitado en el dispositivo por su batería de baja potencia.

que favorecen los controles precautorios y precautorios para explicar por qué no se debe permitir la experimentación continua de prueba y error con nuevas tecnologías o modelos comerciales.

[5] En términos generales, se refiere a la creencia de que las innovaciones nuevas deben reducirse o anularse hasta que sus desarrolladores puedan demostrar que no causarán ningún daño a individuos, grupos, entidades específicas, normas culturales o varias leyes, normas o tradiciones existentes. Los defensores creen que los legisladores deberían regular las nuevas tecnologías "temprano y con frecuencia" para "adelantarse" y abordar preocupaciones sociales y económicas preventivamente.

Pareciera que un punto crucial en esta discusión es que no existe una solución a todos estos complejos problemas de privacidad. En este sentido señala Adam Thierer (2015) que analistas como la firma internacional de abogados Morrison Foerster han argumentado que las amenazas a la seguridad y la privacidad varían considerablemente, y la amplitud de los desafíos que se presentan significa que una talla única para todos enfoque de la política y/o la regulación es poco probable que funcione.

Por otro lado, en relación al tratamiento normativo de los datos por parte de los wearables podemos señalar que acorde a legislación peruana en materia de Protección de Datos Personales -Ley N° 29733[6]- se establece en el artículo 13.1 que éste solo puede darse mediante consentimiento previo, informado, expreso e inequívoco de su titular. Al tiempo que el principio de finalidad tipificado en el artículo 6° señala que los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita y que no debe extenderse a otra finalidad que no haya sido la establecida de manera inequívoca como tal al momento de su recopilación. La ley contempla también el principio de seguridad en su artículo 9° referida al titular del banco de datos personales que al ser encargado de su tratamiento debe adoptar las medidas técnicas organizativas y legales necesarias para garantizar la seguridad de los datos, las mismas que debe ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate.

Señala asimismo, el artículo 5° del Título preliminar que son datos sensibles aquellos datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual.

En este contexto, es importante además tener en cuenta que en muchos lugares los datos recopilados por los wearables también están sujetos a otras protecciones legales. Así, en los Estados Unidos esto incluye legislación específica del sector como COPPA, FCRA o ADA, así como leyes federales y estatales que rigen el seguro y la discriminación ilegal Future Privacy Forum (2014).

En muchos casos, la información de bienestar personal está cubierta por la Ley de Portabilidad y Responsabilidad del Seguro Médico (HIPAA), que impone ciertos requisitos de privacidad y seguridad a los proveedores de servicios de salud y sus asociados comerciales. Los dispositivos médicos que se pueden usar o transportar como un dispositivo wearable para el consumidor también están regulados para su seguridad por la FDA[7]. Cuando la información o las herramientas relacionadas con la salud quedan fuera de estas leyes, también pueden estar regidas por las leyes estatales y federales de protección al consumidor. Sin embargo, es innegable que muchos wearables recopilan datos cuya probabilidad de estar cubiertos por protecciones sectoriales específicas es casi inexistente. A veces, estos datos

[6] En concordancia con el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales DECRETO SUPREMO Nº 003-2013-JUS.

[7] Mientras que la FDA puede regular la seguridad y eficiencia de ciertos wearables de consumo, no asigna estándares de privacidad. Por esta razón, los dispositivos sujetos a las regulaciones de la FDA están pensados para ser cubiertos por las mejores prácticas de privacidad.

serán de poca sensibilidad y del tipo que algunos usuarios compartirán públicamente o con amigos. En otras ocasiones, los datos serán del tipo que puede revelar datos altamente confidenciales sobre los usuarios y es información que los usuarios esperarán que se trate de manera confidencial. Dependiendo del tipo de aplicación y los tipos de usos, los mismos datos pueden estar sujetos a expectativas muy diferentes del usuario. En muchos casos, las expectativas de los usuarios sobre el uso de datos por las nuevas aplicaciones y los nuevos servicios todavía están evolucionando a medida que se hacen evidentes nuevos beneficios y nuevos riesgos.

En Europa[8] y otras jurisdicciones, las leyes de privacidad nacionales también establecen las expectativas básicas de privacidad y seguridad. Si bien dichas leyes brindan el punto de partida para la protección de datos, a menudo también imponen estándares más altos sobre la información personal que se considera especialmente delicada, como los datos financieros o de salud. En algunos casos, es probable que los datos de bienestar generados por el consumidor caigan dentro de tales categorías protegidas.
El Supervisor Europeo de Protección de Datos, por ejemplo, ha observado que los datos de estilo de vida y bienestar serán, en general, considerados datos de salud -es decir datos sensibles- cuando se procesan en un contexto médico o donde la información sobre la salud de un individuo puede razonablemente inferirse de los datos (en sí mismos, o combinados con otra información) especialmente cuando el propósito del dispositivo es monitorear la salud o el bienestar del usuario ya sea en un contexto médico o de otro tipo. Cuando el estilo de vida o el bienestar los datos se consideren sensibles, se imponen restricciones adicionales al procesamiento de datos.

Sin embargo; como bien ha señalado el Grupo de Trabajo del Artículo 29 de la Comisión Europea[9] del otro lado del espectro existe una categoría de datos personales generados por aplicaciones y dispositivos que en general no deben considerarse como datos de salud (datos sensibles). También existen algunas aplicaciones y dispositivos en los cuales no es obvio a primera vista si el procesamiento de estos datos debiera o no debiera de calificar como procesamiento de datos de salud.

Si bien -en términos generales- las leyes existentes en materia de protección son bastante explícitas y tendientes a brindar la mejor tutela jurídica a nuestros datos personales, debemos reconocer que la tecnológica parece haber sobrepasado a los sistemas legislativos existentes.

En este sentido y en esencia, una autorregulación devendría en un factor fundamental ya que implicaría que las organizaciones sean buenos administradores de la información que reúnen y usan ya que el usuario está confiando sus datos personales a una compañía a cambio de un servicio, aunque muchas veces la mayoría de consumidores no sean plenamente conscientes de esta realidad.

---

[8] La Directiva 2002/58/ce del parlamento europeo y del consejo de 12 de julio de 2002 relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) y el Reglamento General de Protección de datos 2016/679. Diario Oficial de la Unión Europea. 27 de abril del 2016.
[9] European Comission (EC). *ARTICLE 29 data protection working party. 14/EN WP 223. Opinion 8/2014 on the on Recent Developments on the Internet of Things*. (Adoptado el 16 de septiembre del 2014)

Sin embargo también debe considerarse que un enfoque centrado en la seguridad y la privacidad por diseño no significa que esos sean los únicos valores y principios de diseño en los que los desarrolladores deben centrarse cuando innovan. El costo, la conveniencia, la elección y la usabilidad también son valores importantes. De hecho, muchos consumidores priorizarán esos valores sobre la privacidad y la seguridad, incluso cuando activistas, académicos y formuladores de políticas sugieran simultáneamente que se debe hacer más para abordar las cuestiones de privacidad y seguridad.

Adicionalmente, García (2015) plantea soluciones de empoderamiento a través de un sistema de encriptación o autenticación de los dispositivos, soluciones de derecho consuetudinario, estándares de responsabilidad en evolución y otros recursos legales; señala la importancia de la supervisión de un Organismo de Comercio a través de sus respectivas normativas y aplicación de normas sociales, presión y sanciones, remarcando que el poder de las normas sociales en este contexto podría convertirse en un determinante crucial de la popularidad de muchas tecnologías portátiles ya que a veces las normas culturales, la presión pública y las sanciones sociales espontáneas forman un "regulador" de las innovaciones mucho más poderoso y la forma en que las personas usan nuevas herramientas que las leyes y reglamentos.

Es innegable que de un lado el futuro se presenta prometedor en torno a los wearables y del otro presenta numerosas interrogantes sobre sus múltiples implicancias en diversas áreas del Derecho.

4. INTERNET DE LAS COSAS Y WEARABLE TECHNOLOGY

Los usuarios disfrutan de la personalización que ofrecen los wearables e Internet of Things (IoT), pero esas mismas capacidades que las hacen tan solicitadas por los usuarios son las que propician la aparición de diversas formas de vulneración que buscarán respuesta en el Derecho debido a que desafían las normas de privacidad tradicionales no sólo en el ámbito legal sino también en el entorno social.

En un intento por conceptualizar a IoT es oportuno hacer referencia al documento de la Comisión de la Unión Europea que la define como una infraestructura en la que miles de millones de sensores integrados en dispositivos cotidianos comunes -"cosas" como tales o “cosas” vinculadas a otros objetos o individuos- están diseñados para registrar, procesar, almacenar y transferir datos y como están asociados con identificadores únicos, pueden interactuar con otros dispositivos o sistemas usando las capacidades de la red[10]. El documento en mención además tiene como objetivo proporcionar una serie de recomendaciones a los distintos agentes que intervienen en el mercado del internet de las cosas con la finalidad de que respeten, desde el origen, el marco legal de protección de datos vigente en la Unión Europea.

[10] European Comission (EC). *ARTICLE 29 data protection working party. 14/EN WP 223. Opinion 8/2014 on the on Recent Developments on the Internet of Things*. (Adoptado el 16 de septiembre del 2014)

Debido a que IoT se basa en el principio del procesamiento extenso de datos a través de estos sensores que están diseñados para comunicarse de forma discreta e intercambiar datos de manera transparente, está estrechamente relacionada con las nociones de computación "omnipresente". En este sentido la nube juega un papel fundamental ya que no solo se ha vuelto omnipresente, sino que también se está tornando en indispensable debido a su accesibilidad desde cualquier lugar y en cualquier momento. Si bien los datos recopilados por los wearables se encuentran en "nubes dispersas" cuando se produzca una conectividad total se generará un impacto de proporciones no previstas por lo que la seguridad cobrará otro sentido y magnitud.

Adicionalmente los diseños de la moda tecnológica probablemente se presentarán mucho más estéticos y en consecuencia llamativos para tratar de "equilibrar" el aspecto de seguridad que llevará a un sector de usuarios a cuestionarse en torno a las ventajas reales y los riesgos implícitos al momento de adquirir un wearable; en tanto otro sector de consumidores continuará guiando su opciones de compra tan solo en base a un atractivo diseño que evidentemente ofrecerá muchas más funcionalidades y para quienes el factor seguridad con todo lo que lleva inmerso pasa a un segundo plano cuando de modernidad, comodidad, estilo y estatus se trata.

Thierer (2015) considera que la wearable technology es un subconjunto de IoT y dentro de este segmento el de más rápido crecimiento, vislumbrándose además su amplia influencia dentro de la sociedad en los próximos años.

En este sentido, Peppet (2014) señala que estos dispositivos prometen una importante eficiencia y beneficios sociales e individuales a través de la cuantificación y monitoreo de cualidades inmensurables. Pero al mismo tiempo precisa que IoT plantea una seria de difíciles cuestionamientos tales como: ¿A quién pertenece los datos generados por estos sensores? ¿Cuantos datos pueden usarse? ¿Son estos dispositivos y los datos que producen seguros? ¿Están los consumidores conscientes de las implicancias legales que tales datos crean?

En síntesis; señala que IoT propicia problemas en torno a la discriminación, privacidad, seguridad y consentimiento. A lo que suma el hecho de que actualmente las leyes en torno a estos temas -que tienen además fuertes implicancias en las normativas sobre los derechos del consumidor- en no pocos países devienen en insuficiente o no están preparadas para manejar las implicaciones legales de la interacción entre los wearables e IoT.

Una gran parte de los wearables no tienen ni teclado ni pantalla por lo que brindar información sobre privacidad y datos a los consumidores y la oportunidad de otorgar consentimiento es particularmente desafiante. Los productos actuales de IoT a menudo no notifican a los consumidores sobre cómo encontrar su política de privacidad relevante, y una vez que se encuentran, dichas políticas a menudo son confusas, incompletas y engañosas.

En esta línea de pensamiento, postula el autor cuatro primeros pasos desordenados e imperfectos para regular IoT:

- Ampliar las restricciones de uso existentes para amortiguar la discriminación;

- Redefinir la "información de identificación personal" para incluir datos biométricos y otras formas de datos de sensores;
- Proteger la seguridad mediante la expansión de leyes estatales de notificación de violación de datos para incluir violaciones de seguridad relacionadas con IoT;
- Mejorar el consentimiento del usuario brindándole una adecuada orientación sobre cómo deberían funcionar la notificación y la elección en el contexto del Internet de las cosas.

Cada paso mencionado considera los problemas técnicos y las formas en que las leyes existentes no están aún preparadas para abordarlos. Siendo así, la discriminación enfrentará el hecho que conjuntamente con Big Data las nuevas cantidades masivas de datos recogidos por los sensores de los dispositivos permitirán inferencias inesperadas sobre los consumidores permitiendo que terceros tomen decisiones económicamente importantes basadas en estas inferencias.

Dentro de este contexto; los reguladores, legisladores y académicos han asumido en gran medida el supuesto de que mientras las empresas proporcionen información precisa a los consumidores y éstos tengan la oportunidad de elegir o rechazar los servicios web de esas empresas, la mayoría de los problemas relacionados con los datos pueden autorregularse.

Desafortunadamente, estas suposiciones ya extendidas no se aplican de la misma forma en el contexto de los bienes de consumo integrante de IoT. Por el momento, sus fabricantes parecen preferir sólo proporcionar información privada y relacionada con datos en las políticas de privacidad de los sitios web.

En base a estas consideraciones Peppet (2014) señala que normalmente las políticas de privacidad se aplican únicamente al uso del sitio web y no al uso de sus productos lo que sugiere que las empresas asumen que los usuarios enfrentarán un segundo aviso de privacidad relacionado con el producto cuando activen la aplicación móvil para usar sus productos ya que encontrarán un acuerdo de licencia de software en el que se hará de su conocimiento los términos en los cuales la aplicación será usada y las políticas de privacidad, por lo que incluso un consumidor diligente que busca información privada sobre determinados productos y los datos de los wearables se encontrará en un círculo interminable de confusión. En consecuencia no existiría una notificación clara ni una opción sobre la información de privacidad

Refiere también que se pueden encontrar diversas políticas en torno al tema en cuestión, algunas parecieran aplicarse tanto al uso del sitio web como al uso del wearable. Otras políticas limitan su aplicación tan sólo al uso del sitio web y no al uso del wearable; pero no proporcionan medios para localizar una política de privacidad relacionada con el dispositivo. Cualquiera sea el caso esta situación dejaría sin respuesta a la pregunta sobre si alguna política relacionada con la privacidad se aplica a los datos generados por estos wearables.

En otras palabras, las diversas políticas actuales de privacidad están creando conflictos entre su definición de “información personal” e “información no personal”. La discusión sobre esta definición es importante ya que la mayoría de éstas les permiten a los fabricantes compartir o vender información no personal mucho más ampliamente que la información personal.

En resumen, estas políticas de privacidad de IoT a menudo son bastante confusas acerca de si los datos recopilados de los wearables cuentan como "información personal" y en consecuencia, resultan ambiguas en cuanto a qué derechos y obligaciones se aplican a dichos datos; al tiempo que, muchas de ellas tampoco abordan algunos puntos importantes para los consumidores como serían el no mencionar la propiedad de los datos del wearable o a menudo no especificar exactamente qué clase de datos recopila o qué tipos de sensores utiliza. Siendo igualmente inconsistentes en los derechos de acceso, modificación y eliminación que les dan a los consumidores y finalmente ninguna de estas políticas explica la cantidad de datos de los sensores que se procesan en el dispositivo en comparación con los que se transmiten y procesan remotamente en los servidores de las compañías.

Podría decirse que estas políticas parecen haber sido moldeadas por las necesidades y expectativas relevantes para la Internet normal y no IoT. No es de extrañar que en los albores de esta Internet no hubiera habido una consideración muy real sobre los problemas especiales vinculados a las políticas en torno a ésta, sin embargo ante su vertiginoso avance y evolución deviene en una necesidad ineludible.
Por otro lado La Ley N° 29571 -Código de Protección y Defensa del Consumidor- en nuestro país, y en muchos países aún no está preparada para afrontar los múltiples problemas que pueden derivarse del uso de los wearables.

La mayoría de los enfoques regulatorios en relación a la privacidad de la información sufren de la ilusión de que el consentimiento puede transparentar las prácticas de privacidad cuestionables. Solove (2013) ha llamado a esto el enfoque de "autogestión de privacidad" entendida como la creencia de que el proporcionar a los consumidores información y control suficientes les permite decidir por sí mismos cómo ponderar los costos y beneficios de la recopilación, uso o divulgación de su información. Sin embargo; sostiene el autor, que la autogestión de privacidad falla por una variedad de razones, entre ellas, que los consumidores no están informados, son abrumados cognitivamente y estructuralmente mal equipados para administrar la vasta información y la infinidad de decisiones que requiere la autogestión de la privacidad.

Los consumidores y los defensores de los consumidores deberían tener al menos alguna posibilidad de utilizar políticas de privacidad para evaluar las implicancias que encierran las opciones de productos. Reconocer las limitaciones de la notificación y elección del consumidor no justifica que las empresas puedan confundir a los consumidores con políticas de privacidad deficientes. Por otro lado y contradictoriamente las políticas de privacidad son una de las pocas herramientas regulatorias actualmente disponibles.
En este contexto, la orientación normativa deberá basarse en la protección de las expectativas del consumidor.

CONCLUSIONES

Si bien las consideraciones mencionadas a lo largo del presente artículo están centradas en algunos tópicos vinculados a la funcionalidad de la wearable technology y los riesgos implícitos en su uso, debe tenerse presente que el diseño y funcionalidad que acompaña a los wearables desempeña un rol fundamental en la elección de los consumidores y por lógica consecuencia en su creciente acogida y crecimiento dentro del mercado tecnológico; de ahí

que una adecuada regulación en materia de propiedad intelectual devenga en un tema trascendente ya que debido a la relación necesidad-dependencia que ha establecido con el usuario se perfila como una tecnología indispensable para el desarrollo de las actividades cotidianas más simples además de denotar cierto estatus social dentro del entorno.

Por otro lado, el factor privacidad en relación a los wearables tal como ha sido discutido presentan cierto nivel de subestima en comparación a su real magnitud, no sólo por parte de los usuarios sino también del lado de las empresas, situaciones ambas que incrementa las razones que sustentan la necesidad de un profundo análisis en torno al presente y futuro de la ubiquidad de nuestra información personal; calidad y cantidad de datos; pertinencia de los mismos, tratamiento y comercialización posteriores -entre otros- en vinculante e indesligable relación al tiempo real o no con los wearables, Big data, nube e Iot.

RERERENCIAS

ALSADOON, Abeer., COSTADOPOULOS, Néctar., PRASAD, P. y SEGURA, Haide. Ethical Implications of User Perceptions of Wearable Devices. *Science and Engineering Ethics*, 2018, vol. 24 n° 1, p. 1-28.

Bussiness Insider Intelligence. The Wearables Report: Growth trends consumer attitudes, and why smartwatches will dominate [En línea], 2015. [Consulta: 18-3-2018]. Disponible en: http://www.businessinsider.com/the-wearable-computing-market-report-2014-10

CHÁVEZ, Ana. Between the Profiles Pay Per View and the Protection of Personal Data: the Product is You. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal Regular [En línea], 2017, Vol. 6, n° 1. [Consulta: 30-4-2018]. Disponible en: https://gredos.usal.es/jspui/bitstream/10366/133637/1/Between_the_Profiles_Pay_Per_View_and_th.pdf

ÇIÇEK, Mesut. Wearable technologies and its future applications. International Journal of Electrical, Electronics and Data Communication [En línea], 2015, Vol. 3, n°4. [Consulta: 10-3-2018]. Disponible en: https://www.researchgate.net/publication/275580004_WEARABLE_TECHNOLOGIES_AND_ITS_FUTURE_APPLICATIONS

Cognizant. Wearable Devices: The Next Big Thing in CRM [En línea], 2014. [Consulta: 11-4-2018]. Disponible en: https://www.cognizant.com/InsightsWhitepapers/wearable-devices-the-next-big-thing-in-crm-codex984.pdf

Comisión Europea. Opinion 8/2014 on the on Recent Developments on the Internet of Things. Diario Oficial de la Unión Europea [En línea], 2014. [Consulta: 15-3-2018]. Disponible en: http://www.pdpjournals.com/docs/88440.pdf

Decreto Legislativo N° 822. Diario oficial El Peruano, Lima, Perú, 23 de abril de 1996.

Future of Privacy Forum. FPF list of Federal Anti-Discrimination laws [En línea], 2014. [Consulta: 28-4-2018]. Disponible en: https://fpf.org/2014/05/21/fpf-list-federal-anti-discrimination-laws/

GARCÍA, Lourdes. Wearables: qué son, cómo funcionan y que peligros entrañan para nuestra privacidad [En línea], 2015. [Consulta: 29-3-2018]. Disponible en: http://centrodeestudiosdeconsumo.com/images/PROTECCION_DE_DATOS/Wearables-qu%C3%A9-son-c%C3%B3mo-funcionan-y-que-peligros-entra%C3%B1an.pdf

HU, Jian Feng. ¿Wearable Device: Bless or Curse? *Applied Mechanics and Materials*, Vol. 727, p. 517-520.

LANGLEY, Matthew. Hide your health: addressing the new privacy problem of consumer wearables. The Georgetown Law Journal Online [En línea], 2014, Vol. 103. [Consulta: 9-4-2018]. Disponible en: https://georgetownlawjournal.org/articles/36/hide-your-health-addressing/pdf

Ley N° 29733. Diario oficial El Peruano, Lima, Perú, 3 de julio de 2011.

LUQUE, Javier. Dispositivos y tecnologías wearables [En línea], 2016. [Consulta: 10-4-2018]. Disponible en: http://www.acta.es/medios/articulos/ciencias_y_tecnologia/041001.pdf

Mind Commerce Staff. Adoption Factors for Wearable Technology Across Industry Verticals [En línea], 2014. [Consulta: 8-3-2018]. Disponible en:https://blog.marketresearch.com/adoption-factors-for-wearable-technology-across-industry-verticals

PEPPET, Scott. Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent. Colorado Law Scholarly Commons [En línea], 2014, Vol. 93. [Consulta: 10-3-2018]. Disponible en: http://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=1086&context=articles

POPAT, Kalpesh. y SHARMA, Priyanka. Wearable Computer Applications A Future Perspective. *International Journal of Engineering and Innovative Technology*, 2013, Vol. 3, n° 1, p. 213-217.

Reglamento General de protección de datos reglamento (UE) 2016/679 del Parlamento europeo y del consejo de 27 de abril de 2016. Disponible en: http://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/RGPD-2016R0679_Articulado-es-eu.pdf

RODRÍGUEZ, Nelesi. El fenómeno del Yo Cuantificado: ¿una nueva tecnología del Yo? Comunicación: Estudios venezolanos de la comunicación [En línea], 2015, Vol. 40. [Consulta: 9-4-2018]. Disponible en: http://www.gumilla.org/biblioteca/bases/biblo/texto/COM2015171-172_37-41.pdf

SALAS, Brenda. La industria de la moda a la luz de la propiedad intelectual. La Propiedad Inmaterial [En línea], 2013, Vol. 17. [Consulta: 28-4-2018]. Disponible en: http://revistas.uexternado.edu.co/index.php/propin/article/%20view/3583/3800

SOLOVE, Daniel. La autogestión de la privacidad y el dilema del consentimiento. *Revista Chilena de Derecho y Tecnología*, 2013, Vol. 2, n° 2, p. 11-47.

THIERER, Adam. The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation. Richmond Journal of Law and Technology [En línea], 2015, Vol. 21, n° 2. [Consulta: 1-3-2018]. Disponible en: https://scholarship.richmond.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com.pe/&httpsredir=1&article=1409&context=jolt

"Plataformas digitales, nuevas tecnologías y grupos vulnerables. Nuevos delitos incorporados a la legislación uruguaya"

Por: ***Paula Victoria Saravia Di Luca***
Uruguay

I.- Introducción.

Las nuevas generaciones han nacido y crecen con las nuevas tecnologías como parte de su vida diaria. Por lo tanto, tienden a crear lazos de afinidad en ellas con personas conocidas y no conocidas. Esto puede dar inicio a que a través de las redes sociales y de las nuevas tecnologías se cometan delitos de diferente índole si no son bien utilizadas.

El trabajo que se expone a continuación trata sobre cómo las nuevas tecnologías, en especial las plataformas digitales han incidido en la vida y quehacer cotidiano de un grupo de la sociedad, sobre todo en niños y adolescentes y las repercusiones que su mal uso tienen. Además se hará hincapié en la nueva creación de delitos, que tienen a las nuevas tecnologías como medio para cometerlos. Es así que la legislación uruguaya ha creado recientemente los delitos de "Divulgación de imágenes o grabaciones con contenido íntimo" y el delito de "Grooming".

Consta esta labor de cuatro puntos bases, los cuales dos de ellos versan sobre que es unas red social y así introducirnos a parte de la idea de esta exposición, la evolución del uso la tecnología, luego se remitirá al comentario de casos reales ocurridos en el Uruguay y como ha desencadenado en la promulgación de normativa para estos hechos y por último luego de realizado el análisis de lo mencionado se llegará a las conclusiones.

II.- ¿Qué es una red social? Incidencias de la misma en la población.

La tecnología ha tenido una gran incidencia en nuestras vidas, sobre esto ya se ha dicho y escrito bastante, pero dentro de la tecnología, las redes sociales como parte de aquella, han incidido e inciden en nuestro día a día de igual forma.

Comenzar el día y abrir en el dispositivo que más a mano se tenga la red social que se utilice ya es algo de rutina. Dentro de esa rutina de contacto con los demás (tal vez para muchos el primer contacto del día con otras personas) a través de una red social es donde vamos a exponer varias cosas de nuestro diario vivir, desde un comentario de cómo estamos de ánimo, subir una foto de lo que estamos haciendo o comentar lo que otro integrante de esa comunidad virtual expuso.

Esto sin duda alguna, es la rutina que los niños y adolescente tienen. La mayoría de la población considerada niño y adolescente tiene uno o varios dispositivos tecnológicos de su propiedad o de fácil alcance y compartan a través de las diversas redes sociales o de las plataformas de mensajería instantánea lo que están haciendo en el mundo real, sea desde

sacar fotos con sus amigos, indicar a través de geolocalización que permite la red social decir donde se encuentran en el aquí y ahora y hasta comentar como están de ánimo en el día.

Primero vamos a realizar un análisis breve de que es una red social y luego seguiremos adentrando en como a través de las mismas las relaciones "ciber-personales" como las he llamado, se hacen cada vez más complejas si es que no se enseña a una buena utilización de la herramienta social cibernética.

Una red social es, siguiendo lo que indica la Real Academia Española: *"Plataforma digital de comunicación global que pone en contacto a gran número de usuarios."*[1] De la definición se pueden extraer varios conceptos, el primero es que es una "plataforma digital", lo cual implica que estamos dentro del ámbito de la informática o del mundo cibernético y no del mundo de las interrelaciones personales de modo presencial. El otro concepto es que es "de comunicación global" esto implica que a través de esa plataforma los usuarios pueden tener una comunicación conjunta, de ida y vuelta.

Por último "pone en contacto a gran número de usuarios", es decir, las rede sociales no van a tener un solo usuario, tienden a tener muchos, lo que hace que esta comunicación, que si bien muchas veces es de un usuario particular a otro, se puede ver por el resto de la comunidad dicha comunicación.

Y sobre este punto quiero poner énfasis, el tener un gran número de usuarios hace que la convivencia en la red social esté marcada por integrantes de distintas edades e intereses, a veces estos últimos pueden tener un buen fin y a veces no.

En Uruguay, podemos tener en cuenta algunas cifras del uso de las redes sociales que fueron extraídas de la encuesta WIP+UY 2013 realizada por el Grupo de Investigación sobre Uruguay, Sociedad e Internet (GIUSI) de la Universidad Católica del Uruguay[2].

Si bien esta encuesta toma como universo de trabajo a personas mayores de 15 años (en esta exposición se pretender ver la incidencia en personas menores de 18 años) nos permite ver cómo está situada la población ante el uso de la tecnología y las redes sociales.

Una de las conclusiones que arriba dicha encuesta es que el uso de internet es prácticamente universal entre los menores de 30 años, las otras dos que destaco para el caso concreto son: 3 de cada 4 internautas utilizó alguna vez una red social y 1 de cada 2 utiliza con frecuencia diaria una red social.

Esta encuesta data del año 2013 pero ayuda a tener una visualización primaria del uso de las redes sociales, por lo cual podemos ver la incidencia que tienen las redes sociales en la vida diaria y si vamos un poco más allá, saliendo del rango propuesto por la encuesta, como inciden en la vida de los jóvenes.

[1] Diccionario de la Real Academia Española http://dle.rae.es/?id=VXs6SD8
[2] https://ucu.edu.uy/difusiones/2015/pdf/Informe_WIP_Uruguay_Final.pdf

Para finalizar este capítulo podemos concluir que, las redes sociales son parte de la vida diaria de las personas, ya no se hace un uso esporádico de las mismas, ni con fines específicos, se utiliza de modo más que frecuente y a veces con ninguna intención específica (subir comentarios o postear fotos), simplemente el hecho de estar presente en la red.

III- Grupos vulnerables.

El otro punto de esta exposición son los llamados grupos vulnerables. En el caso de este trabajo, específicamente se hará mención a un grupo vulnerable, ya que se pueden considerar más de un factor para hablar de vulnerabilidad; en el caso concreto será la edad la que determine el concepto de vulnerabilidad.

Los niños y adolescentes tienden a tener un contacto mucho más fluido con y casi se podría decir un contacto mucho más amigable con la tecnología que otras franjas etarias de la sociedad. Esto se puede entender en que han nacido en una situación mundial donde la tecnología ha tenido un gran avance y es parte de la vida cotidiana el uso de la misma. Ya es casi imposible considerar las comunicaciones entre los individuos sin pensar que las mismas se hacen a través de un mensaje escrito en una plataforma de mensajería instantánea, mucho más, las comunicaciones que los niños y adolescentes tienen con sus pares.

Se ha dado que las comunicaciones interpersonales que llevan a cabo los niños y adolescentes se hacen más en un mundo cibernético que en el mundo real. Más arriba hablaba sobre lo que he llamado las relaciones "ciber-personales" las cuales se dan en un ámbito cibernético, sin tener contacto frente a frente con quien se habla.

Este tipo de contacto, sin tener clara referencia con quien se habla, puede resultar peligroso en determinados casos. Las redes sociales si bien tiene términos y condiciones en las cuales se indica cual es la edad para poder utilizar la misma, es muy fácil poder mentir sobre ello, ya que el control es muy difícil de hacerlo.

Por lo tanto, al poder mentir sobre las edades, pueden ocurrir dos situaciones, la primera es que una persona que no llega a tener la edad requerida para poder usar la red social la pueda utilizar de igual modo y la segunda situación es que al no haber un control de edad, las personas pueden mentir sobre la misma e ingresar a la red social con una edad que no es tal.

Si bien los niños y adolescentes tiene un sentido innato para el uso de las tecnologías y su movimiento dentro de las redes sociales, muchas veces, es mejor que la de los adultos, suele ocurrir, que por una cuestión de madurez típica de la edad, esa desenvoltura que tienen en el uso de la tecnología, quede opacado por situaciones de engaños de adultos hacia ellos.

IV.- La educación del uso de las tecnologías.

Educar en tecnología no es solo educar en el la creación de nuevas herramientas, si no también, en cómo hacer un buen uso de las tecnologías existentes.

En cuanto a las redes sociales podemos ver que muchas veces sucede que el mal uso, y en este caso, no es solo cuestión de la edad del usuario, hace que ocurran determinados hechos

que sean perjudiciales para el mismo, por lo tanto, saber que cada acto que se realice en una red social puede no llegar a tener consecuencias, pero tal vez si y las mismas quizás no sean positivas.

En Uruguay la educación en el uso de la tecnología es una materia pendiente tanto en el ámbito de la educación primaria como de la educación secundaria.

Si bien Uruguay es pionero en el uso de la tecnología en el aula, ya que cuenta con el Plan CEIBAL (lo que es la contraparte de One Laptop per Child) se ha impuesto el uso de la tecnología antes de educar en el uso de la misma.

Para saber más de la educación del uso de las tecnologías se realizó una pequeña serie de preguntas a dos personas que estuvieran en contacto con la educación y la tecnología al mismo tiempo y que se diferenciaran en que uno trabaja en el sector público y el otro en el privado.

Las preguntas fueron las siguientes: a) ¿Considera que por parte de organismos públicos o privados se brinda a niños y adolescentes la educación adecuada en el uso de las tecnologías? b) ¿Qué considera que es necesario realizar para evitar el mal uso de las tecnologías? c) ¿Son evitables los casos de Grooming?

Se ha recabado y transcripto de forma textual las opiniones del Sr. Juan Miguel MARTÍ OTTADO quien es el Director de la Dirección Sectorial de Información para la Gestión y Comunicación de la Administración Nacional de Educación Pública (ANEP-CODICEN) y desde el lado privado se recabó la opinión del Psicólogo y Magister en Educación Roberto Balaguer.

Ante la primera pregunta MARTÍ OTTADO respondió*:* "Hay que tener en cuenta que se educa no solamente desde la Educación formal, sino también por los medios que incluye además de los audiovisuales clásicos, lo que hoy recibimos desde las tecnologías de la información y la comunicación.

Sí, la educación es bastante adecuada sobre el uso de las tecnologías, pero es insuficiente en lo que tiene que ver con la protección de datos personales y sobre todo en el trastocamiento de los valores y la sustitución del significado de las palabras (nos hablan por ejemplo de democracia en referencia a la libertad de las empresas).

Esto se debe fundamentalmente a una suerte de colonización cultural en la que nos han impuesto que compartir nuestras vidas con el mundo entero es una forma de ser "populares". Esta colonización cultural se genera desde los centros de poder dominantes -nótese que no hablo de países- para encarar la actividad política o económica que convenga a esos centros de poder con el conocimiento que les da la información que surge de los datos del perfilado de los usuarios "populares".

A la vez esta información se usa y se usará para hacer la "ficha" de cada uno, con la que ya actualmente y en el futuro se va a definir si una persona puede tener o no un trabajo, acceder a estudiar o vivir en cierto lugar, para definir qué es lo que debe decir que va a hacer un cierto

candidato para lo que sea. La suma de nuestros datos quedará como una especie de "prontuario" de cada uno, el que podrá ser utilizado ahora o dentro de muchos años.

La forma correcta de enseñar el uso de las tecnologías debería ser con criterio social, lo que en definitiva redundará en el beneficio de la humanidad toda.

Si se lograran orientar las políticas en este sentido, habría que comenzar por sensibilizar a las autoridades que en la mayoría de los casos, y debido a que no pertenecen a generaciones con un acceso importante a la tecnología, no tienen una percepción suficiente del problema y por lo tanto no pueden visualizar los cambios que son necesarios para resolver un problema del que no son conscientes, además de que deben tener claro que la batalla es titánica".

En cuanto a la segunda pregunta MARTÍ OTTADO refirió lo siguiente: "Habría que definir "mal uso". La tecnología por definición es neutra. El clavado de un clavo con un martillo es bueno. Golpear a un semejante con un martillo es malo. En ambos casos se puede utilizar correctamente el martillo.

Si la pregunta está orientada al uso correcto de las tecnologías de la información y la comunicación, para saber utilizar el martillo, hay que capacitar a las personas y generarles las destrezas necesarias. Si además queremos que hagan un uso "bueno" de las mismas debemos difundir los valores que queremos se propaguen por toda la sociedad: libertad, igualdad social, solidaridad, fraternidad, etc. Las tecnologías de la información y la comunicación no deberían utilizarse para difundir valores individualistas que separan a los seres humanos dejándolos vulnerables (diría vulnerados) ante el sistema".

Por último si son evitables los casos de Grooming dijo: "El Grooming es una especie de efecto colateral, seguramente no deseado, que genera el uso de las redes sociales (y otros medios tecnológicos) de acuerdo a los valores que nos han impuesto desde los centros de poder.

En el contexto actual donde la mayoría de los adultos pueden ser víctimas de todo tipo de estafas o engaños realizados mediante tecnologías de la información y la comunicación es muy difícil pensar que esos mismos adultos como referentes de niños y adolescentes puedan ayudarles a evitar ser víctimas de Grooming.

Si encaráramos hoy en forma urgente campañas de difusión sobre el uso "bueno" (que no es sólo el buen uso) para adultos y niños posiblemente se puedan mitigar al menos en parte los casos de Grooming.

Descartando de plano las medidas fascistoides de prohibir el uso de las tecnologías de la información y la comunicación la única forma de evitar los casos de Grooming es con educación en valores "buenos". El cambio será social o no será".

El Psic. BALAGUER ante la pregunta de si por parte de los organismos públicos o privados se brinda educación adecuada en el uso de las tecnologías respondió: "No, creo que nos falta todavía mucho al respecto como para hablar de una verdadera educación en ese sentido. Se necesita un fuerte conocimiento de las conductas juveniles, un diagnostico situacional,

objetivos claros a alcanzar y elaboración de materiales adecuados, así como formas de medir los alcances y éxitos de esa educación"

Por su parte ante el cuestionamiento de que es necesario realizar para evitar el mal uso de las tecnologías indicó: "Educar a los jóvenes en la toma de decisiones en distintos contextos situacionales y emocionales ya que los mecanismos de control desde el mundo adulto hoy están llamados al fracaso dado el avance de lo móvil. Son los jóvenes los que deciden qué, cuándo y cómo hacen en el mundo digital. Hay que ayudarlos a autorregularse, a elegir y a utilizar los dispositivos como ampliaciones de la mente. Ponerlos al servicio de la mente y no poner la mente al servicio de los dispositivos.

Otra cuestión a considerar es tomar conciencia sobre la importancia del cuidado de la Identidad digital a presente, pero sobre todo a futuro para estas nuevas generaciones que comienzan a generar contenidos tempranamente, ya a partir de los 8, 9 años de edad".

Par finalizar, sobre la última pregunta BALAGUER indicó: "No, pero lo que se puede evitar es que los niños o niñas caigan en la trampa que plantea el Grooming, que estén alertas al respecto. Se puede ayudarlos a que conozcan los mecanismos a través de los cuales los abusadores se manejan con los jóvenes, sus trucos y artimañas. El problema central es la vulnerabilidad emocional que aprovechan estos sujetos para manipular a los pequeños. Chicos emocionalmente fuertes saben poner límites a los otros y a ellos mismos y ese es el obstáculo principal que le podemos poner por delante al Grooming".

De estas dos visiones, se llegó a las siguientes conclusiones: - Hace más falta de educación en el uso de las tecnologías ya que la que hay es insuficiente y no está logrando los objetivos necesarios. - Es necesario para tener una correcta y adecuada educación en el uso de tecnologías que no solo se realice la capacitación a los adultos referentes, sean estos padres, familiares, educadores, etc. si no también capacitar a los niños y adolescentes. Se tiene que llegar a generar una conciencia por parte de adultos responsables y de los niños y adolescentes del contenido digital que se deja cuando se utiliza la tecnología en especial las redes sociales. – Luego de generada la conciencia de realizar un buen uso de la tecnología, se puede llegar a minimizar y en tal caso evitar los casos de Grooming pero no erradicarlos.

V.- Casos en Uruguay.

Dado el avance del uso de las redes sociales por parte de los niños y adolescentes, se han dado casos donde mayores con malas intenciones, han provocados casos de Grooming y otros delitos como la difusión de material pornográfico.
Se hará un recuento de casos para ver la incidencia de estos temas en la sociedad y en la jurisprudencia uruguaya pero primero se dará la definición de Grooming la cual se puede decir que es *"la acción encaminada a establecer una relación y control emocional sobre un niño/a, cuya finalidad última es la de abusar sexualmente del/la menor"*[3].

[3] XXXII Jornadas de Estudio de la Abogacía. El nuevo Código Penal. Ministerio de Justicia-Gobierno de España pág 365

El primer caso versa sobre un delito de difusión de material pornográfico a través del servicio de mensajería instantánea WhatsApp y páginas web. Se trata de la sentencia del Juzgado Letrado de Primera Instancia en lo Penal de 19º Turno Nº 52 de 11 de Noviembre de 2015.[4] La situación comienza con la denuncia del padre de una menor de 15 años donde indica que durante el año 2014 mantuvo una relación sentimental con el adulto denunciado y este último filmó a la víctima manteniendo relaciones sexuales con él. El denunciado hace circular el video a dos amigos suyos por WhatsApp y además la joven víctima se entera de que la filmación también circulaba por páginas pornográfica de internet. Luego de recabada la prueba, oído el Ministerio Público Fiscal y a la defensa del denunciado, la justicia entiende que en ese entonces, el procesado, incurrió en el delito del artículo 2 de la ley 17.815 que refiere a "Comercio y difusión de material pornográfico en que aparezca la imagen u otra forma de representación de personas menores de edad o personas incapaces" condenándolo a la pena de trece meses de prisión.

En esta sentencia se aplicó la ley 17.815 que es la ley sobre "Violencia sexual comercial o no comercial cometida contra niños, adolescentes o incapaces".

Por otra parte tenemos la sentencia del Tribunal de Apelaciones en lo Penal de 2º Turno Nº 103 de 27 de Abril de 2016.[5] La sentencia del Tribunal confirma la sentencia interlocutoria del Tribunal *ad quem* el cual dispone la prisión preventiva para quien fuera denunciado por el padre de una menor de 12 años donde aquel mediante un perfil falso de Facebook contacta a la víctima y la convence de que le enviara fotos desnuda. Surge de la sentencia los siguientes dichos del procesado *"Chateamos por varios meses a través de Facebook hace varios meses atrás el año pasado…le solicité que me enviara fotos suyas y luego eróticas donde se la viera desnuda, a sabiendas que era menor de edad…" "Le dije que las iba a repartir si no me mandaba más fotos de ella…yo le mandé a los amigos…todos menores"*. El Tribunal confirma la sentencia donde se decretó el procesamiento y prisión bajo la imputación *prima facie* de un delito de difusión de material pornográfico en que aparece imagen de persona menor de edad.

La siguiente sentencia es del Tribunal Penal Especializado en Crimen Organizado de 1º Turno Nº 11 de 14 de Octubre de 2016 donde se condena por dos delitos de retribución o promesa de retribución a personas menores de edad para que ejecuten actos sexuales o eróticos y un delito de fabricación y producción de material pornográfico, siendo Facebook el medio utilizado para contactar con las víctimas.[6] Este caso no solo tiene como víctimas a adolescentes menores de edad sino también a mujeres mayores. En cuanto a la cuestión que nos interesa en este trabajo, referiré al caso de la menor de edad que es víctima. El condenado al delito que se indicó más arriba creaba perfiles falsos de Facebook donde se hacía pasar por una modelo famosa, otro perfil donde se hacía pasar por una gerente de una revista, otro perfil falso donde era fotógrafo y otros dos perfiles falsos donde indicaba ser un organizador

[4] Jurisprudencia Uruguaya en Derecho Informático. Revista CADE Febrero 2017 pág 73.
[5] Derecho Informático. Jurisprudencia 2016 & 2017 & Jurisprudencia Comentada. Revista CADE Marzo 2018 pág. 35.
[6] Derecho Informático. Jurisprudencia 2016 & 2017 & Jurisprudencia Comentada. Revista CADE Marzo 2018 pág. 51.

de concursos y modelo exitosa, también utilizó una falsa empresa de modelos y es que así engañó a las víctimas con la finalidad de mantener con ellas relaciones sexuales.
Por último, en este breve pasaje de jurisprudencia actual, referiré a la Sentencia del Juzgado Letrado de Primera Instancia en lo Penal de 2º Turno Nº 139 de 27 de Octubre de 2016.[7] El autor fue procesado con prisión por un delito de atentado violento al pudor en reiteración real con un delito continuado de fabricación de material pornográfico con menores de edad. El autor se contactaba a través de Facebook como representante de modelos con las víctimas mujeres menores. Concretaba citas y en las mismas les tomaba fotografías con contenido sexual y las tocaba sin su consentimiento.

Luego de exponer estos casos jurisprudenciales, no quiero dejar de mencionar un caso que fue el puntapié inicial para la nueva normativa sobre Grooming en el Uruguay, el cual fue denominado "Caso Brissa". El 20 de Noviembre de 2017, Brissa González de 12 años pierde el ómnibus para ir a la escuela, decide ir caminando pero nunca llega a la misma. Ante la desaparición de la niña, el Fiscal del caso pide se pericie el teléfono celular y la computadora XO propiedad de Brissa. De las pericias a la XO se arroja que a través de la app Anime Amino, Brissa estaba en contacto con alguien que decía tener 13 años. Seguidas las actuaciones en la investigación se da con un video de una cámara de seguridad donde se ve un coche pasando por donde caminaba la niña rumbo a la escuela. Seguida la investigación, dos días después de la desaparición la niña es encontrada muerta. Se da con el sospechoso y posteriormente procesado, donde se confirma que antes de tener el encuentro con Brissa, él ya había contactado con la niña haciéndose pasar por un adolescente de 13 años en Anime Amino.

Este caso dejó consternada a la sociedad uruguaya y posteriormente a esto, el Parlamento Nacional sanciona la ley 19.580 donde se crea en el artículo 94 el delito de Grooming, dejando así sentada la creación de un nuevo delito que es incorporado al Código Penal uruguayo. Como se verá en el capítulo siguiente, esta ley venía en estudio desde principios del año 2016.

VI.- Nueva legislación uruguaya.

En Uruguay no se contaba con una normativa específica sobre Grooming hasta el 22 de diciembre de 2017 donde se promulgó la Ley Nº 19.580 titulada "Violencia hacia las mujeres, basada en género". Si bien fue promulgada a fines del año 2017, el proyecto de ley se presentó ante la Asamblea General del Parlamento Nacional en el mes de abril de 2016.

La Ley Nº 19.580 contiene noventa y ocho artículos y como indica la presentación del proyecto por parte del Poder Ejecutivo al Parlamento Nacional *"el Proyecto de Ley, (...) tiene como objetivo garantizar a las mujeres una vida libre de Violencia Basada en Género"*[8]. Esta ley como se aprecia tiene un amplio contenido sobre la temática violencia de género, es más, es la normativa que crea el Femicidio en Uruguay. Para el caso de estudio

[7] Derecho Informático. Jurisprudencia 2016 & 2017 & Jurisprudencia Comentada. Revista CADE Marzo 2018 pig 111.
[8] https://parlamento.gub.uy/documentosyleyes/ficha-asunto/129185

se remitirá a lo que en la exposición de motivos del Proyecto de Ley el Poder Ejecutivo establece en cuanto a la creación de Normas Penales en especial *"la incorporación de dos tipo penales directamente vinculados a las nuevas tecnologías de comunicación: la divulgación de imágenes de contenido íntimo (art. 97 y 98) y el embaucamiento de personas menores de edad con fines sexuales por medios tecnológicos (Grooming, art. 99)"*[9]

Esta ley ingresa al marco normativo nacional el nuevo delito de Grooming. Si bien no se lo nombra de ese modo, el nuevo artículo 277 bis del Código Penal, creado por el artículo 94 de la ley Nº 19.580, hace referencia a este tipo de delito.
La nueva normativa, además del delito antes mencionado, crea el delito de "Divulgación de imágenes o grabaciones con contenido íntimo" el cual se encuentra en el artículo 92 de la ley Nº 19.580 y en el artículo 93 se encuentran las agravantes del mismo.

El delito de divulgación de imágenes o grabaciones con contenido íntimo hace referencia a "El que difunda, revele, exhiba o ceda a terceros imágenes o grabaciones de una persona con contenido íntimo o sexual, sin su autorización, será castigado con una pena de seis meses de prisión a dos años de penitenciaría.

En ningún caso se considerará válida la autorización otorgada por una persona menor de dieciocho años de edad. Este delito se configura aun cuando el que difunda las imágenes o grabaciones haya participado en ellas.

Los administradores de sitios de internet, portales, buscadores o similares que, notificados de la falta de autorización, no den de baja las imágenes de manera inmediata, serán sancionados con la misma pena prevista en este artículo".

Del estudio de este delito podemos ver que la comisión del mismo se puede hacer por cuatro acciones, es decir, el delito está integrado por cuatro verbos nucleares que pueden ser ejecutados de forma indistinta, ellos son: -difundir, -revelar. -exhibir y –ceder. Lo que se castiga es que mediante la ejecución de esos verbos nucleares, se haga circular imágenes o grabaciones de contenido íntimo o sexual a terceros. Lo importante al caso en estudio es que nunca es válida la autorización de un menor de edad que permita se divulguen, revelen, exhiban o cedan sus imágenes de contenido íntimo o sexual.

El artículo 92 de la ley Nº 19.580 tiene como base, si se los lee solo hay un par de diferencias, en el artículo 197 inciso 7 del Código Penal Español vigente desde julio de 2015.

Ahora bien, el artículo 94 de la Ley Nº 19.580 reza "ARTÍCULO 277 bis.- El que, mediante la utilización de tecnologías, de internet, de cualquier sistema informático o cualquier medio de comunicación o tecnología de trasmisión de datos, contactare a una persona menor de edad o ejerza influencia sobre el mismo, con el propósito de cometer cualquier delito contra su integridad sexual, actos con connotaciones sexuales, obtener material pornográfico u obligarlo a hacer o no hacer algo en contra de su voluntad será castigado con de seis meses de prisión a cuatro años de penitenciaría".

[9] https://parlamento.gub.uy/documentosyleyes/ficha-asunto/129185

Este artículo se incorpora al cuerpo del Código Penal al capítulo IV "De la violencia carnal, corrupción de menores, ultraje público al pudor". El delito no tiene *nomen iuris* ya que está dentro del artículo 277 que se denomina "Ultraje público al pudo" pero más allá de eso, es el delito que hace referencia al Grooming.

El artículo de la ley tuvo cambios en cuanto al original que se planteaba en el proyecto de ley y uno de ellos fue que en el proyecto se hacía referencia a que el sujeto pasivo tendría que ser un menor de 15 años, mientras que en la ley promulgada se hace referencia a persona menor de edad quedando así el guarismo de edad del sujeto pasivo más amplio. También fueron modificados los guarismos de las penas donde en el proyecto de ley se indicaba de seis meses de prisión a dos años de penitenciaría, quedando sancionado en la ley la pena de seis meses de prisión a cuatro años de penitenciaría.

Ocurre que Uruguay ya cuenta con la Ley Nº 17.815 "Violencia sexual comercial o no comercial cometida contra niños, adolescentes o incapaces" lo cual resulta que en la parte en que se hace referencia a la obtención de material pornográfico se podría llegar a tener problema de aplicación normativa.
Más allá de esto, lo que hay que tener en cuenta es que Uruguay tiene en su sistema normativo dos delitos que tienen como base de creación el uso de las nuevas tecnologías y en uno de ellos, el sujeto pasivo son menores de edad.

VII.- Conclusiones

Como es estudiado, la normativa nace luego de que los hechos han ocurrido y en el caso que se expone en este trabajo, se puede llegar a concluir que los hechos se pueden evitar educando en el buen uso de las tecnologías.

Se tiene que partir de la base que la enseñanza es la clave de la prevención, teniendo buenas políticas educativas en el uso de las tecnologías podemos llegar a prevenir, tal vez no eliminar, los casos de Grooming por ejemplo y de difusión de imágenes de contenido sexual o pornográfico.

Con la normativa lo que se pretende es castigar las malas conductas, quizás prevenirlas, pero la verdadera prevención es la educación temprana.

BIBLIOGRAFÍA

Diccionario de la Real Academia Española http://dle.rae.es/?id=VXs6SD8

Encuesta WIP+UY 2013 Grupo de Investigación sobre Uruguay, Sociedad e Internet (GIUSI) de la Universidad Católica del Uruguay https://ucu.edu.uy/difusiones/2015/pdf/Informe_WIP_Uruguay_Final.pdf

XXXII Jornadas de Estudio de la Abogacía. El nuevo Código Penal. Ministerio de Justicia-Gobierno de España.

Jurisprudencia Uruguaya en Derecho Informático. Revista CADE, Uruguay, Febrero 2017

Derecho Informático. Jurisprudencia 2016 & 2017 & Jurisprudencia Comentada. Revista CADE, Uruguay, Marzo 2018

Parlamento del Uruguay https://parlamento.gub.uy/documentosyleyes/ficha-asunto/129185

VIEGA RODRÍGUEZ, María José y HERNÁNDEZ VARELA, María Jimena "Derecho Informático e Informática Jurídica II", Editorial Fundación de Cultura Universitaria, Montevideo, Uruguay, 2018.

POLÍTICA 2.0: LA REGULACIÓN JURÍDICA DE LAS CAMPAÑAS ELECTORALES EN LAS REDES SOCIALES EN COLOMBIA.

Por: ***Paola Consuelo Ramos Martínez***
Laura Sofía Andrade Suaza
Waldir David Rentería Sánchez
Colombia

INTRODUCCIÓN

Con el avance de la tecnología la sociedad ha venido sufriendo grandes cambios. Uno de ellos ha sido la nueva forma de hacer campañas electorales. Las plataformas digitales se han convertido en un potente escaparate para los actores políticos con cargos públicos de elección popular o con intenciones de serlo. En el caso de las redes sociales, estas resultan ser un punto clave para el aseguramiento de simpatizantes.

En Colombia, las autoridades en materia electoral como el Consejo Nacional Electoral y la Registraduría Nacional del Estado Civil no han logrado armonizar la normatividad aplicable frente al uso de las redes sociales en épocas previas y durante las contiendas electorales, existiendo un vacío normativo que solamente a través de interpretaciones analógicas, poco concretas, se han intentado pronunciar sobre la problemática que se genera.

En ese orden de ideas, se ha hecho necesario exigir a las autoridades correspondientes un pronunciamiento específico que pueda dar solución al abuso de las redes sociales, sin embargo, existe la contradicción de caer en una posible censura vulnerando así el derecho a la libertad de expresión constitucionalmente reconocido. Por ende, es pertinente identificar la normatividad aplicable frente al uso de las redes sociales en épocas previas y durante las contiendas electorales y la afectación de la libertad de expresión como problemática en la limitación de estas campañas políticas en las redes sociales.

PLANTEAMIENTO DEL PROBLEMA

¿Cuál es el tratamiento jurídico aplicable al uso de las redes sociales en épocas electorales en Colombia?

I. REDES SOCIALES

La influencia de las redes sociales es cada día más fuerte, ya que pasó de ser una herramienta que en un inicio fue creada para comunicarnos con mayor facilidad, a ser una plataforma en la cual se comparten distintos aspectos de los usuarios siendo también utilizada para expresarse de manera libre en los temas que son de su interés. Son un entorno digital que nos invade, y que han logrado incidir en gran medida en la realidad social, política y económica de los países. La necesidad de analizar la regulación jurídica de las redes sociales en

Colombia, en el contexto de las campañas electorales, surgió por la falta de vigilancia y control de estas plataformas. Es decir, no existe ninguna limitación a la actividad que realizan los candidatos o partidos políticos en dichos entornos.

Actualmente en Colombia la Resolución 3066 de 2011 de la Comisión de Regulación de Comunicaciones (CRC) define la red social como:

> ***"Red social**: Aplicación Web dirigida a comunidades de usuarios en las que se les permite intercambiar fotos, archivos, aplicaciones, mensajes cortos de texto –SMS– y otro tipo de contenidos en línea y en tiempo real."*

A partir de esta revolución en la forma de comunicar, es claro que se encuentra la necesidad de regular este tipo de plataformas pues sus usuarios depositan en ella datos personales que son de especial protección. En ese sentido, la Ley Estatutaria 1581 de 2012 fue creada con el fin de brindar la debida protección de los datos personales. La realidad, en materia de legislación colombiana frente a las redes sociales, es que no se ha desarrollado una completa y clara regulación del uso que se le da a las redes sociales, el contenido que se comparte y el contenido que se crea sin afectar claramente la libertad de expresión.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) se pronunció mediante el Concepto Jurídico N° 54042010 expresando que:

> *"En Colombia no existen normas o regulaciones sobre la materia. Con la web 2.0 o redes sociales, los usuarios son consumidores y productores, por lo tanto, enfrentan la problemática de compartir contenidos sin consideración de la propiedad intelectual ni de leyes de copyright, por lo cual, corresponde a las redes sociales establecer una autorregulación."*

II. CAMPAÑA ELECTORAL

2.1. ¿Qué es Campaña Electoral?

De acuerdo al artículo 34 de la Ley 1475 de 2011, se define campaña electoral como:

> "*Para efectos de la financiación y de la rendición pública de cuentas, entiéndase por campaña electoral el conjunto de actividades realizadas con el propósito de convocar a los ciudadanos a votar en un determinado sentido o a abstenerse de hacerlo*".

2.2. Diferencia de conceptos: Campaña electoral, Propaganda electoral y Divulgación política.

Figura n°1: Diferencia conceptual

	CAMPAÑA ELECTORAL	PROPAGANDA ELECTORAL	DIVULGACIÓN POLÍTICA
CONCEPTO	Es el conjunto de actividades realizadas con el propósito de convocar a los ciudadanos a votar en un determinado sentido o a abstenerse de hacerlo.	Es la que realizan los partidos, los movimientos políticos y los candidatos a cargos de elección popular y las personas que los apoyen, con el fin de obtener apoyo electoral (Artículo 35 de la ley 1475 de 2011). También se constituye como una de las actividades principales de la campaña y cumple la función de promover masivamente los proyectos electorales sometidos a consideración de los ciudadanos o una determinada forma de participación en la votación de que se trate.	Es la que con carácter institucional realicen los partidos, movimientos, con el fin de difundir y promover los principios, programas y realizaciones de los partidos y movimientos, así como sus políticas frente a los diversos asuntos de interés nacional (Artículo 23 del Código Electoral y 23 de la Ley 130 de 1994).
TIEMPO	La recaudación de contribuciones y la realización de gastos de campaña podrá ser adelantada por los partidos, movimientos políticos y grupos significativos de ciudadanos, durante los seis (6) meses anteriores a la fecha de la votación. Los candidatos, por su parte, solo podrán hacerlo a partir de su inscripción.	Tiene un período de tiempo específico para su realización: - La propaganda a través de los medios de comunicación social únicamente podrá realizarse dentro de los sesenta (60) días anteriores a la fecha de la respectiva votación - La propaganda a través del espacio público, únicamente podrá realizarse dentro de los tres (3) meses anteriores a la fecha de las elecciones.	No implica la publicidad que busca apoyo electoral para los partidos o movimientos, razón por la cual se permite que la misma se pueda realizar en cualquier tiempo.

Fuente: Elaboración propia

La ley estatutaria por medio de la cual se adoptan reglas de organización y funcionamiento de los partidos y movimientos políticos, de los procesos electorales, Ley 1475 de 2011 (Congreso de la República de Colombia, s.f.), contiene un capítulo especialmente destinado para referirse a las campañas electorales y su reglamentación en materia de propaganda electoral.

La Ley hace una distinción entre la divulgación política y la propaganda electoral: la divulgación política es la que con carácter institucional realicen los partidos, movimientos, con el fin de difundir y promover los principios, programas y realizaciones de los partidos y movimientos, así como sus políticas frente a los diversos asuntos de interés nacional

(Artículo 23 del Código Electoral y 23 de la Ley 130 de 1994). Por su parte, la propaganda electoral es la que realizan los partidos, los movimientos políticos y los candidatos a cargos de elección popular y las personas que los apoyen, con el fin de obtener apoyo electoral (Artículo 35 de la ley 1475 de 2011). La ley colombiana establece que la divulgación política no implica la publicidad que busca apoyo electoral para los partidos o movimientos, razón por la cual se permite que la misma se pueda realizar en cualquier tiempo. Por su parte, la propaganda electoral tiene un período de tiempo específico para su realización: si es a través de los medios de comunicación social únicamente podrá realizarse dentro de los sesenta (60) días anteriores a la fecha de la respectiva votación; y si es a través del espacio público, únicamente podrá realizarse dentro de los tres (3) meses anteriores a la fecha de las elecciones.

Con base en lo anterior, la Ley ha encomendado a los partidos y movimientos políticos que en sus estatutos contengan cláusulas o disposiciones que desarrollen los principios señalados en la ley y especialmente los consagrados en el artículo 107 de la Constitución, en todo caso, que como mínimo contengan reglamentación sobre varios asuntos, entre los cuales encontramos: la utilización de los espacios institucionales en televisión y en los medios de comunicación para efectos de la divulgación política y la propaganda electoral (Artículo 4 numeral 16 de la Ley 1475 de 2011).

III. CAMPAÑAS ELECTORALES Y REDES SOCIALES

3.1. Antecedentes normativos colombianos

Figura n°2 Antecedentes normativos

AÑO	FECHA	NORMA	TEMA
1986	15 de julio	Decreto 2241	Por el cual se adopta el Código Electoral.
1994	23 de marzo	Ley Estatutaria 130	Por la cual se dicta el estatuto básico de los partidos y movimientos políticos, se dictan normas sobre su financiación y la de las campañas electorales y se dictan otras disposiciones
1994	02 de septiembre	Ley Estatutaria 163	Por la cual se expiden algunas disposiciones en materia electoral.
2011	18 de mayo	Resolución 3066 de la CRC	Por la cual se establece el Régimen Integral de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones.
2011	14 de julio	Ley 1475	Por la cual se adoptan reglas de organización y funcionamiento de los partidos y movimientos políticos, de los procesos electorales y se dictan otras disposiciones.

2016	10 de noviembre	Resolución 5050 de la CRC	Por la cual de compilan las Resoluciones de Carácter General vigentes expedidas por la Comisión de Regulación Comunicaciones.
2017	24 de febrero	Resolución 5111 de la CRC	Por la cual se establece el régimen de protección de los derechos de los usuarios de servicios de comunicaciones, se modifica el capítulo 1 del título II de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones.
2018	05 de marzo	Decreto 430	Por el cual se dictan normas para la conservación del orden público durante el período de elecciones al Congreso de la República del 11 de marzo de 2018 y se dictan otras disposiciones

Fuente: elaboración propia

3.2. Marco Normativo Vigente

La Constitución Política de Colombia consagra el derecho fundamental de todos los ciudadanos a fundar, organizar y desarrollar partidos y movimientos políticos, y la libertad de afiliarse a ellos o de retirarse (Artículo 107 CN). Derecho enmarcado en el deber de presentación y divulgación de sus programas políticos. Con base en lo anterior, la Constitución ha hecho referencia expresa a las campañas electorales relacionándolas con la financiación de las mismas, de manera específica, se ha manifestado que las campañas serán financiadas parcialmente por recursos estatales (Artículo 109 CN). A su vez, indica la Carta Política que, en materia de consultas populares, a éstas se les aplicarán las normas sobre financiación y publicidad de campañas y acceso a los medios de comunicación del Estado que rigen para las elecciones ordinarias. De igual manera, la Constitución se ocupa de las campañas electorales para la elección del Presidente, teniendo en cuenta la reforma constitucional que permitió su reelección, con la cual se elevó a rango constitucional la regulación de varias materias:

- Normas sobre acceso a espacios publicitarios y espacios institucionales de radio y televisión costeados por el Estado.
- Obligación de rendición de cuentas de los partidos, movimientos, grupos significativos de ciudadanos y candidatos sobre el volumen, origen y destino de sus ingresos.

Adicionalmente, la Constitución Política creó el órgano estatal encargado de ejercer la suprema inspección y vigilancia de la organización electoral: el Consejo Nacional Electoral, el cual de conformidad con el artículo 265 C.P., tiene como atribución especial: regular y controlar el cumplimiento de las normas en materia de propaganda electoral.

Teniendo claro lo que son las redes sociales podemos decir que a través de esta plataforma se interactúa sobre los distintos acontecimientos que suceden a nivel mundial en tiempo real, es decir que han llegado a distintas esferas sociales, en este caso las campañas que emprenden

los candidatos y los partidos políticos en tiempo de elecciones no son ajenas a este fenómeno, pues es normal que a medida que la sociedad avance y cambie la manera en la que se comunica e interactúa con otras personas todo lo que rodea a la sociedad evoluciona de la misma forma. Llegamos al punto donde es claro que las redes sociales en general no cuentan con regulación por parte del Estado colombiano entonces ¿qué sucede en relación con las campañas electorales? pues es sabido que en materia de campaña electoral y de propaganda electoral la legislación colombiana cuenta con regulación frente al tema.

La Ley estatutaria 163 de 1994 en el artículo 10 hace mención a la propaganda hecha en el día de las elecciones, sobre la cual expresa que queda prohibido todo tipo de propaganda que se haga en pro de votar por un candidato, de la misma manera la Ley 1475 de 2011 nos define el concepto de propaganda electoral en el artículo 35, como aquella que realicen los partidos, los movimientos políticos y los candidatos a cargos de elección popular y las personas que los apoyen, con fin de obtener apoyo electoral.

De igual forma la Ley 1475 de 2011 en el artículo 34 define a la campaña electoral como el conjunto de actividades realizadas con el propósito de convocar a los ciudadanos a votar en un determinado sentido o a abstenerse de hacerlo. Recientemente en el país se llevaron a cabo las elecciones al Congreso y a la Presidencia, en víspera de las elecciones para el Congreso se emitió el decreto 430 de 2018 con el fin de conservar el orden público. El decreto reguló el tema de propaganda electoral en el artículo 4 prohibiendo para las elecciones todo tipo de propaganda electoral incluyendo la móvil.

Teniendo en cuenta la regulación que en materia de campaña electoral y propaganda electoral abarca la legislación colombiana, es evidente que en ningún momento se hace mención a la que se hace por medio de redes sociales o portales web lo que deja abierta la brecha para que en el día de las elecciones por medio de estas herramientas, de cierta forma, no se cumpla con lo dispuesto en la mencionada normatividad respecto al tema de propaganda electoral.

Figura n°3 Marco normativo vigente

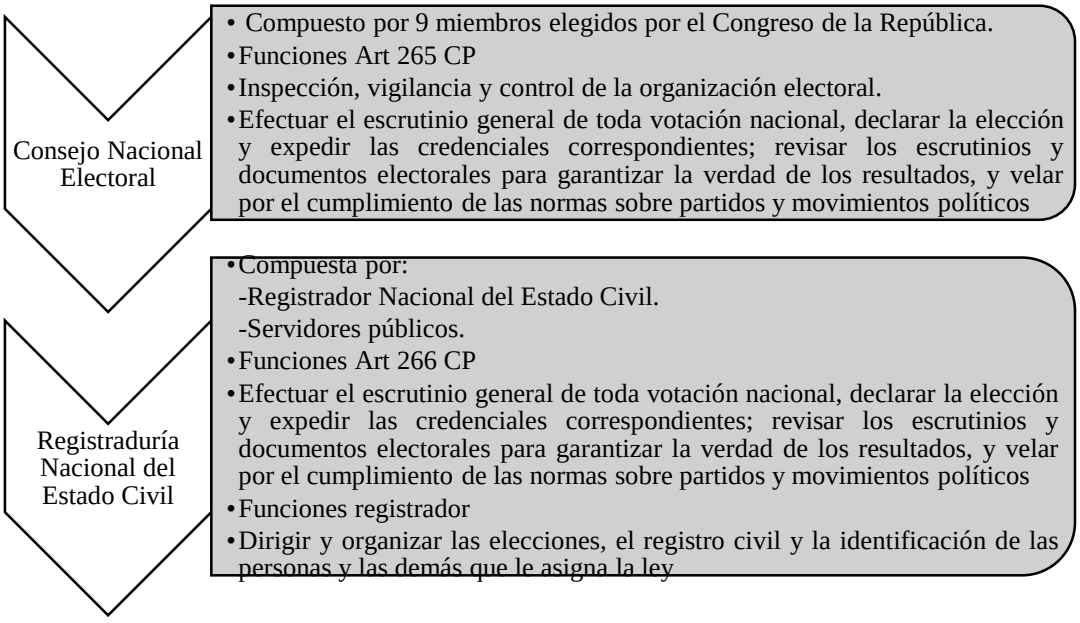
CONSTITUCIÓN	
ART. 107	Derecho fundamental de todos los ciudadanos a fundar, organizar y desarrollar partidos y movimientos políticos, y la libertad de afiliarse a ellos o de retirarse.
ART. 109	Las campañas serán financiadas parcialmente por recursos estatales.
ART. 265	El Consejo Nacional Electoral tiene como atribución especial: regular y controlar el cumplimiento de las normas en materia de propaganda electoral.
LEYES	
Ley Estatutaria 130 del 23 de marzo de 1994	Por la cual se dicta el estatuto básico de los partidos y movimientos políticos, se dictan normas sobre su financiación y la de las campañas electorales y se dictan otras disposiciones.
Ley Estatutaria 163 del 02 de septiembre de 1994	Por la cual se expiden algunas disposiciones en materia electoral.

Ley 1475 del 14 de julio de 2011	Por la cual se adoptan reglas de organización y funcionamiento de los partidos y movimientos políticos, de los procesos electorales y se dictan otras disposiciones.
DECRETOS	
Decreto 2241 del 15 de julio de 1986	Por el cual se adopta el Código Electoral.
Decreto 430 del 05 de marzo de 2018	Por el cual se dictan normas para la conservación del orden público durante el período de elecciones al Congreso de la República del 11 de marzo de 2018 y se dictan otras disposiciones.
RESOLUCIONES	
Resolución 5111 del 24 de febrero de 2017 de la Comisión de Regulación de Comunicaciones (CRC)	Por la cual se establece el régimen de protección de los derechos de los usuarios de servicios de comunicaciones, se modifica el capítulo 1 del título II de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones

Fuente: elaboración propia

3.2. Autoridades Encargadas En Materia Electoral En Colombia

Figura n°4 Autoridades electorales



Fuente: elaboración propia

En Colombia las autoridades encargadas de la organización electoral están conformadas, según lo expresa la Constitución Política en el artículo 120, por el Consejo Nacional Electoral (CNE) y la Registraduría Nacional del Estado Civil.

Las funciones de la Registraduría y del CNE son de tipo administrativo. Esto implica que, en términos generales, sus decisiones pueden ser controladas por los jueces (principalmente por el Consejo de Estado). La Registraduría se encarga de dirigir y organizar las elecciones, el registro civil y la identificación de las personas (CP, art. 266); el CNE, por su parte, regula, inspecciona, vigila y controla toda la actividad electoral de los partidos y movimientos políticos, de los grupos significativos de ciudadanos, de sus representantes legales, directivos y candidatos (según el Acto Legislativo 01 de 2009).

3.3. Propaganda electoral a través de medios digitales

No existe certeza absoluta sobre el tratamiento de este tipo de publicidad por parte de las leyes colombianas, teniendo en cuenta que no hay referencias expresas sobre su regulación en las leyes en materia de propaganda electoral, por lo cual su regulación se ha visto resuelta por el Consejo Nacional Electoral a través de la respuesta a consultas por parte de los ciudadanos sobre este tema.

En este sentido, el CNE ha manifestado que:

> "*la publicidad o propaganda electoral por internet goza de la misma finalidad y objetivo que la realizada por prensa escrita, pasacalles, radio y T.V. entre otros, lo que la hace diferente es el medio por el cual es difundido, el cual es el internet. Dentro del Internet – siendo este un universo interactivo- se puede realizar publicidad en términos generales a través de diferentes medios, tales como Portales interactivos, textos, link o enlaces, banner, web, weblog, blog, logos, anuncios, audio, video, animación, videojuegos, descargas, redes sociales y mensajería instantánea, entre otros*" (Resolución N° 4030, 2010)

De igual manera el Concepto – Radicado No. 5650 de 201135 se manifestó sobre la propaganda en medios digitales, indicando que: "toda forma de publicidad realizada con el fin de obtener el voto de los ciudadanos a favor de partidos o movimientos políticos, listas o candidatos a cargos o corporaciones públicas de elección, del voto en blanco, o de una opción en los mecanismos de participación ciudadana" deberá ser tenida como propaganda electoral. Un aspecto adicional a tener en cuenta es que debe entenderse por medios digitales de acuerdo a la terminología utilizada por la consultante, para lo cual entenderemos que se trata de una especie de medio de comunicación, es decir aquellos "órgano(s) destinado(s) a la información pública" o "Instrumento o forma de contenido por el cual se realiza el proceso comunicacional o comunicación", refiriéndose a los medios de comunicación masiva, encontrándose dentro de ellos los llamados medios digitales o "también llamados "nuevos medios" o "nuevas tecnologías". Habitualmente se accede a ellos a través de internet…", por lo que puede entenderse como los medios de comunicación masiva que se publican a través del internet. (Resolución No. 5650, 2011)

Concluyendo así el CNE en dicho Concepto que, dado que no existe un régimen legal especial a este respecto, la propaganda electoral en estos medios debe ceñirse a lo dispuesto en las normas generales. Los anteriores Conceptos nos indicarían que cualquier espacio de internet se enmarca en la definición de propaganda electoral que contiene la Ley, sin embargo, el Consejo Nacional Electoral ha dilucidado la distinción entre el uso de espacios en internet como páginas web del uso de las redes sociales, de la siguiente manera:

3.3.1. Sobre los portales web

Debemos manifestar que no ha sido unívoca la posición del CNE sobre si los portales web constituyen propaganda electoral o no, en primer lugar en Concepto – Radicado No. 0947 de 2007, el Consejo manifestó sobre la creación portales web que indican específicamente el nombre de un ciudadano aspirante a un cargo de elección popular, tal y como lo consultó el ciudadano en los siguientes términos: "¿De igual manera les solicito me informe si colocar en la red una página web constituye propaganda electoral aunque en ella sólo aparezca mi nombre: www.eduardozambrano.com?". El CNE respondió que: "toda actividad encaminada a obtener el apoyo electoral, constituye propaganda electoral, por lo cual no se requiere que explícitamente se indique el cargo o período al que se aspira, sino que el mensaje, incite al conglomerado a depositar su voto a favor del candidato que se promociona. Por consiguiente, si la página web de la hipótesis planteada se utiliza con fines de promoción de aspiraciones a cargos de elección popular, en búsqueda del apoyo popular constituye propaganda electoral" (Concepto N° 0947, 2007)

Así mismo, en el Concepto – Radicado No. 625 de 2007 con ponencia del magistrado Ciro Muñoz indicó: "la publicidad contenida en afiches, pasacalles, carteles, casas, volantes y por supuesto la publicidad contenida en páginas web, solamente podrán hacerse a partir del próximo 27 de julio de 2007, pues a partir de dicha fecha se contabiliza el plazo de los tres meses autorizados por la ley para realización de propaganda electoral en cualquiera de sus modalidades".

Sin embargo, en Concepto – Radicado No. 2843 de 201137 el CNE indicó que la información política sobre un determinado candidato a través de página web, no constituye propaganda electoral que pueda emitirse tres (3) meses antes de la fecha de elecciones, dado que, a juicio de dicho pronunciamiento, los mensajes que se emiten a través de este medio no estarían dirigidos a un público general e indeterminado. Lo cual permitió concluir que se encuentra autorizada por el CNE la realización de propaganda electoral a través de portales web. (Concepto N° 2843, 2011)

Lo anterior fue reiterado en Concepto - Radicado No. 6099 de 2011, con ponencia de la Magistrada Nora Tapia, al referirse a la propaganda electoral mediante el uso de las redes sociales y la web, se expuso lo siguiente: "(...) en el evento en que una persona tenga una página web, entendida ésta como el ofrecimiento de una interface simple y consistente en que brinda información en forma de páginas electrónicas, éstas solo funcionan siempre y cuando el usuario esté conectado a Internet, y utilice un navegador que le permita leer los documentos de hipertexto y buscar libremente la información o la página deseada y comenzar a navegar por las diferentes posibilidades que ofrece el sistema. Lo que se publique en esta página, no constituiría propaganda electoral, por cuanto sus mensajes no estarían dirigidos al público en general e indeterminado en el que no participa la voluntad de dicho público.

Por el contrario, para acceder a dicha página web y al contenido de la misma, debe mediar necesariamente la voluntad del interesado, quien, de no acceder voluntariamente a dicha interface, no estaría en condición de conocer su contenido.

Este Concepto indicó entonces que no se entendería propaganda electoral la realizada a través de páginas web, no obstante, señaló sobre las páginas web de contenido periodístico que si constituían propaganda electoral cuando los contenidos versan sobre publicidad de campañas electorales:

> *"(...) como es la prensa virtual, en la que existe una relación de carácter informativo, pues por un lado está, el derecho a informar al público en general y por otro el derecho a informarse de quien accede a este tipo de páginas web, la información alusiva a la publicidad de campañas electorales, antes de los tres meses previos a la elección, constituiría violación al inciso segundo del artículo 24 de la Ley 130 de 1994."*

Finalmente, el Concepto más reciente sobre el particular varió la postura que vimos con el pronunciamiento del 2011, así las cosas el CNE con Concepto – Radicado No. 1185 de 201438 señaló que: "se observa que en las normas de carácter legal que regulan tantos las campañas electorales a la presidencia como las campañas electorales en general, no se aprecia regulación especial sobre la propaganda electoral en internet o en vehículos, razón por la cual, en principio, ésta debe regirse por las normas generales antes citadas, las que fijan límites temporales a la emisión y fijación de este tipo de propaganda". Con base en esto, no es posible realizar esta propaganda fuera del tiempo destinado para ella.

3.3.2. Sobre las redes sociales.

En materia de redes sociales, tampoco existe claridad total sobre la regulación de la propaganda electoral a través de este medio, sin embargo, podemos dilucidar que este no se enmarcaría en los criterios dados por el CNE para entender qué es propaganda electoral, recordemos que el CNE ha manifestado que la propaganda electoral se caracteriza por la difusión de mensajes dirigidos al público en general e indeterminado, utilizando medios de comunicación que permitan impactar a las personas, sin que medie su voluntad; con lo cual vemos que para el caso de las redes sociales, las mismas son de uso privado.

Sumado a lo anterior, el CNE se ha manifestado sobre el particular a través de diversos conceptos, entre los cuales encontramos: - Concepto- Radicado No. 1434 de 2011 con ponencia del magistrado Carlos Ardila, en el cual se le preguntó si la creación de páginas en las redes sociales donde se indica que un sujeto en particular aspira a un cargo de elección popular constituye propaganda electoral o no. El CNE respondió: "Para efectos de dar respuesta a éste interrogante, se diferenciará entre páginas Web y redes sociales:

Figura n°5 Página web y redes sociales

PAGINA WEB	REDES SOCIALES
La creación de páginas Web, alusivas a la campaña electoral al Concejo Municipal o cualquier otra Corporación Pública, de determinado candidato, **constituye propaganda electoral,** toda vez que es la	La utilización de las redes sociales en Internet **no constituye propaganda electoral**, siendo esta una forma de interacción social e intercambio dinámico entre personas, grupos e instituciones en un sistema abierto en permanente construcción, permitiendo que una persona publique información e ideas, generando comunicación directa que permite al usuario ingresar libremente en cualquier tiempo a la

invitación para obtener apoyo electoral, utilizando medios de comunicación masivos que impactan al público de manera general.	red social, siempre y cuando haya sido aceptado por el otro usuario. La diferencia en estos casos está marcada por la voluntad que media en las personas para decidir acceder a ver o escuchar dichos contenidos, y la comunicación directa entre los sujetos, sin que llegue a constituir búsqueda de apoyo de manera indiscriminada".

Fuente: Elaboración propia

Concepto – Radicado No. 1456 de 2011 con ponencia del magistrado José Vives:

> "*Ahora bien, no toda invitación a votar está limitada antes de los tres meses anteriores al debate electoral, puesto que no podría sancionarse la invitación a votar por una candidatura que personalmente, de manera verbal o escrita, un ciudadano hace a otro en comunicación privada, como tampoco aquella que se conoce en desarrollo del derecho a informar, sino solamente aquellas invitaciones o propagandas que se realicen utilizando medios de comunicación que impacten al público de manera general*".

Concepto - Radicado No. 6099 de 2011, con ponencia de la Magistrada Nora Tapia, al referirse a la propaganda electoral mediante el uso de las redes sociales señaló:

> *"En el caso de utilización de redes sociales en Internet, siendo éstas una forma de interacción social e intercambio dinámico entre personas, grupos e instituciones en un sistema abierto y en construcción permanente: como la red social Facebook, (sitio web gratuito de redes sociales, en ella el usuario puede agregar a cualquier persona que conozca y esté registrada, siempre que el invitado acepte su invitación) o Twitter (sitio web que permite a sus usuarios enviar y leer micro-entradas de texto de una longitud máxima de 140 caracteres: siendo las actualizaciones enviadas en forma inmediata a otros usuarios que han elegido la opción de recibirlas), que entran en funcionamiento cuando los usuarios libremente confirman que son amigos, lo que les permite ver sus perfiles, entrar en contacto con ellos y revisar voluntariamente el contenido del espacio que cada usuario tiene en la red social, de la cual son miembros."*

Con respecto a las redes sociales, el autor Emilio MÁRQUEZ en su artículo sobre Política Internacional, Redes Sociales, Usos y Costumbres nos aclara que:

> *"Las redes sociales otorgan la posibilidad de establecer verdaderas conversaciones entre ciudadanos y representantes de la política. Si se anula la interacción, se mutila el verdadero sentido de tener perfil en una red social. Por supuesto si cualquiera mima con gran esmero su identidad personal, aún con más motivo un político. La diplomacia y el respeto a la hora de intervenir en un medio de acceso público son una exigencia para cualquiera. (...). El atractivo más grande que tiene poseer un perfil en las redes sociales es tener la posibilidad de contar con un canal de comunicación directo y personal, si olvidamos esto pierde todo el sentido tener un perfil y se convierte en una simple herramienta propagandística*. (...).

Como se aprecia, la ganancia o utilidad que tiene una persona con respecto a otra con el empleo de estas nuevas formas de comunicación son las mismas, de lado y lado, es decir las de aprender, seguir, incluir, escuchar, difundir e implementar propuestas de forma personal y directa. Sin embargo, tratándose de correos que contengan propaganda electoral alusiva a campañas políticas y sean enviados masivamente a cuentas de correos de los usuarios del sistema, logrando invadir la esfera privada del propietario de la cuenta, se estaría ante la vulneración del término de tres meses previsto en la Ley 130 de 1994.

En términos generales debemos ver la aplicación o utilización de blogs y redes sociales en el tema político como una manera de generar el diálogo que siempre ha proclamado el modelo de Democracia Participativa que rige nuestro país, en la cual lo verdaderamente importante son las comunidades que se estructuran y donde nos sentimos partícipes de la sociedad, nos relacionamos, y desde donde podemos generar nuevas amistades, conocimientos e ideas y compartir lo que hacemos y lo que somos.

Para que pueda configurarse lo anteriormente expuesto, debe partirse del principio básico según el cual quién recibe el mensaje tiene el control de lo que se quiere ver y escuchar. De allí que los periodistas, políticos y analistas se hayan percatado de la importancia que revisten los usuarios de las redes sociales como líderes de opinión capaces de irradiar ideas, información y tendencias. Sin embargo, no puede todavía pensarse que, en nuestro país a diferencia de otros países en el mundo, los mecanismos modernos de comunicación hayan alcanzado una fuerte penetración y credibilidad entre los ciudadanos, y si así sucediera no ejercerían estos ningunos tipos de presión, pues como expresa el profesor Marcelino BISBAL: "El internet más que influir en la decisión del voto, ayuda a reforzar una idea ya concebida".

Para esta Corporación, los perfiles y grupos registrados en las redes sociales y asociados con mensajes e imágenes de contenido electoral, buscan generar un diálogo entre los usuarios de la red, trátese de precandidatos o candidatos a cargos de elección popular con la ciudadanía, los usuarios pueden resultar siendo un grupo de apoyo electoral, pero antes que nada la interacción de los mismos está dada para construir un proyecto político, aportar al mismo las observaciones que demande la sociedad e intercambiar ideas sobre los puntos objeto de propuestas de un eventual ejercicio de cargo de elección popular.

Esta Corporación advierte, que cualquier ciudadano, una vez inscrito como usuario de la Red Social, consiente en la posibilidad de recibir invitaciones, trátese de perfiles o de grupos que promuevan en los usuarios el conocimiento y promoción de un producto, difusión de alguna ideología, inclusive de un candidato, de tal manera, que el usuario está facultado para aceptar, rechazar o acudir, por sí mismo al perfil de cualquier aspirante a cargo de elección popular para iniciar un diálogo directo con el mismo y/o con su campaña.

Con base en lo anterior, concluyó el Concepto citado:

> "*De lo anterior, pretender que el Consejo Nacional Electoral intervenga en los perfiles o grupos de Redes Sociales "Facebook", "Twitter", entre otras, en los que se hace referencia a algunos aspirantes a cargos de elección popular, sería*

invadir la órbita de la intimidad de cada uno de los usuarios, desconocer la capacidad que tiene cada ciudadano para decidir acerca de la información que pretende recibir en su perfil y la naturaleza misma de cada Red Social, ya que fueron creadas para establecer diálogos entre los usuarios, en el caso de los aspirantes a cargos de elección popular y de los usuarios, se interactúa para conocer el presunto candidato, las acciones promovidas por el mismo en la comunidad y las propuestas para su eventual gobierno."

Así las cosas para el CNE: "los anuncios o mensajes propios de perfiles o grupos de las redes sociales "Facebook", "Twitter", entre otras, no constituyen propaganda electoral, toda vez que la esencia misma de las redes sociales consiste en generar una comunicación directa entre los usuarios de la red o de la web, de otra parte, los ciudadanos están en capacidad de aceptar, rechazar e inclusive de buscar de manera libre y voluntaria, el espacio de cualquier aspirante a cargo de elección popular".

En conclusión, podemos apreciar que la posición mayoritaria indica que la propaganda a través de páginas web se entiende como propaganda electoral en los términos de la Ley 1475 de 2011 en su artículo 35. Sin embargo, ante la ambivalencia de posiciones al interior del Consejo Nacional Electoral no podríamos tener certeza sobre el tratamiento del proselitismo político a través de estos medios. Por su parte, en materia de redes sociales es más claro que no constituye propaganda electoral por sí misma, teniendo en cuenta que la información que se recibe a través de ellas hace parte de la esfera privada de los ciudadanos (Misión de Observación Electoral, 2015).

Según estos pronunciamientos del Consejo Nacional Electoral(CNE) las redes sociales en si no constituirían propaganda electoral pues hacen alusión a que si se hace una intervención por parte del CNE a estas plataformas afectarían de manera directa a los usuarios pues según ellos se estaría vulnerando la intimidad de estos, pero al mismo tiempo estos usuarios se ven afectados pues encuentran sus redes sociales llenas de propaganda política la cual en ningún momento ha sido aceptada o solicitada por los usuarios por ende no ha habido consentimiento del usuario para tener su bandeja de entrada o de inicio con los candidatos para elecciones, ahora bien este tipo de propaganda política no se hace solo mediante un mensaje que un usuario le envié a otro en la esfera privada en este tipo de casos es clara la intimidad que en ciertas posturas ha demostrado el CNE para argumentar el motivo por el cual no intervienen en esta esfera, pero la realidad es que este tipo de propaganda no se hace solo por mensajes privados si no que son publicados para que todos lo puedan ver que es lo mismo que se hace cuando se colocan vallas publicitarias, la problemática aquí se genera porque las reglas sobre propaganda electoral son claras pues están prohibidas en el día que se estén llevando a cabo las elecciones y para las redes sociales es claro que no hay regulación ni límites.

IV. LIBERTAD DE EXPRESIÓN EN EL CONTEXTO DE LAS CAMPAÑAS ELECTORALES Y LAS REDES SOCIALES

La transformación de los espacios en donde se transmite información en lo que llevamos del siglo XXI ha supuesto un gran reto para los procesos democráticos alrededor del mundo. Cada vez es más evidente que las nuevas tecnologías de la información y de la comunicación juegan un papel crucial en cuanto a la propaganda electoral se refiere; en unos años hemos

ido de los carteles y afiches, pasando por los spots publicitarios en televisión, a los tuits, las cadenas de difusión y la actualización prácticamente en tiempo real, a través de las redes sociales, de lo que sucede en la campaña electoral.

A partir de los profundos cambios sociales vividos en Colombia desde la Constitución de 1991 y el final del bipartidismo institucionalizado durante el periodo histórico conocido como el Frente Nacional (1957-1974), la ciudadanía experimento un fuerte desapego por las fuerzas políticas tradicionales, pero paralelamente la irrupción de nuevas formaciones políticas en todo el espectro. La libertad de expresión una vez más se convirtió en motor del pensamiento independiente y plural en nuestro país amparado por la gama de derechos en la Carta de 1991, a pesar de la violencia y crispación social. Un primer esbozo del papel que tuvieron las redes sociales fue la llamada Ola Verde del año 2010, cuando el candidato Antanas Mockus se perfiló ampliamente para ganar las elecciones presidenciales de aquel año frente a Juan Manuel Santos, gracias en parte a las redes sociales que movilizaron el voto joven y de otros sectores políticos. Más recientemente, se evidenció la incidencia de las redes en las campañas del año 2018 y el plebiscito que buscaba aprobar los acuerdos del Gobierno Nacional tuvieron su principal escenario de discusión, ya no en la plaza pública, sino en internet.

La gran exposición a la información con la que convive el electorado, así como la activa participación propiciada por las redes sociales, ha traído consigo un fenómeno de desinformación y distorsión de la realidad amparado por el anonimato que en ocasiones brindan las redes sociales, la falta de fuentes que permitan verificar la información difundida, el descrédito de los medios tradicionales de comunicación, el fácil acceso a la internet y de manera evidente, por la falta de regulación sobre la materia. Todo lo anterior permite que la opinión pública se configure en torno a distintas versiones de la realidad, influyendo en la decisión final de las personas y afectando la transparencia electoral. En nuestro país debemos sumar la vaga situación del contenido que se difunde por los medios de comunicación masiva y su calificación como propaganda electoral o mera divulgación de principios e ideas políticas.

La actual situación de indefinición por parte de las autoridades respecto del uso y en ocasiones abuso de las redes sociales, pone de relieve una tensión entre la intervención de las autoridades en defensa de la idoneidad del proceso electoral, los derechos de participación política que poseen los ciudadanos, y el derecho a la libre expresión y difusión de información.

En este sentido, la existencia misma de los partidos políticos y la divulgación de sus principios e ideas constituyen un pilar fundamental del orden democrático y los derechos políticos, como expresa en sentencia la Corte Constitucional de Colombia: "*en el constitucionalismo y en la doctrina de los derechos humanos, las libertades de expresión, reunión y asociación forman una trilogía de libertades personales que se constituye, además, en prerrequisito de los derechos de participación política*."(MP. MARTINEZ CABALLERO, Alejandro, Sentencia C-265 de 1994.). Lo anterior permite apreciar que como pilar que es de la participación política, cualquier limitación que se imponga sobre la divulgación afecta la legitimidad del sistema democrático y la *operatividad* de los partidos políticos entendiéndola, como la capacidad que tienen estas organizaciones para servir de

canal ideológico con la ciudadanía, que libremente se encuentra en la facultad de pertenecer y participar en los partidos políticos.

No se concibe entonces que, en el marco de las redes sociales, una estricta regulación respecto del contenido expuesto se plantee como una forma de proteger los procesos democráticos cuando no existe claridad si se busca evitar que las personas y sobre todo los partidos, busquen apoyo por un determinado candidato (que de hacerlo con más de tres meses de anterioridad a las elecciones, representaría una infracción a la ley) o limitar, ya en la esfera personal que simpatizantes o no de los partidos políticos difundan su pensamiento sin que esto signifique una especie de propaganda.

Entonces, el problema se ahonda cuando las redes sociales por su naturaleza misma son un escaparate de expresión y difusión que no se ve limitado sino por el acceso a internet de sus usuarios, de manera que en lo que llevamos de esta década, y especialmente en los últimos procesos electorales los colombianos han estado expuestos a un mar de información que no necesariamente proviene de los partidos políticos o de sus militantes, que no siempre es veraz y que coopera con la destrucción de un debate sano para la democracia representativa. La situación es más grave aun cuando son los miembros de los partidos y sus candidatos los que propician desde el lenguaje la confrontación o promueven el abuso de las redes sociales.

Aun así y según la máxima autoridad electoral en Colombia (Consejo Nacional Electoral) cuando las invitaciones a votar por un candidato se realizan por las redes sociales, aunque no de forma pública, esta no debe ser entendida como propaganda. No obstante, es clara la misma Corporación en enunciar que cuando dichas invitaciones aparezcan en las plataformas digitales sin que medie el ánimo del espectador si constituye propaganda electoral. Esta posición es respetuosa de los derechos individuales de los usuarios de las redes sociales, pero no contempla en ningún momento el mal uso de estas y la afectación que puede generar en los derechos de los demás.

Por tanto, es importante enunciar que, en el entendido de la libertad de expresión como un derecho, solo es posible cuando y evidentemente se difunde el pensamiento, pero también cuando se recepta. Según el artículo 13 de la Convención Americana de Derechos Humanos, la libertad de expresión no solo comprende la emisión del pensamiento en sí misma, sino que también comprende la posibilidad de difundirlo y recibir información de otros, además de imponer un límite en las libertades y derechos de los otros.

Por consiguiente, se configura una característica crucial en todo este asunto frente a lo que es la libertad de expresión y es que en los procesos democráticos y cuando está en juego el interés público, recae sobre las personas una responsabilidad al recordar que este derecho no es absoluto. Al respecto la Corte Interamericana de Derechos Humanos nos dice: “Con todo, la libertad de expresión no es un derecho absoluto y puede estar sujeta a restricciones, en particular cuando interfiere con otros derechos garantizados por la Convención”. Es por tanto que es de suma delicadeza que se pretenda ejercer mal este derecho, sobre todo cuando en la contienda electoral la información falsa afecta directamente el ejercicio de los derechos políticos por parte de los ciudadanos, influenciando en su decisión final.

Debe recaer entonces un especial interés en la situación generada por el conflicto entre los derechos anteriormente mencionados. No puede en ningún momento la preservación de unos derechos afectar el disfrute de otros, sino más bien toda intervención de los Estados debe estar encaminada en el disfrute máximo de la libertad de expresión con el objetivo de enriquecer el debate público. Lo que en el entendido de la Carta Democrática de la OEA se configuran como elementos fundamentales de la democracia "la transparencia de las actividades gubernamentales, la probidad, la responsabilidad de los gobiernos en la gestión pública, el respeto por los derechos sociales y la libertad de expresión y de prensa". Es por tanto pertinente encontrar la fórmula que respete los derechos, y que no pase por castigar el anonimato o la denuncia social, ambas cruciales para la defensa de los derechos colectivos y la formación de la opinión pública, además de la preservación del pluralismo político.

El pluralismo político amparado por la Constitución colombiana, debe ser protegido no solo por su consignación en el articulado constitucional, sino también por el hecho de que para el fortalecimiento de las practicas e instituciones democráticas del siglo XXI es necesario más que nunca la discusión pública, en donde los derechos de todos no se encuentren contra los intereses de unos pocos, sino que se promueva de manera vehemente un espacio propicio para una mayor transparencia en el manejo de nuestras democracias.

CONCLUSIÓN

La era de la tecnología ha exigido consigo cambios en las estructuras jurídicas tradicionales, y el ámbito electoral no ha quedado por fuera de ello. En materia de campañas electorales, para el ordenamiento jurídico colombiano ha resultado bastante difícil arriesgarse a regular el campo de las redes sociales, ya que, se constituyen como un medio de comunicación masiva dentro de una jurisdicción de nadie: internet. La idea de entrar a regular el comportamiento de un candidato en este medio, podría atentar contra los derechos fundamentales que la misma Carta Política le reconoce. Sin embargo, ha sido evidente en la realidad colombiana, que el uso indebido de las redes sociales ha llevado a desinformar a la población, puesto que se presta para difundir información que anteriormente no pasa por filtros que examinen su veracidad.

Las redes sociales tales como Facebook y Twitter han permitido una mayor conexión entre la población, no obstante, al momento de referirnos al uso incontrolado que hacen los candidatos en contiendas electorales reconocemos que debería vigilarse dicha actividad puesto que supone una extralimitación en el ejercicio de sus derechos. Hemos creado entornos digitales similares a los del mundo real; tenemos una identidad digital que representa a la identidad verdadera en comunidades también digitales (Facebook, Twitter, Instagram). El derecho tiene que adaptarse a los avances de la tecnología, aunque representen grandes retos, no debe darse pie a que continúen existiendo vacíos jurídicos que permitan a las personas actuar como quieren simplemente porque es un mundo intangible.

Se tenía la idea de que dichos entornos digitales hacían parte de la esfera privada de la persona, quien encontraba en los mismos un espacio para poder interactuar de una forma menos restringida y desenvolverse con libertad. Sin embargo, se ha demostrado que lo realizado o difundido en dichos entornos afecta la realidad social, política y cultural del Estado. Conscientes de ello, los países no pueden continuar siendo indiferentes a una mínima

regulación en estos espacios. Así como se extienden los derechos del ciudadano a su identidad digital, también es hora de que se extiendan sus deberes y que se haga necesario sancionar a quienes utilicen indebidamente las redes sociales. En materia electoral, la propaganda electoral se ha hecho completamente insoportable en el entorno digital. Aquí no hablamos de vallas publicitarias ni de cuñas, ni nada de esa terminología que esta mandada a recoger, hablamos ahora un idioma diferente, términos actuales que se utilizan en la jerga común de la población tecnificada: *fanpage*, *Facebook live*, *boomerang*, trino, perfil, estado, muro, *hashtag*, *tweet*, *retweet*, *like*, *share*, *Follower*, etc.

Un candidato actualmente goza de numerosas herramientas para poder llegar a las personas, es decir, no necesita ahora salir a reunir simpatizantes en una plaza, simplemente puede tomar su celular y por medio de *Facebook live* grabarse en vivo para el público que se encuentre en su entorno digital, y causaría el mismo impacto, incluso uno mayor, porque dicho video se prestaría para ser difundido y así los entornos digitales de cada individuo simpatizante se conectarían a través de una publicación que comparten, que guste o no, quien no sigue al candidato inevitablemente tiene que ver el video en su "inicio" (en el caso de Facebook).

Las autoridades en materia electoral deben arriesgarse a estudiar el entorno de las redes sociales que al presente nos invade, es ahora una incipiente correlación de mundos: el digital y el real. Regular el comportamiento de un candidato o partido político en las redes, especialmente en lo que concierne a su propaganda electoral, no significa violar ninguna de sus libertades, sino más bien, salvaguardar los derechos de toda una sociedad.

BIBLIOGRAFÍA

Asamblea Nacional Constituyente . 1991. Constitución Politica de Colombia . [En línea] 20 de julio de 1991. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html.

Comisión de Regulación de Comunicaciones (CRC). 2011. Resolución N° 3066 de 2011 . [En línea] 18 de mayo de 2011. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=42871.

Comision de Regulacion de Comunicaciones (CRC). 2017. Resolucion No. 5111 de 2017. [En línea] 24 de febrero de 2017. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=42871.

Congreso de la República de Colombia . Ley 1475 de 2011. [En línea] http://www.secretariasenado.gov.co/senado/basedoc/ley_1475_2011.html.

Congreso de la República de Colombia. 1994. Ley 130. [En línea] 23 de marzo de 1994. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4814.

—. 1994. Ley 163 . [En línea] 31 de agosto de 1994. http://www.secretariasenado.gov.co/senado/basedoc/ley_0163_1994.html.

Consejo Nacional Electoral. 2007. *Concepto N° 0947*. s.l. : Consejo Nacional Electoral, 2007. MAg. Adelina Covo.

—. 2011. *Concepto N° 2843.* s.l. : Consejo Nacional Electoral, 2011. MAg. Oscar Giraldo JImenez.

—. 2010. *Resolucion N° 4030.* s.l. : Consejo Nacional Electoral, 21 de Septiembre de 2010. MAg. Bernardo franco Ramirez.

—. 2011. *Resolución No. 5650.* s.l. : Consejo Nacional Electoral, 2011. MAg. Jose Joaquin Vives.

Corte Constitucional De Colombia. 1994. Sentencia C-265 de 1994. *Mp. Martinez Caballero, Alejandro,* . 1994.

Corte Interameticana de Derechos Humanos (CIDH). 2009. Sentencia de 28 de enero de 2009. *Caso Rios y otros vs. Venezuela.* 2009.

Ministerio de Tecnologías de la Información y las comunicaciones. Concepto N°5404210. [En línea] https://www.mintic.gov.co/portal/604/w3-article-3202.html.

Ministerio del Interior. 2018. Decreto 430 de 2018. [En línea] 05 de marzo de 2018. https://www.mininterior.gov.co/sites/default/files/noticias/decreto_430_del_05_marzo_de_2018.pdf.

Mision de Obervacion Electoral. 2015. La Propaganda Politica en las Campañas Electorales en Colombia. [En línea] Octubre de 2015. https://moe.org.co/home/doc/moe_juridica/2015/La_propaganda_politica_en_colombia.pdf.

Presidencia de la República. Decreto 2241 de 1986. [En línea] http://www.secretariasenado.gov.co/senado/basedoc/decreto_2241_1986.html.

Revelo, J., García, M. La organización electoral en Colombia. [En línea] https://www.dejusticia.org/wp-content/uploads/2017/04/fi_name_recurso_184.pdf.

LOS DERECHO DE AUTOR Y LAS NUEVAS TECNOLOGIAS EN EL MARCO DEL COMERCIO ELECTRONICO

Por: ***Horacio Fernández Delpech***
Argentina

I.-
La propiedad intelectual y el Comercio Electrónico

El derecho de **propiedad** es el poder que tiene una persona, en forma directa e inmediata, sobre un bien, atribuyéndose a esa persona la capacidad de disponer de ese bien con las únicas limitaciones que pueda imponer la ley.

Tradicionalmente se entendió que el derecho de propiedad se refería a los bienes muebles y a los bienes inmuebles, pero ya desde hace años surge un tercer destinatario de este derecho, y me refiero a las obras intelectuales que son el fruto de la capacidad del hombre en la creación intelectual.

La creación intelectual, que nutre todos los días nuestra vida aportándonos conocimientos o recreando nuestro espíritu, es fruto de trabajo y sacrificio y como tal necesita y debe ser tutelada por el derecho mediante una legislación que proteja esta peculiar forma de propiedad. Es por ello que podemos decir que el derecho a la propiedad intelectual se integra por las normas que regulan los derechos que tienen los autores, inventores y otros titulares sobre las producciones fruto de su intelecto.

Estos derechos de propiedad intelectual surgen recién a fines del siglo 18, primero como privilegios a favor de las imprentas y luego, fundamentalmente con el Estatuto de la Reina Ana en Inglaterra [1] y con la ley de Derecho de Autor de Francia de 1793, como verdaderos derechos a favor de los autores de las obras intelectuales, concibiéndose desde entonces a la propiedad intelectual como un tipo más de propiedad sobre un bien inmaterial, creado por el hombre y al cual se debe proteger.

Este derecho a la propiedad intelectual se estructura a nivel mundial fundamentalmente a partir del Convenio de Berna para la Protección de las Obras Literarias firmado en 1886 y ratificado por la mayoría de las naciones [2] , y luego con las legislaciones de esas naciones, las que en mayor o menor medida adoptaron los principios de Berna.

---

[1] An Act for the Encouragement of Learning, by vesting the Copies of Printed Books in the Authors or purchasers of such Copies, during the Times therein mentioned,promulgado el 10 de abril de 1710.
https://archive.org/stream/thestatuteofanne33333gut/33333.txt

[2] Convenio de Berna para la Protección de las Obras Literarias y Artísticas del 9 de septiembre de 1886, completado, revisado y enmendado en 1896, 1908, 1914, 1928, 1948, 1967, 1971, que fuera ratificado por Argentina por la Ley 25140, http://www.wipo.int/treaties/es/text.jsp?file_id=283700

La propiedad intelectual comprende tanto a los derechos de autor como a los derechos de propiedad industrial.
Los primeros se refieren fundamentalmente a los aspectos estéticos y artísticos de la creación intelectual, aunque también se relacionan con otros activos intangibles de las empresas como los sitios web de estas o el software en algunos países.

La propiedad industrial se refiere en cambio, a las patentes, las marcas, en fin un sinnúmero de objetos producto del intelecto que tienen aplicación industrial, que componen el activo de las empresas y, que como, tal integran el comercio electrónico.

Muchos de estos activos de propiedad industrial, tienen las siguientes características

- Son bienes inmateriales
- Componen un valioso activo de las empresas
- Es necesario protegerlos, para evitar su apropiación por parte de terceros
- Son fundamentalmente temporales ya que tienen una limitación en el tiempo

El Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio (ADPIC o TRIPS en inglés) de 1994 [3], uniformó los estándares básicos de protección de los bienes intangibles en:

- Derechos de Autor o Copyright - se protege la expresión de la idea pero no la idea en sí mismo, dando al autor o editor de esa obra , expresión de la idea, derechos de propiedad sobre la misma
- Patentes - (en Argentina Ley 24481 Patentes de Invención y Modelos de Utilidad) - derecho exclusivo a la explotación de una invención durante un período determinado. A los efectos de la ley de patentes, es considerará invención a toda creación humana que permita transformar materia o energía para su aprovechamiento por el hombre, debiendo. cumplirse con: novedad, actividad inventiva y utilidad o aplicación industrial -
- Modelos de Utilidad - Toda disposición o forma nueva obtenida o introducida en herramientas, instrumentos de trabajo, utensilios, dispositivos u objetos conocidos que se presten a un trabajo práctico, en cuanto importen una mejor utilización en la función a que estén destinados, conferirán a su creador el derecho exclusivo de explotación, que se justificará por títulos denominados certificados de modelos de utilidad".
- Diseños Industriales - Las formas o el aspecto incorporados o aplicados a un producto industrial que le confieran carácter ornamental
- Secretos comerciales (incluyen fórmulas, algoritmos, Know how, métodos de organización, métodos de distribución, procesos de control de calidad etc.) - no se registran. su monopolio es mantenido por la no divulgación - su negociación se lleva a cabo a través de contratos de transferencia de tecnología.
- Marcas - Es una o más palabras o signo, con capacidad distintiva, que permite

3 El Acuerdo sobre los ADPIC es el Anexo 1C del Acuerdo de Marrakech por el que se establece la Organización Mundial del Comercio, firmado en Marrakech, Marruecos, el 15 de abril de 1994.
http://www.wipo.int/wipolex/es/other_treaties/details.jsp?group_id=22&treaty_id=231

diferenciar productos y servicios. El derecho exclusivo que una marca confiere puede ser ejercido solamente en el país de registro.

Podríamos también agregar otros activos intangibles de las empresas, que si bien no son mencionados por el ADPIC, integran también la propiedad Intelectual

- Nombres de dominio Internet - regulados por las normas de ICANN en cuanto a los internacionales gTLDs, o por las normas de los organismos NIC de cada estado, en cuanto a los ccTLDs.
- Bases de Datos - Reguladas por los regímenes de Protección de los Datos Personales – en la Argentina por Ley 25326

Con relación al software, algunos estados lo regulan y protegen en el marco de los derechos de autor (Argentina), mientras que otros lo incluyen en la propiedad industrial , permitiendo su patentamiento (EEUU y Japón).

La propiedad intelectual involucra a todos estos activos intangibles que son importantes en el desarrollo del comercio electrónico, ya que son los que lo hace funcionar . Los programas informáticos, los sitios web, las redes, los diseños de circuitos integrados, son elementos importantes en el Comercio electrónico y deben ser protegidos

En este nuevo mundo de las nuevas tecnologías gran parte del valor de muchas empresas esta conformado fundamentalmente por activos de propiedad intelectual. El valor de una empresa depende hoy en día más de los activos intangibles que de los activos tangibles. El valor de los sitios, las carteras de patentes y marcas etc. son las que aumentan el valor de su empresa.

Podemos ver que hoy en día que empresas que manejan activos intangibles como Google, Apple, Amazon, son posiblemente más valiosas que una gran empresa petrolera o Automotriz.

Pero voy a referirme ahora a algunos de estos activos intangibles.

II.-
Los derechos de autor. El concepto de reproducción

Dentro de los derechos de autor el PRINCIPIO BASICO es el Derecho de Reproducción, que es un derecho exclusivo de los autores, sus herederos y los editores a quienes se les haya cedido una obra, de autorizar la reproducción de sus obras.

Estos autores, herederos o editores son los únicos que pueden autorizar la reproducción de sus obras intelectuales, y cualquier reproducción que se realice sin esa autorización la debemos calificar con una reproducción ilegal, pudiéndose configurar un ilícito civil y hasta en algunos casos un ilícito penal.

Desarrollando ese derecho de reproducción, la inmensa mayoría de las legislaciones del mundo protegen a las obras intelectuales contra la reproducción sin la autorización del titular de los derechos de propiedad intelectual, estableciendo expresamente que "la protección

existe frente a cualquier procedimiento de reproducción", adoptando así en todas las legislaciones el concepto amplio de reproducción que fue establecido por diferentes Convenios Internacionales partiendo del Convenio de Berna en donde en el art. 9.1 se establece que *"los autores de obras literarias y artísticas protegidas por el presente Convenio gozarán del derecho exclusivo de autorizar la reproducción de su obras por cualquier procedimiento y bajo cualquier forma".* [4]

Pero debo resaltar que este concepto de reproducción utilizado por las diferentes legislaciones y por el Convenio de Berna, es no solo aplicable a la obra intelectual en un formato tangible, sino también a la obra digital de formato intangible.

Pero esta nueva era de la información y la comunicación en que vivimos , nos ha traído nuevas tecnologías las que facilitan enormemente la reproducción y divulgación de las obras del intelecto, en soportes no tradicionales.
El libro hecho en papel, como lo conocimos durante muchos siglos, va dejando paso a las obras en soportes virtuales, apareciendo así el libro electrónico, y la obra digitalizada que se vuelca a Internet.

Pero mayor es el tema de la obra musical, cinematográfica o audiovisual , a la que se llega luego de un rápido proceso de digitalización de la obra. y que consecuentemente facilita la libre reproducción de la misma. Cuando esa reproducción no es autorizada por el titular del derecho, es ilícita y da lugar a lo que vulgarmente se conoce como piratería.

En **la República Argentina**, la Constitución Nacional en la segunda parte del art. 17 establece, que: *"…Todo autor o inventor es propietario exclusivo de su obra, invento o descubrimiento, por el término que le acuerde la ley…".* Este principio constitucional se desarrolló con la ley 11723, del año 1933 [5], que regula el régimen de los derechos de autor, entendiendo por tales a los derechos que nacen de la creación de producciones científicas, literarias o artísticas.

Además, las leyes 24481, 22362 y el Decreto Ley 6673/63 regulan el régimen de los derechos a la propiedad industrial, referido en la Argentina también a creaciones intelectuales, pero cuando estas tienen una finalidad industrial, fundamentalmente en la protección de las patentes, marcas y diseños industriales.

El proceso de digitalización de las obras y el acceso a las mismas vía Internet, tiene grandes beneficios para los usuarios, pero trae peligros para los autores con relación a su uso, muchas veces producto de que las normativas de propiedad intelectual no fueron pensadas para el mundo de las nuevas tecnologías, ni fueron aún adecuadas a éste.

[4] Concepto consagrado en diferentes Convenios Internacionales a partir del Convenio de Berna para la Protección de las Obras Literarias y Artísticas del 9 de septiembre de 1886, completado, revisado y enmendado en 1896, 1908, 1914, 1928, 1948, 1967, 1971, que fuera ratificado por la Ley 25140,en donde en su art. 9.1 se establece que "los autores de obras literarias y artísticas protegidas por el presente Convenio gozarán del derecho exclusivo de autorizar la reproducción de su obras por cualquier procedimiento y bajo cualquier forma"
[5] Ley 11723 (B.O. 30.9.33)

La intangibilidad de la obra en formato digital y su fácil y rápida circulación por la red, no solo dificulta el control de los derechos de propiedad intelectual sobre las obras, sino que exige además una adecuación y una correcta interpretación de los principios de la protección existentes en las diferentes normativas, acorde con esta nueva herramienta producto de las modernas tecnologías.

Muchos proclaman el libre derecho de reproducción de la obra digital, afirmando que los derechos de propiedad intelectual en particular el derecho exclusivo de los autores a autorizar la reproducción de sus obras, no existen en la red, en donde todo se se podría copiar y reproducir sin el más mínimo respeto a los legítimos derechos de los autores.

Para quienes así piensan, Internet es un ámbito totalmente libre en donde todo es posible y donde no deben existir ninguna restricción ya que debe reconocerse la libre subida de contenidos a Internet, y a los usuarios de Internet el acceso irrestricto e incondicionado a la totalidad de los contenidos incorporados a la red, ya que de no ser así se impediría gozar del derecho a la cultura. Se ha creado así una industria de la piratería que afecta enormemente a la industria editorial, fonográfica y cinematográfica, tratándose de crear una conciencia de total inocencia por eludir derechos de autor.

Ello no es así, ya que los derechos de propiedad intelectual no son, como dicen algunos, un impuesto que limita el acceso a los bienes culturales, por el contrario son el mejor estímulo para la creación y para defender una justa retribución por la tarea realizada. Personalmente creo que configuran el más justificado de los derechos a la propiedad existente, pues se corresponden con un bien inmaterial constituido por una creación intelectual propia a la que se llega con trabajo, a diferencia de los bienes materiales producto muchas veces de otras circunstancias.
Para poder subir una obra intelectual, musical o audiovisual a Internet es necesario contar con la autorización expresa del autor o del titular del derecho sobre esa obra. De no ser así, esa subida a internet, que llamamos aproad de la obra, se convierte en un accionar ilícito.

Podemos entonces partir de una premisa: Toda obra intelectual sobre la cual su autor o editor posee derechos de propiedad intelectual, requiere necesariamente la autorización previa y expresa de éstos para ser incorporada a un sitio de Internet.

De no contarse con tal autorización, tal incorporación es un acto ilícito generador de responsabilidad tanto **para el titular del sitio** que incorpora la obra sin esa autorización, como incluso en algunos casos **para los Proveedores de Servicios de Internet** (Proveedor de Acceso y Proveedor de Hosting - ISPs), que posibilitan tal incorporación.

La doctrina y legislación predominante en el mundo funda esa responsabilidad de los ISP en un **criterio de responsabilidad subjetiva**, en la cual la responsabilidad de los ISPs sólo se da en la medida que hayan advertido o hayan sido advertidos de la infracción al derecho de propiedad intelectual, y pese a ello, no hayan impedido la introducción de la obra al sitio. Esta posición es la que ha adoptado EE.UU. en la Digital Millenium Copyright Act (DMCA), la Unión Europea en la Directiva 2000/31/CE , y España en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Creo que esta es la postura correcta y responde al real y efectivo funcionamiento de Internet y de sus sitios Web. El ISP sólo debe ser responsabilizado cuando se trate de contenidos propios o se demuestre una actitud culpable o negligente de su parte.

III.
La protección de la obra intelectual en el medio digital y en Internet

Pero para solucionar este candente problema de la reproducción ilícita volcada a formatos intangibles o subida a Internet, se van poco a poco esbozando soluciones que tienden a defender los derechos de propiedad de los autores sobre sus obras, para así lograr que estos reciban una retribución por sus obras, así como la defensa y protección de los sitios web frente al copiado de sus contenidos y otros problemas que pueden afectar a los sitios web y muchas veces afectar entonces al comercio electrónico.

Me referiré entonces a

- Las disposiciones de los Tratados Internet de la OMPI de 1996;
- La implementación de Medidas Tecnológicas de Protección;
- La gestión colectiva de los derechos digitales;
- Nuevas licencias de derechos de autor;
- La copia privada y el canon digital;
- La protección y defensa de los sitios Web

IV
Los Tratados Internet de la Ompi de 1996

El proceso de introducción de una obra a un sitio de Internet, upload de la obra, constituye conforme las disposiciones del Convenio de Berna y las leyes de Derechos de Autor, un acto de reproducción y, consecuentemente, requiere la expresa autorización de su autor o titular de derechos. Pero no solo esa incorporación de la obra debe ser autorizada, sino también que cualquier reproducción posterior de ella en Internet es también, conforme la ley una reproducción protegida para la ley.

Es así como la descarga de la obra desde el servidor en donde está alojada la Web, al disco duro del ordenador del usuario para que éste pueda visualizarla, es un proceso de reproducción en ese concepto amplio de reproducción, adoptado por la mayoría de las normativas. Pareciera que esto no debiera ser así ya que esa descarga de obras desde Internet para que el usuario pueda visualizarla es parte del proceso técnico de Internet, y para solucionar este problema aparecen los Tratado sobre Derechos de autor de la OMPI: **Tratado de la OMPI sobre Derecho de Autor** [6] (conocido como TODA o WCT) y **el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas** [7] (conocido como TOIEF o WPPT).

[6] TODA sigla en español y WCT sigla en inglés y que corresponde a Tipo Copyright Treaty http://www.wipo.int/wipolex/es/treaties/text.jsp?file_id=295158

[7] TOIEF. sigla en español y WPPT sigla en inglés y que corresponde a WIPO Performances and Phonograms Treaty. http://www.wipo.int/wipolex/es/treaties/text.jsp?file_id=295478

Estos tratados, si bien reafirman el derecho exclusivo de los autores a autorizar la reproducción, y establecen que el almacenamiento de una obra en formato digital, en un soporte electrónico o en Internet constituye una reproducción en el sentido del Artículo 9 del Convenio de Berna , establece también que los estados podrán prever en sus legislaciones limitaciones al derecho de reproducción del autor, en circunstancias como las que hemos analizado de reproducción temporal o permanente en el disco del usuario de Internet.
Se ha sostenidos reiteradamente, que cuando un usuario de Internet, accede a una obra, y a los fines de su exclusivo uso privado posterior, la almacena en su ordenador, está efectuando una actividad normal e inherente a Internet y que como tal acto debe considerarse una reproducción autorizada por el autor desde el momento en que éste efectuó el upload de la obra sin condicionarlo al cumplimiento de requisito alguno, dándose así el supuesto antes analizado contemplado por el tratado Internet de la OMPI.

V
Las medidas tecnológicas de protección

Aparecen ya hace años las medidas tecnológicas de protección como una solución técnica a la creciente violación de los derechos de los autores sobre sus obras intelectuales.

Las medidas tecnológicas de protección son sistemas informáticos que tienen como finalidad controlar y, en caso que sea necesario, impedir o restringir el uso en Internet de obras intelectuales protegidas por derechos de propiedad intelectual. Estas son una respuesta al intento de violar el derecho de propiedad intelectual de los autores y editores sobre sus obras. Pero resulta que ante esas medidas tecnológicas que puede el autor colocar en su obra para protegerla de la reproducción, surge y hoy en día un nuevo intento como es el de eludir tales medidas tecnológicas.

Conforme la OMPI [8], existen cuatro categorías de medidas tecnológicas de protección:
Medidas que protegen efectivamente un acto sujeto al derecho exclusivo de los autores; "

- Sistemas de acceso condicionado;
- Dispositivos de marcado e identificación de las obras;
- Sistemas de gestión de derechos digitales DRM – Digital Right Management; "

Como he dicho varias veces en trabajos y publicaciones, la primera categoría se refiere a ciertos dispositivos tecnológicos cuya finalidad es impedir que se realicen determinados actos que implican una violación al derecho de propiedad intelectual sobre una obra. Tal el caso de los dispositivos que impiden imprimir o copiar una obra de Internet.

La segunda categoría, referida a los sistemas de acceso condicionado, refiere a técnicas que condicionan el acceso a un sitio o a una obra incorporada a ese sitio, al cumplimiento de alguna condición preestablecida. Tal el caso de los sitios que exigen una clave o contraseña

[8] ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL – Taller sobre Cuestiones de Aplicación del Tratado de la OMPI sobre Derecho de Autor (WCT) y el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas (WPPT) - Ginebra, 6 y 7 de diciembre de 1999
http://www.wipo.int/meetings/es/details.jsp?meeting_id=3944

previa al ingreso al sitio o a la obra protegida, o que utilizan sistemas criptográficos o de firma digital para posibilitar tal acceso.

La tercera categoría cumple una función diferente, ya que son técnicas que tienden a marcar e identificar de alguna forma a las obras protegidas, proveyendo así al titular del derecho una forma de demostrar que la obra ha sido reproducida indebidamente. Tal el caso de la impresión en las obras protegidas de filigranas visibles o invisibles (esteganografía), marcas de agua (watermarks), u otras técnicas de marcado. Su función básica es informar sobre la utilización indebida de la obra y servir como prueba a la hora de tener que demostrar esa reproducción indebida.

Por último la OMPI se refiere a sistemas de gestión de derechos digitales, Digital Right Management (DRM), que son ttecnologías utilizadas para la gestión de los derechos mediante sistemas que difunden y gestionan la utilización de las obras protegidas.

Estas cuatro categorías descriptas por la OMPI pueden encontrarse muchas veces en forma única o complementándose entre si, y tienden todas a proteger a la obra intelectual, fundamentalmente frente a su reproducción ilícita, ilicitud que deviene del legítimo derecho exclusivo de los autores y editores sobre sus obras.

Destaco también, tal como lo han expresado varios autores, que, *la medida tecnológica de protección debe para ser válidas y obtener entonces la protección de la ley.*

- *ser eficaz o efectiva. La medida tecnológica que puede ser violada por cualquiera no es eficaz y consecuentemente no es válida ni debe obtener la protección legal. Tal criterio es tomado tanto por los Tratados Internet como por la Directiva Europea* [9]
- *No debe producir daño a los equipos de los usuarios. Es ilustrativo lo ocurrido no hace mucho tiempo en Estados Unidos y Europa cuando una importante empresa discográfica incorporó a gran cantidad de cd de música un sistema anticopia defectuoso que, al ser reproducidos esos cd en las computadoras, produjeron importantes daños, que obligaron a esta empresa a retirar del mercado esos cd, debiendo además resarcir por los daños causados.*
- *No pude invadir la privacidad de los usuarios. En el choque entre la medid a tecnológica y la privacidad del usuario, debe primar sin duda alguna la privacidad de este, aunque con ello se desproteja a la obra.*
  Un interesante caso al respecto es la utilización como parte de la medida tecnológica de protección de cookies, que obtienen y difunden informaciones personales del usuario y violan de esta forma su privacidad;
- *No puede dejar de informarse al consumidor sobre cualquier consecuencia querida o no querida que pudiera causarse, como podría ser una medida tecnológica anticopia que en determinados equipos impidiese la lectura del contenido protegido.*

[9] La Directiva 2002/29/CE establece en su art. 6.3 2 parte*: "las medidas tecnológicas se considerarán "eficaces" cuando el uso de la obra o prestación protegida esté controlado por los titulares de los derechos mediante la aplicación de un control de acceso o un procedimiento de protección, por ejemplo, codificación, aleatorización u otra transformación de la obra o prestación o un mecanismo de control de copiado, que logre este objetivo de protección"*

Pero frente al desarrollo de las medidas tecnologías para proteger a las obras, se han creado mecanismos destinados a eludir estas medidas tecnológicas, esos actos de elución de las medidas tecnológicas de protección implican la manipulación de las medidas tecnológicas con la finalidad de limitar o eliminar su finalidad protectoria.

Es por ello que es necesario implementar una nueva protección contra las acciones elusivas de las medidas tecnológicas. Se trata de dos soluciones distintas y complementarias entre si, la primera de carácter técnico tiende a proteger a la obra, y la segunda, de carácter jurídico y que es complementaria de la primera, trata de dar una protección no ya técnica sino jurídica frente al acto violatorio o elusivo de la protección técnica.

Esta protección jurídica frente al acto elusivo está dirigida fundamentalmente

- A prohibir tales actos elusivos;
- A prohibir y/o controlar los dispositivos y/o servicios que puedan utilizarse a tal fin. Recordemos aquí que muchas veces existen dispositivos y/o servicios con múltiples usos, muchos de ellos lícitos, pero también en algunos casos con finalidades elusivas de las medidas de protección.
- A regular las limitaciones y/ excepciones a la protección contra los actos elusivos en determinados casos

Los Tratados Internet, contemplan el tema estableciendo en el art. 11 del **Tratado de la OMPI sobre Derechos de Autor de 1996**, y con relación a las obligaciones relativas a las medidas tecnológicas, establece:

> *"Las Partes Contratantes proporcionarán protección jurídica adecuada y recursos jurídicos efectivos contra la acción de eludir las medidas tecnológicas efectivas que sean utilizadas por los autores en relación con el ejercicio de sus derechos en virtud del presente Tratado o del Convenio de Berna y que, respecto de sus obras, restrinjan actos que no estén autorizados por los autores concernidos o permitidos por la Ley".*

Por su parte el artículo 18 del **Tratado de la OMPI sobre Fonogramas de 1996**, y con relación a las obligaciones relativas a las medidas tecnológicas, establece:

> *"Las Partes Contratantes proporcionarán protección jurídica adecuada y recursos jurídicos efectivos contra la acción de eludir medidas tecnológicas efectivas que sean utilizadas por artistas intérpretes o ejecutantes o productores de fonogramas en relación con el ejercicio de sus derechos en virtud del presente Tratado y que, respecto de sus interpretaciones o ejecuciones o fonogramas, restrinjan actos que no estén autorizados por los artistas intérpretes o ejecutantes o los productores de fonogramas concernidos o permitidos por la Ley.*

Podemos ver que tanto en el Tratado sobre Derecho de Autor (WCT) como en el Tratado sobre Fonogramas (WPPT) se establece la protección contra la acción elusiva de la medida tecnológica pero no se precisa como debe darse esa protección ni que actos deben ser prohibidos, dejando ello al criterio de los estados.

Mi país, la Argentina, no ha dado cumplimiento a estos tratados pese a haberlos suscripto y ratificado, ya que no ha adecuado la ley de Propiedad Intelectual a lo que disponen los mismos en cuanto al concepto de reproducción en el mundo digital, a la incorporación de las medidas tecnológicas de protección y a la sanción de una legislación antielusiva de esas medidas tecnológicas.

Otros países en cambio han cumplido con el compromiso asumido al suscribir los Convenios Internet y han regulado al efecto. Un ejemplo es EEUU en donde la Digital Millennium Copyright Act (DMCA), admite y regula a las medidas tecnológicas de protección y penaliza la producción y difusión de tecnología, dispositivos o servicios destinados a eludir las medidas. En igual sentido las actuales legislaciones de Chile, Perú y Brasil, en Europa la Directiva 2001/29 del Parlamento y del Consejo de la Unión Europea insta a las partes a incluir y regular las medidas tecnológicas dentro de su legislación interna.

VI
La gestión colectiva de los derechos digitales

Existen ciertas formas de explotación de las obra intelectuales en las que se hace imposible, o muy difícil, el efectivo control y cobro de los derechos de autor por parte de los titulares de estos derechos.
Me refiero específicamente a la obra música transmitida por radio, televisión, en fiestas y locales, o la representación de obras, o el fotocopiado de libros.
Tradicionalmente surgen así entidades que representan a los autores y editores y perciben colectivamente los derechos de quien utilizan las obras reproduciéndolas.
Es así como las entidades de gestión colectiva, negocian tarifas y las condiciones de utilización con los usuarios, otorgándoles licencias y autorizaciones de uso, al mismo tiempo que perciben de estos regalías que luego distribuyen regalías, entre los titulares de derechos.

La OMPI ha definido a la gestión colectiva como: *el ejercicio del derecho de autor y los derechos conexos por intermedio de organizaciones que actúan en representación de los titulares de derechos, en defensa de sus intereses.*[10]

Esta gestión Colectiva llega hoy también al entorno digital donde la transmisión y reproducción de obras por intermedio de Internet, puede ser ejercida por entidades específicas.
En estos casos es donde la gestión colectiva aparece como un medio efectivo de protección, control y cobro de los derechos de los autores, editores y titulares de derechos conexos.

Es así como en muchos países existen entidades que tienen a su cargo la gestión colectiva de los derechos de propiedad intelectual sobre las copias digitales de obras literarias y artísticas. Tal el caso de CEDRO [11] en España o de CADRA [12] y SADAIC [13] en la Argentina.

10 Gestión colectiva del Derecho de autor y los derechos conexos
http://www.wipo.int/copyright/es/management/
[11] Centro Español de Derechos Reprográficos
[12] Centro de Administración de Derechos Reprográficos
[13] Sociedad Argentina de Autores y Compositores

VII
Nuevas Licencias sobre derechos de autor

Tradicionalmente la forma de retribuir a los autores por sus creaciones intelectuales, siempre fueron las licencias de los autores y editores. Estas licencias se instrumentaban a través de contratos en los cuales los autores cedían los derechos sobre una obra para ser publicada o editada, y los editores (editoriales, discográficas, empresas cinematográficas, etc.,) se comprometían a que por la publicación o difusión de la obra le abonarían al autor derechos de autor, fijados generalmente en un porcentaje sobre el precio de venta de la obra.

Pero esa licencias individuales se vuelven insuficientes frente al nuevo panorama en donde se distribuyen las obras a través de Internet, llegando a miles de usuarios que bajan las canciones, libros, etc. de Internet, sin pagar ningún derecho, en donde obviamente esta conducta es ilícita y defrauda al autor.

Es por ello que aparecen en los últimos años nuevas licencias digitales por las cuales se ceden, o venden libros, archivos musicales, cinematográficos o de texto, para que sean colocados en sitios de Internet (Netflix, Spotify, Amazon, etc.), de donde el usuario los puede bajar pagando un importe dinerario. En el caso de Netflix se las denomina licencias de derechos de transmisión para diversas series y películas.

El usuario que compra la obra paga, directamente o mediante una suscripción, una cantidad mínima, pero multiplicado por miles de usuarios se convierten cantidades de dinero interesante con el cual el vendedor puede retribuir a los autores o recuperar lo abonado en caso de que haya adquirido previamente los derechos.

También existen hoy en día como una nueva forma de licenciamiento, las licencias Creative Commons, en las cuales el licenciador, titular del derecho de propiedad sobre una obra permite su uso libre dentro de ciertos parámetros fijados de antemano. Este sistema esta fundamentalmente dirigido al licenciamiento del software

VIII
La copia privada. El sistema de compensación equitativa por copia privada. Canon digital. El caso de España

En España, [14] si bien se sigue el régimen general de protección de los derechos de autor mediante el derecho patrimonial de reproducción, que únicamente legítima a su titular a autorizar o prohibir la producción de copias de su obra, existen algunos limites a este derecho, entre los que se encuentra la copia privada, por la cual una persona física puede realizar una copia de una obra ya divulgada cuando sea para su exclusivo uso privado y sin fines comerciales. La contrapartida a este derecho obliga a establecer una vía para que los titulares de los derechos sobre la obra reproducida reciban una compensación equitativa. [15] A tal fin

[14] Texto refundido de la Ley de Propiedad Intelectual, http://www.wipo.int/wipolex/es/text.jsp?file_id=443328

15 Ello deriva de la Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información, en la cual el art 5 establece «Los Estados miembros podrán establecer excepciones o limitaciones al derecho de reproducción contemplado en el artículo 2 en los siguientes casos:

desde1993 rigió el sistema conocido como «canon digital» que era abonado por las empresas que fabricaban y distribuían equipos, soportes y dispositivos que permitían la realización de copias privadas de obras protegidas.

El 30 de noviembre de 2011 el Gobierno dictó el Real Decreto-ley 20/2011, y suprimió de forma inesperada el sistema de compensación equitativa por copia privada, vigente desde 1993 en España. Desde entonces La financiación de la compensación equitativa por copia privada estaba a cargo de una partida de los Presupuestos Generales del Estado de cada año. Sin embargo recientes decisiones judiciales han dejado sin efecto este sistema de financiación, y Mediante el **Real Decreto-ley 12/2017 en vigencia desde el 1 de agosto de 2017,**[16] se tiende a sustituir el actual sistema de compensación equitativa financiado con cargo a los Presupuestos Generales del Estado por un modelo basado en el pago de un importe a abonar por los fabricantes y distribuidores de equipos, aparatos y soportes de reproducción.

La ley entiende como copia privada, en el art.31, a la que se lleve a cabo por una persona física exclusivamente para su uso privado, no profesional ni empresarial, y sin fines directa ni indirectamente comerciales, exigiendo además que la reproducción se realice a partir de una fuente lícita y que no se vulneren las condiciones de acceso a la obra o prestación.

IX
La protección y defensa de los sitios Web y de los elementos de la Propiedad Industrial

Los sitios Web de las empresas son hoy en día uno de los instrumentos más importantes para promover las ventas y los negocios de las empresas y de esa forma contribuir al desarrollo del Comercio Electrónico. Es común hoy en día encontrar casos en que han sido copiados la apariencia, el funcionamiento y el contenido de sitios web de carácter comercial por empresas de la competencia, generándose conflictos que muchas veces se deben dirimir ante la justicia.

Vemos también numerosos casos en los que se ha usurpado el nombre de una empresa o de una marca, creando un tercero un sitio, atrayendo así engañosamente a ese sitio a compradores del producto. De allí que es sumamente importante que los titulares de los sitios Web adopten una serie de medidas necesarias para proteger a los sitios Web de su empresa.

- El nombre de dominio del sitio, y que integra un derecho de autor, debe protegerse mediante la pertinente inscripción en los Registros de nombres de dominio, así como la inscripción del sitio y su contenido en la Dirección Nacional de Derechos de autor.

b) en relación con reproducciones en cualquier soporte efectuadas por una persona física para uso privado y sin fines directa o indirectamente comerciales, siempre que los titulares de los derechos reciban una compensación equitativa, teniendo en cuenta si se aplican o no a la obra o prestación de que se trate las medidas tecnológicas contempladas en el artículo 6;

[16] Real Decreto-ley 12/2017, de 3 de julio, por el que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril, en cuanto al sistema de compensación equitativa por copia privada. (BOE núm. 158, de 4 de julio de 2017) http://www.wipo.int/wipolex/es/details.jsp?id=17103

- Los sistemas de comercio electrónico, los motores de búsqueda y otras herramientas técnicas de Internet deben protegerse mediante el sistema de patentes o como modelos de utilidad, inscribiéndolos en los pertinentes registros de propiedad industrial.
- los programas de software, pueden protegerse por el régimen de los derecho de autor y/o por el sistema de patentes, según la legislación de cada estado; en la República Argentina su protección corresponde al régimen der los derechos de autor, por el contrario en otros países como EEUU o Japón, la protección se da en el marco de las patentes
- el diseño y el contenido del sitio Web, incluyendo su principal aspecto, sus textos, gráficos, etc., pueden protegerse por el sistema de derecho de autor;
- las bases de datos pueden protegerse por derecho de autor ya que en casi todas las legislaciones están incluidas en ese régimen
- los nombres comerciales, nombres de productos y cualquier otro signos que aparezca en el sitio Web pueden protegerse como marcas;
- los elementos confidenciales del sitio Web (como los gráficos, el código fuente, el código objeto, los algoritmos, los programas u otras descripciones técnicas, los gráficos de datos, los gráficos lógicos, los manuales de usuario, las estructuras de datos y el contenido de las bases de datos) pueden protegerse mediante la legislación sobre secretos comerciales que rija en cada estado

Todos estos elementos integran el marco normativo de la Propiedad Intelectual, ya sea dentro del régimen de los derechos de autor o del sistema de la Propiedad Industrial.
En cada uno de estos regímenes y variando en los diferentes estados existen oficinas de derechos de autor u oficinas de marcas, en donde deben inscribirse estos activos intangibles de las empresas.
Con relación a los derechos de autor, en la Argentina existe la Dirección Nacional de Derechos de Autor en donde además de inscribirse los libros y obras escritas, hoy en día esta contemplado el registro de los sitios Web, dando así protección a la propiedad intelectual en todos estos casos

Con relación a las marcas comerciales, previo a todo debe verificarse que la marca elegida deber ser distintiva para tu producto o servicio, y no encontrarse dentro de los términos genéricos del rubro. Asimismo debe ser lícita y original y no tener ninguna similitud, ni siquiera fonética, con otra marca registrada previamente en ese mismo rubro.

X
Conclusión

Como hemos podido analizar en este trabajo, la propiedad intelectual que comprende tanto a los derechos de autor como a los derechos de propiedad industrial, tiene una relación directa con el Comercio Electrónico, ya que los activos de propiedad intelectual constituyes un patrimonio importante en las empresas.

De allí que la violación a los derechos de Propiedad Intelectual, no puede ser admitida y debe tenderse a buscar los medios para su protección, medios estos que hemos tratado de explicar sintéticamente acá.

Al aplicar esta protección debemos tener especialmente en cuanto lo dispuesto en el art. 7 del Acuerdo sobre los ADPIC del Acuerdo de Marrakech cuando establece: " *La protección y la observancia de los derechos de propiedad intelectual deberán contribuir a la promoción de la innovación tecnológica y a la transferencia y difusión de la tecnología, en beneficio recíproco de los productores y de los usuarios de conocimientos tecnológicos y de modo que favorezcan el bienestar social y económico y el equilibrio de derechos y obligaciones* ".

BIBLIOGRAFIA

ARRABAL, Pablo - Manual práctico de propiedad intelectual e industrial, Ediciones Gestión, España, 1991.

BONDIA ROMAN, Fernando - El significado de la propiedad intelectual en la sociedad de la información, Universidad de Salamanca, Ediciones de la Universidad, 1987.

BORETTO, Mónica M. – E-Book. Sistema de licencias en el entorno digital. Sitio de Internet: www.creandopalabras.com

BLOJ, Sebastián – Comentario a la Modificación de la Ley de Propiedad Intelectual de Argentina respecto de la Autoría - Publicado en el sitio Web del Centro Colombiano del Derecho de Autor - http://www.cecolda.org.co/index.php?option=com_content&task=view&id=36&Itemid=40

CABANELLAS, Guillermo - Diccionario de Derecho, Editorial Heliasta, Buenos Aires, 2007 (con M. Ossorio).

CABANELLAS, Guillermo - Derecho de las patentes de invención, Editorial Heliasta, Buenos Aires, 2ª edición 2004.

CARRANZA TORRES, Martín y BRUEBA, Horacio, Software propietario y software libre ¿opciones compatibles o posiciones irreductibles?, Publicado en: Sup. Act. 14/10/2008, 1.

CARRANZA TORRES, Martín – Problemática Jurídica del Software Libre, Editorial Lexis Nexis, Buenos Aires, 2004.

CASADO, Laura - Manual de derechos de autor, Editorial Valletta, Florida, Pcia de Buenos Aires, 2005.

COLOMBET, Claude - Grandes principios del derecho de autor y los derechos conexos en el mundo: estudio de derecho comparado, Ediciones UNESCO/CINDOC, Madrid, 1997.

CORREA, Carlos M. - Propiedad intelectual y políticas de desarrollo, Editorial Ciudad Argentina, Buenos Aires, 2005.

CORREA, Carlos M. - Derechos de propiedad intelectual competencia y protección del interés público, Editorial B de F, Buenos Aires, 2009.

DAVARA RODRIGUEZ, Miguel – Manual de Derecho Informático, Aranzadi, Navarra, España, 2004.

DELLA COSTA, Héctor - Derecho de Autor y su novedad, Fundación Editorial de Belgrano, Buenos Aires, 2006.

DELGADO PORRAS, Antonio - Propiedad Intelectual, Ediciones Thomson Civitas, España, Edición 15, 2007.

DE SANCTIS, Valerio – Contratto di edizione. Contratto de rapresentazzione e di esecuzione, Ed.Giuffré, Milan 1965.

ELIAS, Stephen - Patent, Copyright, and Trademark: A Desk Reference to Intellectual Property Law, Berkeley, California, Nolo Press, 1997.

EMERY, Miguel Ángel - Propiedad Intelectual, Ley 11723 Comentada, anotada y concordada con los tratados internacionales, Editorial Astrea, Buenos Aires, 1999.

EMERY, Miguel Ángel y GARCIA SELLART, Marcelo – El software ¿Obra protegida?, ED 176-240.

EMERY, Miguel Ángel - Aplicación de los Tratados y Convenios Internacionales a los derechos de propiedad intelectual, ED 177-601.

EMERY, Miguel Ángel. - La protección de los modelos y obras de arte o ciencia aplicada al comercio o a la industria en la ley 11723, LL 1986-B-774.

EMERY, Miguel Ángel – La interpretación restrictiva de derecho de autor, LL 1991-C-401.

EMERY, Miguel Ángel – Aplicación de los tratados y convenios internacionales a los derechos de propiedad intelectual, ED, 177-601.

FERNANDEZ BALLESTEROS, Carlos A. - Marco Jurídico Internacional del Derecho de Autor y de los Derechos Conexos. De Berna (1886) a los Tratados de la OMPI (1996) , Documento Desarrollado en la II Jornada de Derecho de Autor en el Mundo Editorial, Buenos Aires, 28 y 29 de Abril de 2004. (Inédito).

FERNANDEZ DELPECH, Horacio - Protección Jurídica del Software, Editorial Abeledo-Perrot, Buenos Aires, 2000.

FERNANDEZ DELPECH, Horacio - Internet: Su Problemática Jurídica, Editorial Lexis Nexis, Buenos Aires, 2004.

FERNANDEZ DELPECH, Horacio . Manual de los Derechos de autor. Editorial Heliasta Buenos Aires, 2011

FERNANDEZ DELPECH, Horacio - Nueva Directiva de la Unión Europea sobre Conservación de Datos de Tráfico, Revista de Contratación Electrónica, Nº 68, Editora de Publicaciones Científicas y Profesionales, Madrid, Febrero 2006.

FERNANDEZ DELPECH, Horacio – La reproducción de las obras intelectuales por los usuarios de Internet en la doctrina, en la legislación iberoamericana y a la luz de los últimos documentos internacionales, Número Especial de Jurisprudencia Argentina - LexisNexis, Buenos Aires, 25 de febrero de 2004.

FERNANDEZ DELPECH, Horacio - Medidas Tecnológicas de protección de la Propiedad Intelectual, los actos elusivos, la protección jurídica contra la elusión, Revista Electrónica del Centro Colombiano del Derecho de Autor, http://www.cecolda.org.co/index.php?option=com_content&task=view&id=237&Itemid=40

FERNANDEZ NUÑEZ, Javier - Derechos Intelectuales, Ley 11723 y su Reglamentación Comentada y Anotada, Editorial Lexis Nexis, Buenos Aires, 2004.

FILIPELLI, Gerardo - Derechos de autor, reproducción ilegal y protección de las obras en espacios virtuales, III Encuentro de la Red de Bibliotecas de Derecho y Ciencias Jurídicas, Buenos Aires, septiembre de 2001, publicación electrónica: http://bibliotecajuridicaargentina.blogspot.com/2006/11/derechos-de-autor-reproduccin-ilegal.html

GARROTE FERNANDEZ, Ignacio - El derecho de autor en Internet: la directiva sobre derechos de autor y derechos afines en la sociedad de la información, Editorial Comares, Granada, 2001.

GARROTE FERNANDEZ, Ignacio - El derecho de autor en internet: los tratados de la OMPI de 1996 y la incorporación al derecho español de la directiva 2001/29/CE, Editorial Comares, Granada, 2003.

GARROTE FERNANDEZ, Ignacio - La reforma de la copia privada en la Ley de propiedad intelectual, Editorial Comares, Granada, 2005.

GEUGUER HERNANDEZ, Luis - Limitaciones al ejercicio de los derechos intelectuales en las obras didácticas, científicas, artísticas y literarias, Editor Universidad Nacional Autónoma de México, 1963.

GOLDSTEIN, Guillermo - Propiedad intelectual y nuevas tecnologías (televisión por cable y por satélite), LL 1991-B-1009.

GREGORINI CLUSELLAS, Eduardo L. – La violación del derecho a la propia imagen y su reparación, LL 1996-D-136.

HARVEY, Edwin – Derecho de Autor, Abeledo Perrot, Buenos Aires, 1997.

HERRERA SIERPE, Dina – Propiedad Intelectual. Derechos de Autor. Ley no. 17.336 y sus modificaciones, Editorial Jurídica de Chile, 1999

IGLESIAS, Gonzalo - Licencias de Uso No Propietarias: Software Libre y Software de Código Abierto, Alfa Redi Revista de Derecho Informático, No. 120 - Julio del 2008. edición electrónica http://www.alfa-redi.org/rdi-articulo.shtml?x=10651

IGLESIAS PRADA, José Luis - Los derechos de propiedad intelectual en la Organización Mundial del Comercio (OMC) : el acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio, Centro de Estudios para el Fomento de la Investigación, España 1997

ITHURRALDE, María Pía – La expresión del autor como único objeto de protección, LL 27.11.2009.

LAU, Iván – Propiedad Intelectual, Imprenta Universal Books, Panamá, 2004.

Ledesma, Julio – La Piratería en el Campo Informático, ED 129-793.

LIPSZYC, Delia - Derechos de autor y derechos conexos – Ediciones Unesco-Cerlac-Zavalia, Buenos Aires, 2007.

LIPSZYC, Delia – El derecho de autor y los derechos conexos en el acuerdo sobre los ADPIC (o TRIPs), LL, 1996-E-1395.

LIPSZYC, Delia – Nuevos temas de derecho de autor y derechos conexos, Editorial Zavalia, Buenos Aires, 2004.

LIPSZYC, Delia y VILLALBA , Carlos Alberto – El derecho de autor en la Argentina: Ley 11,723 y normas complementarias y reglamentarias, concordadas con los tratados internacionales, comentadas y anotadas con la jurisprudencia, Editorial La Ley , Buenos Aires, 2001.

MARESCA, Fernando - Aspectos Jurídicos del Software Libre, Alfa Redi Revista de Derecho Informático, No. 084 - Julio del 2005, edición electrónica http://www.alfa-redi.org/rdi-articulo.shtml?x=917

MILLE, Antonio - Impacto del Comercio electrónico sobre la propiedad intelectual, Derecho de la Alta Tecnología. Nº 117, mayo de 1998.

MILLE, Antonio - Propiedad intelectual del software para computadoras y bases de datos, ED, 157-681.

MOUCHET, Carlos – Los Derechos de los Autores e Intérpretes de Obras Literarias y Artísticas, Monografías Jurídicas, Abeledo Perrot , Buenos Aires, 1966.

NUÑEZ, Javier F. - DERECHOS INTELECTUALES. LEY 11723 Y SU REGLAMENTACIÓN, Abeledo Perrot, Buenos Aires, 2004.

OMPI - ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL, Glosario de derechos de autor y derechos conexos – Ginebra – 1978.

OMPI - ORGANIZACIÓN MUNDIAL DE LA PROPIEDAD INTELECTUAL - Taller sobre Cuestiones de Aplicación del Tratado de la OMPI sobre Derecho de Autor (WCT) y el Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas (WPPT) - Ginebra, 6 y 7 de diciembre de 1999

OMPI - Organización Mundial de la Propiedad Intelectual - Conclusiones de la Decimoctava sesión del comité permanente de derecho de autor y derechos conexos, Ginebra, 25 a 29 de mayo de 2009.

OMPI - Organización Mundial de la Propiedad Intelectual, Study on Copyright Limitations and Exceptions for Libraries and Archives, prepared by Kenneth Crews, Director, Copyright Advisory Office, Columbia University, Ginebra, November 3 to 7 2008 .

OSSA ROJAS, Claudio Patricio - Medidas técnicas de protección de los derechos de autor y los derechos conexos en el entorno digital, Revista Electrónica de Derecho Informático, Alfa Redi, número 121, año 2008

OSSA ROJAS, Claudio Patricio - Derechos de autor y derechos conexos como herramientas estratégicas para avanzar hacia una Sociedad del Conocimiento. El Caso de Chile, Revista Electrónica de Derecho Informático, Alfa Redi, número 104, año 2007

PALAZZI, Pablo A. - La exclusión del régimen de Derecho de Autor de las ideas, sistemas, métodos, aplicaciones prácticas y planes de comercialización, Documento Nº 6, Centro de Tecnología y Sociedad, Universidad de San Andrés, (Inédito).

PALAZZI, Pablo A. - El software en la ley 11.723. Reseña jurisprudencial, Jurisprudencia Argentina, Nº 5940 del 5/7/1995.

PASTRANA, Juan David – Derechos de Autor, Ediciones Flores, 2008

PEIRETTI, Graciela - "Función del Registro en el Derecho de Autor", Trabajo presentado en la III Jornada de Derecho de Autor en el Mundo Editorial organizada por CADRA en la Feria del Libro Buenos Aires, 21 y 22 de Abril de 2005.
http://www.cadra.org.ar/upload/Peiretti_Registro_Obras.pdf

PIOLA CASSELLI, Eduardo - Trattato del Diritto di Autore e del Contratto di Edizioni, Unione Tipográfico Editrice Torinese, Torino, 1927.

RADAELLI, Sigrido Augusto y MOUCHET, Carlos - Delitos contra los derechos intelectuales: la Ley argentina 11.723, Editorial V. Abeledo, Buenos Aires, 1935.

RAGEL, Luis Felipe – La duración de la propiedad intelectual y las obras en dominio público, Editorial Reus, Madrid, 2003.

ROGEL VIDE, Carlos - Estudios completos de propiedad intelectual, Volumen 1 y 2, Editorial Reus, Madrid, 2003 y 2006.

ROGEL VIDE, Carlos - Autores, coautores y propiedad intelectual, Tecnos, España, 1984.

ROGEL VIDE, Carlos - Cinematographers copyright, Editorial Reus, Madrid, 2009

ROGEL VIDE, Carlos - Nuevas Tecnologías y Propiedad Intelectual, Editorial Reus, Madrid, 1999

SANCHIS MARTINEZ, María Trinidad - Derechos de autor, digitalización e Internet, Editorial Universitas, 2004, Córdoba

SATANOWSKY, Isidro - Derecho Intelectual, Tomo I, Tipográfica Editora Argentina, Buenos Aires, 1954.

SHERWOOD, Robert M. – Los sistemas de Propiedad Intelectual y el estímulo a la inversión, Editorial Heliasta SRL, Buenos Aires.

SERRANO GOMEZ, Eduardo - Administraciones públicas y propiedad intelectual, Editorial Reuss, Madrid, 2007

STRONG, William S – El Libro de los Derechos de Autor, Cuarta Edición, Editorial Heliasta SRL, Buenos Aires, 1995.

TRABALLINI de AZCONA, Mónica - Delitos contra la propiedad intelectual, Editorial Mediterránea, 2004.

UNITED STATES CONGRESS, House. Committee on the Judiciary, WIPO Copyright Treaties Implementation Act; And Online Copyright Liability Limitation Act: Hearing before the Subcommittee on Courts and Intellectual Property, 105th Congress, 1st Session, 16, 17 January 1997.

UNITED STATES CONGRESS, United States Information Infrastructure Task Force, Working Group on Intellectual Property Rights. Intellectual Property and the National Information Infrastructure. Washington, D.C.: U.S. Patent and Trademark Office, 1995.

VALDES OTERO, Estanislao - Derechos de autor: régimen jurídico uruguayo, Biblioteca de publicaciones oficiales de la Facultad de Derecho y Ciencias Sociales de la Universidad de la República, Montevideo 1953

VIBES, Federico Pablo – El Impacto de Internet en la Propiedad Intelectual, LL 2002-1106.

VIBES, Federico Pablo – Derecho de Autor. Entorno digital y copia privada, LL 2006-F-771.

VILLALBA, Carlos A. – Actualidad en la Jurisprudencia sobre Derecho de Autor, LL, 1996-D-1107.

VILLALBA, Carlos A. - Derecho del productor de fonogramas. Estado de la Jurisprudencia, ED 125-455.

VILLALBA, Carlos A. - El derecho de ejecución de música grabada, LL 1987-B-12.

VILLALBA, Carlos A. - El denominado contrato de edición musical. Los contratos en la ley de propiedad intelectual, LL 1990-A-551.

VILLALBA, Carlos A. - Análisis de la jurisprudencia en materia de derechos de autor. LL 1995-C-557.

VILLALBA, Carlos A. – Ratificación de varios tratados. Derechos de Autor y Derecho de los Intérpretes y los Productores de Fonogramas, LL 1999-F-1168.

WEGBRAIT, Pablo – Empresas Fonográficas e Intérpretes, LL 2007-F-703.

BIG DATA: A LA BÚSQUEDA DEL EQUILIBRIO CON LOS DD.HH.

Por: ***Marcelo Bauzá R.***
Uruguay

1. BIG DATA: ¿UN TEMA NUEVO?

La primera vez que escuché hablar del Big Data en forma sustancial y directa, fue en la 34ava. Conferencia Anual de Autoridades de Protección de Datos y Privacidad, celebrada en Punta del Este (Uruguay) durante unos literalmente tormentosos días de octubre de 2012 (un inusitado ciclón se abatió durante esos mismos días sobre el conocido balneario costero de mi país).

Varios expertos intervinientes en el importante evento, por lo general provenientes del ámbito anglosajón (Brad Smith, Cristopher Wolf…), acercaron a esta región las últimas cuestiones tecnológico-sociales incidentes en la protección de datos personales, novedosas al menos para mí y que me hicieron ebullir la mente.

Entre tales cuestiones figuraba este tema, de importancia creciente ya en aquél entonces, tanto que determinó que una de las Declaraciones oficiales de la Conferencia se detuviera en el asunto[1], aunque aún en forma tangencial, esto es en relación con una de sus más ostensibles vinculaciones, no la única por cierto (el perfilamiento o *profiling*), aludiendo a ventajas y riesgos al mismo tiempo:

We recognize the many useful applications of big data and the advantages large data collections could bring to, among others, healthcare, energy efficiency and public safety. However, at the same time the collection of personal information into large databases and the subsequent use presents risks to the protection of personal data and privacy. This is especially the case if large data collections are used for analysis and profiling in order to, among others, carry out risk analyses, which help organizations and companies to target persons.[2]

[1] "Uruguay Declaration on profiling "– Punta del Este-Maldonado / Juanicó-Canelones, Uruguay – 26 October 2012. [última consulta: 13 julio 2018]. Disponible en https://edps.europa.eu/sites/edp/files/publication/12-10-26_uruguay_declaration_profiling_en.pdf. Habría que esperar un par de años más, para que en 2014 la misma Conferencia en su edición 36° compusiera una Resolución sobre el mismo tema, ahora de lleno, cuyo comentario exhaustivo desarrollamos más adelante. [última consulta: 13 julio 2018]. Disponible en https://www.datospersonales.gub.uy/inicio/institucional/noticias/resoluciones+adoptadas+en+la+36+conferencia+internacional+de+autoridades+de+proteccion+de+datos+y+privacidad

[2] Traducción libre no oficial: "Reconocemos las muchas aplicaciones útiles de *big data* y las ventajas que las grandes colecciones de datos podrían aportar, entre otros, a la asistencia sanitaria, la eficiencia energética y la seguridad pública. Sin embargo, al mismo tiempo, la recopilación de información personal en grandes bases de datos y el uso posterior presenta riesgos para la protección de los datos personales y la privacidad. Este es especialmente el caso si se utilizan grandes recopilaciones de datos para el análisis y la elaboración de perfiles con el fin, entre otros, de llevar a cabo análisis de riesgos, que ayudan a las organizaciones y empresas a enfocarse en las personas."

De aquéllos años a hoy, la búsqueda del manido "equilibrio" continuó renovada y vigente[3]. En el devenir transcurrido, el crecimiento y la importancia de esta nueva tecnología han sido exponenciales. Como todo lo que históricamente ha venido sucediendo en materia de TIC desde su aparición a nuestros días.

Cabe sostener que esta tecnología configura en la actualidad la punta de vanguardia del llamado *Yo digital* (o *Personalidad virtual*), donde son los algoritmos matemáticos predictivos los que terminan por señalar, a los más diversos fines, lo que se considera que somos y las singularidades de conducta y personalidad (supuestas o reales) que derivan de nuestro accionar social. Lo cual arrostra la vulnerabilidad de todas las personas, en cuanto a su privacidad y no discriminación. La interacción con las redes y buscadores, permite llegar a una generación de perfiles de conducta muy afinados. El reciente caso de Cambridge Analytics y la utilización predictiva de datos masivos de los usuarios de Facebook, demuestra tanto la factibilidad y alto valor de esta técnica, como sus riesgos y la afrenta directa con la privacidad y el derecho autónomo de protección de datos personales, si no se la coloca bajo controles y exigencias adecuados.

No somos afectos, tampoco formados, a manejar cifras ni enfoques de pura economía o tecnología. Los medios y las innumerables pero a la vez facilitadoras fuentes de consulta, se encargan de ello. Tal afirmación no nos impide acordar o reflexionar sobre soluciones nunca totales pero sí novedosas, que podrían contribuir a domeñar el fenómeno. En ese sentido apreciamos que "la digitalización y por tanto el generar datos se considera el ´nuevo petróleo´, el contexto a través del cual se genera esta información es ahora el nuevo yacimiento del petróleo, con las industrias haciendo su mejor esfuerzo por controlar territorios para perforar su búsqueda y obtener mayores dividendos digitales" (BECERRIL, 2016).

A partir de la expresada premisa, la citada autora nos pone por delante un interesante desafío: la necesidad de que sean no solamente las empresas IT las que se beneficien del mercado del Big Data, dándoles poco y nada a cambio a los internautas que van dejando sus trazos digitales, poniéndole un valor de contraprestación. Sin desconocer la dificultad de cuantificar este tipo de elementos, la autora acompaña con cifras y afirmaciones muy sustantivos un planteo de ponerle valor a nuestra información personal; incluso alude con pormenores a una persona de nombre Shawn Bucles que en el año 2014 lo hizo En otras palabras, si el Big Data es negocio, que lo sea para todos, y no para unos pocos.

2. Y SIN EMBARGO, SE CONSTATA UN DERROTERO

Desde un punto de vista sencillo, pero entiendo que inatacable y útil, cabe sostener que Big Data, no es sino una consecuencia evolutiva natural, casi que normal se podría decir, del

[3] De hecho, el lema de la 34ª Conferencia del 212 fue "Privacidad y Tecnología en Equilibrio". Incluso aún hoy está disponible por Internet el Libro Digital de la Conferencia bajo el mismo título (ver referencia bibliográfica). Los tiempos avanzan, y los desafíos –incluso los jurídicos- siendo una constante. No es ajeno a esta evocación en paralelo, el título elegido para la presente ponencia. La necesidad de buscar "equilibrios" entre las TIC y los DD.HH., e incluso entre estos últimos desplegados en contextos de TIC, ha sido puesta de manifiesto por numerosos estudiosos, entre otros Carlos DELPIAZZO (ver "bibliografía").

desarrollo incesante de las TIC. No hay que ser augur para darse cuenta que todo hacía prever que este nuevo modo o dimensión de tratar los datos (no personales y personales), advendría a poco que la tecnología lo permitiese. Por lo tanto, todo lo que contribuya a su adecuación con otros valores y derechos en juego, es de orden que se ponga en juego.

La realidad muestra que el avance de esta técnica en el ámbito de las empresas e instituciones, es un hecho incontenible. No debe desconocerse esa realidad, por el contrario se la debe analizar asimilar en sus contornos y contenidos. Para luego apuntar a las zonas de confluencia del fenómeno con lo benéfico, y también con lo nocivo que representan para los DD.HH. De eso se trata cuando se pretenden y buscan los equilibrios entre la Tecnología y el Derecho, sin olvidar los valores éticos que dan basamento a ambos polos.

La explotación de datos en términos de Big Data, es un fenómeno que aparece a principios de la década del 2000, donde la gran cantidad de fuentes diversas de generación y gestión de información digital, junto con la explosión incontenible de e-móvil, hacen saltar por los aires los dispositivos y técnicas tradicionales del tratamiento de los datos (Política Nacional… Colombia, 2018 ref. ampliada en "Bibliografía).

A partir de ese momento la recolección deja de ser exclusivamente selectiva y de datos estructurados, pasando a desafiar los sistemas clásicos por medio de las conocidas 3V a que referiremos más adelante.

En 2005 aparece el primer software especialmente concebido para el almacenamiento y explotación de datos digitales de naturaleza originaria diversa (audio, textos sin estructura, videos). Las nuevas formas de almacenamiento, procesamiento, análisis y visualización, colocan el tratamiento de la información digital una nueva escala, dando pie al uso extendido del término Big Data.

Y al potencial tecnológico se le suma, la capacidad de generar valor social y económico apoyados en esta tecnología, lo que a la postre la posiciona como "un nuevo factor de producción". Esto, unido a la identificación del potencial de los datos en clave masiva para generar valor social y económico, la posicionó como un nuevo factor de producción, al servicio de la creación de nuevos bienes, servicios y procesos, así como mejorar los existentes.

El documento gubernamental colombiano, advierte sobre el carácter relativo de las referencias técnicas al mayor volumen, variedad y velocidad, puesto que lo que hasta ayer era enorme hoy dejó de serlo. Y culmina afirmando que el reto o desafío ya no está en la tecnología y el almacenamiento, sino en la definición de las condiciones de mejor aprovechamiento de una masa inusitadamente grande de información, traducida a términos de políticas públicas como centro de una economía digital.

3. DEFINICIONES Y DIMENSIONES

Es claro, entonces, que estamos ante una de las tendencias más específicas y propias del constante avance de las TIC, en ese caso "…consistente en almacenar, procesar y analizar

cantidades masivas de datos con la finalidad de obtener, con carácter predictivo, información concreta, relevante y fiable" (CRESPO GARCÍA, 2016).

Por ende, cuando se habla de Big Data ("datos grandes" en traducción literal), se está pensando en un gran conjunto de datos, que por su tamaño excede toda capacidad de captura, almacenado, gestión y análisis mediante herramientas informáticas tradicionales (los programas de "bases de datos" para facilitar el entendimiento común).

Como bien se señala en las Directrices del Consejo de Europa específicas al tema y referenciadas en la bibliografía de la presente ponencia, la definición pertinente debe incluir no solamente la caracterización de los datos, sino también su capacidad o función predictiva, el llamado "Big Data analytics", que identifica "tecnologías informáticas que analizan grandes cantidades de datos para descubrir patrones ocultos, tendencias y correlaciones".

Siempre abundando en esta faz predictiva, el mismo documento cita la definición de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea, en tanto "refiere a todo el ciclo de la gestión de datos al recolectar, organizar y analizar datos para descubrir patrones, inferir situaciones o para predecir y entender comportamientos (ENISA. 2015. Privacidad desde la concepción en los Big Data. Descripción general de las tecnologías que fomentan la privacidad en tiempos de Big Data analytics)".

Se dice que con Internet ha cambiado todo. Técnica y socialmente es así. Para entender realmente la especial influencia de este cambio sobre la gestión de datos, hay que pensar que en tiempos precedentes las empresas manejaban y controlaban la producción y tratamiento de su información. Pero hoy día ya no sucede de ese modo, porque la tecnología habilita que, tanto usuarios como máquinas, generen y adicionen sus propios datos y procesos, sumándolos a lo ya existente de otro origen. De esta manera, se va formando un volumen progresivo, un volumen de datos en constante, rápido y variado crecimiento, que escapa al control y organización de la propia entidad que diera inicio al ciclo.

Concomitante con esta nueva dimensión, emerge un mercado de profesionales gestores de este tipo de tecnología, que antes tampoco existía. Lógicamente ello ocurre, ante la dificultad de procesar tal tipo de datos (por volumen, velocidad y variedad), de parte de los informáticos habitualmente formados en conocimientos y técnicas insuficientes para ello.

En un primer momento se aludía a las 3 V como paradigma de esta tecnología (volumen, velocidad, variedad). Pero hoy día se amplía el elenco a 5 V. Siguiendo nuevamente a Pilar CRESPO GARCÍA, se trata de los siguientes atributos:

1) El *Volumen*, que remite a la característica más notable de esta tecnología, en tanto supone la disponibilidad de una cantidad inusitada de datos.

2) La *Velocidad* en todas las fases por las que transitan los datos, o sea su capación, procesamiento y análisis en tiempo real, reduciendo los períodos de latencia.

3) La *Variedad* en cuanto a la tipología (alfanuméricos, fechas, etc.), y origen de los datos, que bien pueden ser estructurados como no, así como generados por personas, por derivaciones automáticas a partir del impulso de aquéllas (transacciones, navegación

web, etc.), o incluso ingenios tecnológicos (*Machine to Machine*, lectores de códigos o caracteres biométricos, etc.).

4) La *Veracidad* que obviamente siempre está presente en relación directa con el aumento de la masividad de los datos, haciendo necesario tareas de filtrado que preserven la fiabilidad y calidad de los mismos.

5) El *Valor* en tanto objetivo último y fundamental de esta tecnología, que más que apuntar al volumen por sí mismo, lo hace a la extracción de riqueza analítica del conjunto, verificable en la fase de "predicción" (suficiencia de la interrogación sobre el conjunto, para obtener respuestas adecuadas).

4. ESCENARIOS Y APLICACIONES DE LA BIG DATA

Los escenarios y aplicaciones en los que el Big Data se presenta como útil (no necesariamente alineado al interés general en todos los casos), son numerosos y significativos (PULIDO CAÑABATE, E. 2014; COLMAREJO FERNÁNDEZ, 2017).

En apretado catálogo repasamos:

- Prevención, detección e investigación de actividades terroristas y delincuencia.
- Salud y atención sanitaria (medicina predictiva anticipativa de la enfermedad con base en perfiles genéticos del paciente o población involucrados).
- Ciencia, con ejemplos preclaros como el Bosón de Higgs o la secuenciación del genoma humano.
- Los proyectos de "ciudades inteligentes" *(smart cities)*, donde se mejora la gestión de los servicios públicos a partir del análisis de hábitos de los ciudadanos.
- El *Business Intelligence* empresarial, entre otros contenidos apoyado en la publicidad personalizada y anticipativa.
- Los programas de ayuda humanitaria, la propagación de enfermedades, los fenómenos migratorios, la gestión de situaciones de crisis política y social (¿seguimiento de manifestantes?).

Bajo un punto de vista funcional, resulta ilustrativo en el enfoque de quien clasifica las aplicaciones de Big Data según objetivos (no exhaustivos), todos ellos tendientes a "prever posibles pautas de comportamiento de una persona o grupo de personas" (MORTE FERRER, 2017):

" - Analizar la posibilidad de un comportamiento determinado en relación con diferentes tipos de contratos (*scoring*).
- Acumular datos en principio inconexos con el fin de crear un perfil detallado de una persona o de un grupo de personas (*profiling*).
- Valorar diferentes características de una persona, como pueden ser su estado de salud, sus gustos o su fiabilidad (*personalizing*).

- Seguir a una persona en base al rastro que deja, por ejemplo en Internet (*tracking*).”

El mismo autor concluye luego de esta clasificación, que “parece evidente que estas actividades traen consigo diferentes riesgos, [por lo que] algunos autores hablan de una “dictadura *smart*” (Weltzer, 2016) en base a esos riesgos y al grado de desarrollo que algunas tecnologías están alcanzando”. Y agrega finalmente: “Conviene recordar que muchas de esas tecnologías han sido ya implementadas sin que se hayan llevado a cabo estudios previos sobre los posibles peligros para los derechos fundamentales y sin que existan políticas adecuadas de seguridad informática para esas nuevas aplicaciones y productos”.

5. LA PARADOJA DE LA TRANSPARENCIA

Una de las exigencias de catálogo de la Protección de Datos Personales más difíciles de cumplir en contextos de Big Data, es la relacionada con el consentimiento informado del titular de los datos personales.

La información personal tratada y accesada por Internet, tiene una particularidad singular, tan penosa como comprobable: muy pocas personas leen las condiciones comprometidas para su colecta y tratamiento, y las que lo hacen entienden poco y nada de ello, pasando por alto rápidamente el aviso respectivo y autorizando sin más este uso.

Las causas de esta realidad son numerosas, uno de ellos de importancia: el común de la gente no entiende el significado de estos avisos. A partir de lo cual parece necesario dotar estos avisos de un lenguaje más sencillo. Pero la sencillez va de la mano con la pérdida de precisión. Esto es lo que ha sido denominado como la “paradoja de la transparencia” acuñada por los expertos Barrocas y Nissebaum: a mayor simplicidad y claridad, mayor pérdida de precisión en el mensaje; y por ende un mayor alejamiento de un consentimiento plausiblemente informado para obtener y tratar los datos

La interrogante aflora con fuerte dramatismo según lo ha dicho sin la doctrina: “Lo dicho hasta ahora nos hace preguntarnos ¿cómo ha de ser redactada la información para que los usuarios puedan otorgar su consentimiento informado? El funcionamiento del *big data* hace que esta tarea sea tremendamente difícil, por cuanto los datos se mueven de un lugar a otro, y de un receptor a otro de modo impredecible, ya que el valor de los datos no se conoce en el momento en que son recogidos. Así, el consentimiento se parece cada vez más a un cheque en blanco” (GIL GONZÁLEZ, 2016). Y no parece haber respuestas ni soluciones unilaterales.

Se habla también de otros factores que contribuyen a agravar más aún este panorama crítico relativo al consentimiento, piedra angular de todo el sistema jurídico en la materia. En primer lugar, porque “la cadena de emisores y receptores de datos es potencialmente infinita, e incluye actores e instituciones cuyo rol y responsabilidades no están delimitados o comprendidos” con lo cual “la cesión de datos puede llegar a ser relativamente oscura”. Y en segundo lugar no menos importante, la llamada “tiranía de la minoría” que hace que se perfilen y tomen decisiones sobre la mayoría de titulares de datos (los que no leen o no entienden las condiciones previas de tratamiento) en base a la recolección de datos

pertenecientes a la minoría que sí los entiende y se ha informado de ello en forma oportuna y correcta (GIL GONZÁLEZ, 2016).

6. LA INTERVENCIÓN DE LA ÉTICA

Hoy día me atrevo a percibir una especie de repristinación urgida del foco de atención ético de las TIC, con una consecuente reflexión en profundidad, a partir del Big Data (al que se suma el IoT).

El mundo de los valores, que nunca fue ajeno al decurso temporal de las TIC (ni tampoco al Derecho en tanto ciencia y praxis), va enfrentando dilemas cambiantes según el estado evolutivo de la técnica. Por lo cual, se ha podido afirmar lo siguiente: "El tamaño y omnipresencia de estas grandes colecciones de datos están forzando nuevas cuestiones relacionadas con nuestra identidad, los cambios en nuestra valoración de la privacidad y la intimidad, el significado real de poseer/controlar datos propios y ajenos, y sobre cómo gestionamos nuestra reputación, tanto en modo *online* como *offline*, una vez asumido que nuestros datos *online* no solo la afectan sino que de hecho la moldean y conforman cada día". Para rematar en que "Existe, por tanto, una necesidad académica, profesional y ciudadana de confrontar los problemas que surgen de este espacio de intersección, pues es en este espacio donde se están conformando las sociedades del siglo XXI" (COLMAREJO FERNÁNDEZ, 2017).

La amplitud cuanto la importancia del fenómeno en términos jurídicos se advierten al señalarse con contundencia que "Es evidente que la privacidad es quizás el problema más acuciante en lo que respecta a BD y derechos civiles (Easton-Calabria; Allen, 2015)". Y más aún cuando a renglón seguido se concluye que "Esto debería ser razón suficiente para que los gobiernos garanticen el desarrollo y aprobación de nuevos sistemas de leyes, o bien se diseñen nuevas tecnologías que ayuden a prevenir la destrucción de nuestras valiosas reglas de civilización, al mismo tiempo que se garantiza que la evolución de *big data* enriquece nuestras vidas tanto social como individualmente".

Como de sólito, no existen soluciones parciales a los fenómenos de riesgo que presentan las TIC para la sociedad en su conjunto. Partimos de la base que el problema de la gestión de la privacidad en contextos de Big Data, para ser justa y equitativa exige una "inteligente combinación entre ética, ley y decisiones políticas", y que "ninguna de ellas por sí sola será capaz de confrontar un problema tan complejo como el que abordamos, necesariamente de un modo superficial". (COLMAREJO FERNÁNDEZ, 2017).

7. LOS RIESGOS DEL BIG DATA Y SU ENFOQUE EN CLAVE JURÍDICA

El Supervisor Europeo de la Protección de Datos, ha señalado dos riesgos específicos del Big Data, a saber la "falta de transparencia", y el "desequilibrio en la información entre personas y empresas".[4]

[4] Supervisor Europeo de Protección de Datos / Opinion 7/2015 Meeting the challenges of Big Data / 19 de noviembre de 2015.

Sobre el primero apunta al celo de las organizaciones, que tienden a no revelar los resultados de sus tratamientos de información como parte de su know-how, lo que puede conducir a que los ciudadanos no sepan realmente qué ocurre con sus datos una vez facilitados.

Y en cuanto a lo segundo, es una tendencia en aumento que el Big Data favorece, por cuanto las empresas tomarán decisiones relevantes y que afectan a quienes dieron sus datos (consumidores transformados en "prosumers"), en base a los análisis predictivos de conductas masivas en el mercado.

Por su parte, la Agencia Española de Protección de Datos ha puesto el acento en aspectos tales como:[5]

- los tratamientos basados en predicciones y utilizados en forma discriminatoria excluyendo a los sectores minoritarios de los resultados concluidos (la llamada "dictadura de los datos);
- la afectación de sectores poblacionales vulnerables (menores, ancianos, colectivos marginados);
- las dificultades derivadas del origen y procedencia de la información, no siempre proveniente de fuentes propias sino también de terceros, y su uso por diferentes figuras (responsables y encargados de tratamientos);
- las cuestiones que derivan de los plazos de conservación y retención de datos, así como el uso y reutilización disociados de los datos disociados;
- los riesgos y amenazas que imponen aspectos técnicos y de seguridad, (entre otros las medidas reforzadas frente al riesgo de reidentificación de la información originariamente anónima, o el uso del *cloud computing*, en los tratamientos de Big Data).

8. LAS TENDENCIAS ACTUALES

8.1. Comentarios introductorios

Debemos acostumbrarnos a que no existen fórmulas únicas que hagan del fenómeno Big Data un asunto totalmente controlado o controlable, por el Derecho.

Ya lo hemos dicho antes: se trata de apelar a una combinatoria de políticas públicas, revaloraciones o puestas en práctica de códigos de conducta (el factor ético entra mayormente por aquí), y finalmente *last but not least* la norma jurídica, en muchos casos representada por textos de *soft law.*

Esta tríada no es ajena a prácticamente la totalidad de fenómenos constatables en la sociedad, a la hora poner el acento de los dispositivos y conductas comunicativas sustentados en TIC.

Llegados a este punto abordaremos algunos documentos que buscan encuadrar la legitimidad del Big Data. No sin antes apreciar, que la mayor parte de los modelos a estatuir (normas, directrices, guías de actuación…) encuentran hoy día sustento o inspiración en el Reglamento

[5] Ver en Bibliografía, Agencia Española de Protección de Datos: "Código de buenas prácticas…".

General de Protección de Datos aprobado por la Unión Europea el 18 de abril de 2016, y plenamente aplicable a partir del 25 de mayo de 2018.

Un Reglamento Europeo que, nos apresuramos a aclarar, no contiene previsiones específicas sobre Big Data, pero que –de todos modos- dispone de una caja de herramientas bastante precisa y perfectamente aplicable, posiblemente suficiente como para encuadrar el tema. Entre otros aspectos, porque, bien se ha afirmado, el RGPD dispone de "dos elementos de carácter general [que] constituyen la mayor innovación del RGPD para los responsables y se proyectan sobre todas las obligaciones de las organizaciones: el principio de responsabilidad proactiva, y el enfoque de riesgo" (AGENCIAS ESPAÑOLAS DE PROTECCIÓN DE DATOS, 2014).

En particular el art. 35 del RGPD (Evaluación de impacto relativa a la protección de datos), resulta ampliamente aplicable a la especie, cuando presta especial atención a las "nuevas tecnologías [que], por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas…" (núm. 1). Y sobre todo los numerales 3 y 4 del mismo artículo, que aluden a la obligatoriedad de la evaluación de impacto, cuando se trata de "elaboración de perfiles…" y "tratamientos a gran escala…" de datos sensibles, imponiendo a las autoridades de control el establecimiento y publicación de una lista de tipos de operaciones de tratamiento que requieran este tipo de evaluaciones.

De consuno con el mismo criterio del RGPD, los "Estándares de Protección de Datos Personales para los Estados Iberoamericanos", disponen en su art. 41 la realización de evaluaciones de impacto cuando "se pretenda llevar a cabo un tipo de tratamiento de datos personales que, por su naturaleza, alcance, contexto finalidades, sea probable que entrañe un alto riesgo de afectación del derecho a la protección de datos personales de los titulares", remitiendo a las legislaciones nacionales la especificación de los casos en que ocurra tal necesidad y demás previsiones necesarias.

8.2. La Resolución sobre Big Data adoptada por la 36° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (2014).

Por su carácter si se quiere precursor en la materia, vale la pena mencionar en forma sintética este documento que realiza un llamado a todas las partes que utilizan el Big Data para:

1. Respetar el principio de especificación de finalidad.

2. Limitar la recolección y almacenamiento a niveles de necesidad con el propósito legítimo pretendido.

3. Obtener "cuando sea apropiado" (sic) el consentimiento válido del titular de los datos, afines de análisis y creación de perfiles.

4. Ser transparentes (qué información se recolecta, cómo se procesa, con qué propósito se utilizará, y si será transferida terceros).

5. Dar acceso y posibilidades de corrección de la información.

6. Ofrecer acceso "cuando sea apropiado" (sic) a los insumos principales y criterios de toma de decisiones (algoritmos).

7. Llevar a cabo una evaluación de impacto en la privacidad, especialmente si la técnica de Big Data implica usos novedosos o inesperados de los datos personales.

8. Desarrollar y utilizar la "privacidad por diseño" en contextos de Big Data.

9. Considerar la utilización de datos anónimos siempre que mejoren la protección de la privacidad.

10. Cuidado al compartir o publicar conjuntos de datos con seudónimos o identificables indirectamente.

11. Demostración del carácter justo, transparente y responsable del uso del Big Data (valoración y revisiones continuas, tanto de los perfiles logrados como de los algoritmos empleados para ello; evitar falsos positivos o falsos negativos; disponibilidad continua de valoraciones manuales de los resultados).

8.3. Las Directrices sobre la Protección de las Personas en relación con el tratamiento de datos de carácter personal en un mundo con Big Data (2017)

Se trata de 9 Directrices articuladas en un documento emergente del Concejo de Europa, y dirigido a los países signatarios del Convenio 108 (entre los que cabe recordar figura Uruguay), donde se aborda la temática bajo varios sesgos o pautas.

Luego de una "Introducción" y una especificación de la "Terminología" a utilizar en las Directrices (Big Data, Controlador, Procesador…), se abordan propiamente los principios y directrices", en los siguientes términos:

1. Utilización de datos con ética y conciencia social, evitando la entrada en conflicto con los valores generalmente aceptados y no perjudicando los intereses de la sociedad, ni de los propios valores y normas, incluida la protección de los derechos humanos, recogidos en las cartas internacionales.

   En este mismo punto, y cuando se determine un alto impacto del uso de los Big Data sobre los valores éticos, se establece que los controladores podrán establecer un comité de ética independiente *ad hoc*, o utilizar otros ya existentes, a efectos de identificar tales valores y preservarlos.

2. Adopción de Políticas preventivas y evaluación de riesgos (análisis de impacto), apelando a la prudencia dada la creciente complejidad del tratamiento de datos y los usos transformativos de los Big Data, y abarcando aspectos que trascienden la privacidad y la protección de datos individuales (dimensión colectiva de estos derechos, como el derecho de igualdad de trato y no discriminación).

3. Participación de las partes interesadas en estos procesos de evaluación y diseño de tratamientos, o sea de las personas y grupos potencialmente afectados por el uso de Big Data. Y consideración de las medidas adoptadas por los controladores con el fin de mitigar riesgos, entre otros aspectos, al momento de evaluar posibles sanciones administrativas.

4. Limitación de la finalidad y transparencia, evitando los cambios no esperados, inadecuados u objetables de cualquier modo, que supongan la aparición de riesgos mayores a los contemplados al fijar las finalidades iniciales.

5. Atención al principio de transparencia, traducible en la disponibilidad pública de los resultados de la evaluación de impacto, salvo que se trate de información confidencial, que el controlador deber a incluir en anexo aparte del informe de evaluación, y que no siendo público, no obstante podrá ser accedido por las autoridades de control.

6. Enfoque desde la concepción. Se trata de las conocidas técnicas de "privacidad por diseño" y "por defecto", de necesaria contemplación por los controladores y los procesadores cuando corresponda, a fin de minimizar la presencia de datos redundantes o marginales, evitar potenciales datos sesgados ocultos, y riesgos de discriminación o impacto negativo sobre derechos y libertades fundamentales de los titulares de los datos, tanto en etapa de recolección como de análisis.

7. Utilización de simulaciones antes de pasar a los tratamientos de gran escala, permitiendo así contar con análisis y pruebas previos, identificatorios de futuros riesgos. Especial atención al uso de datos sensibles y medidas como seudonimización, estas últimas que no eximen de la aplicación de los principios de protección de datos correspondientes..

8. Consentimiento libre, específico, informado e inambiguo, fundado en la información proporcionada al titular de los datos de conformidad con el principio de transparencia de tratamiento de Big Data, que incluirá exhaustivamente el resultado del proceso de evaluación, con facultativos enfoques de aprendizaje a través de la experiencia proporcionada por un simulador de efectos.

9. Existencia de recursos técnicos simples y fáciles de utilizar para que los titulares de los datos puedan reaccionar ante tratamientos incompatibles y retirar su consentimiento. Demostración de inexistencia de desequilibrios que afecte el consentimiento, por parte del controlador.

10. Anonimización, con expresa atención al riesgo de reidentificación en función del tiempo, esfuerzo y recursos necesarios para ello, exigiéndosele al controlador la debida adecuación de las medidas tomadas a tales fines.

11. Salvaguarda de la autonomía de la intervención humana en los procesos de toma de decisiones afincados en Big Data, pudiendo y debiendo dicha intervención alejarse de las recomendaciones emanadas del Big Data. Y asimismo quedando a resguardo el derecho de los afectados por una decisión fundamentada en Big Data, a impugnarla ante la autoridad competente.

12. 8. Especial atención a las Políticas de Datos Abiertos por las entidades públicas y privadas, dado que la disponibilidad de las herramientas predictivas en la materia (Big Data Analytics), hacen de aquéllos uno de los yacimientos preferidos para inferir información sobre personas y grupos.

13. Lo que lleva a sumar la exigencia de que, en los análisis de impacto respectivos, se incluyan los efectos de la fusión y minería de datos, pertenecientes a conjuntos diversos pero de plausible conexión.

14. 9. Consideración de la información y la alfabetización digital como una habilidad educativa esencial, que ayude a las personas en la comprensión de las implicancias del uso de los datos personales bajo el contexto de los Big Data.

BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AGPD). *Código de buenas prácticas en protección de datos para proyectos Big Data.* [En línea: última consulta 13 julio 2018]. Disponible en https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf

AGENCIAS ESPAÑOLAS DE PROTECCIÓN DE DATOS (AGPD-APDCAT-DATUAT BABESTEKA). *Guía del Tratamiento de Protección de Datos para el Responsable del Tratamiento.* AEPD 2014. [En línea: última consulta 13 julio 2018]. Disponible en https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf

BAUZÁ, Marcelo. "La protección de datos personales y su armonización con otros derechos y las políticas de e-gobierno", pág. 53, en *"Derechos Humanos y Protección de Datos Personales en el Siglo XX. Homenaje a Cinta Castillo Jiménez",* AA.VV., obra colectiva dirigida y editada por Álvaro Sánchez Bravo, ed. Punto Rojo, España, 2013.

BAUZÁ, Marcelo. "La Ley 18.331 y el Reglamento (UE) 2016/679". En *Revista Uruguaya de Protección de Datos Personales* Número 2, agosto 2017, págs. 9 a 23. Asimismo en línea, en el sitio de la URCDP uruguaya https://www.datospersonales.gub.uy/

BECERRIL, Anahiby. El Valor de nuestros datos personales en la era Big Data e IoT. En *Hacia una Justicia 2.0: Actas del XX Congreso Iberoamericano de Derecho e Informática.* Salamanca: Ratio Legis Ediciones, 2016, pp. 27-40. (ISB N: 978-84-16324-43-9).

COLMAREJO FERNÁNDEZ, Rosa. *Una ética para big data: Introducción a la gestión ética de datos masivos*. Barcelona: UOC, 2017. (ISBN: 978-84-9116-940-6).

CRESPO GARCÍA, Pilar. El impacto del Big Data en los derechos fundamentales de las personas. En: *Fodertics 5.0. Estudios sobre nuevas tecnologías y Justicia.* Granada: Editorial Comares, 2016, pp. 13-23. (ISBN: 978-84-9045-463-3).

DELPIAZZO, Carlos. *A la búsqueda del equilibrio entre privacidad y acceso.* [En línea: última consulta 13 julio 2018]. Disponible en https://docplayer.es/7112746-A-la-busqueda-del-equilibrio-entre-privacidad-y-acceso.html

DEPARTAMENTO NACIONAL DE PLANEACIÓN – MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO. Política Nacional de

Explotación de Datos (Big Data). Versión aprobada. *Documento Conpes 3920*. Bogotá, 2018. [En línea: última consulta 13 julio 2018]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3920.pdf

GIL GONZÁLEZ, Elena. *Big data, privacidad y protección de datos*. XIX Edición del Premio Protección de datos Personales de Investigación de la Agencia Española de Protección de Datos. Madrid: Agencia Española de Protección de Datos – Agencia Estatal Boletín Oficial del Estado, 2016. (ISBN: 978-84-340-2309-3) [En línea: última consulta 13 julio 2018]. Disponible en file:///C:/Users/Marcelo/Downloads/documentop.com_big-data-privacidad-y-proteccion-de-datos_5a152a3a1723dde519dc9834.pdf

GRANERO, Horacio Roberto. Smart Cities: Hacia una reconceptualización del término privacidad por la reutilización de datos masivos (Big Data). En *Hacia una Justicia 2.0: Actas del XX Congreso Iberoamericano de Derecho e Informática.* Salamanca: Ratio Legis Ediciones, 2016, pp. 155-170. (ISBN: 978-84-16324-43-9).

MORTE FERRER, Ricardo. ¿Protección de datos/privacidad en la época del Big Data, IoT, wearables…? Sí, más que nunca. *Dilemata: Revista Internacional de Éticas Aplicadas – nro. 24-2017* [En línea: última consulta 13 julio 2018]. Disponible en https://www.dilemata.net/revista/index.php/dilemata/article/view/412000108

PULIDO CAÑABATE, Big data: ¿solución o problema?. Lección Inaugural Curso Académico 2014-2105, [En línea: última consulta 13 julio 2018]. Disponible en http://arantxa.ii.uam.es/~epulido/bigdata.pdf

RED IBEROAMERICANA DE PROTECCIÓN DE DATOS. *Estándares de Protección de Datos Personales para los Estados Iberoamericanos.* [En línea: última consulta 13 julio 2018]. Disponible en http://www.redipd.es/documentacion/common/Estandares_Esp_Con_logo_RIPD.pdf

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES. 34° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. *Privacidad y Tecnología en Equilibrio*. [En línea: última consulta 13 julio 2018]. Disponible en https://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/fea77ed6-4b1c-4e5b-b16f-128373b44792/Libro+Privacidad+y+Tecnologia+en+Equilibrio.pdf?MOD=AJPERES&CONVERT_TO=url&CACHEID=fea77ed6-4b1c-4e5b-b16f-128373b44792

UNIDAD REGULADORA Y DE CONTROL DE DATOS PERSONALES. 36ª. Conferencia Internacional de Autoridades de Protección de Datos y Privacidad [En línea: última consulta 13 julio 2018] Disponible en https://www.datospersonales.gub.uy/wps/wcm/connect/urcdp/5f1a6646-fdc7-49c9-9a15-c83ba9d5a7b7/Resoluci%C3%B3n-Big-Data.pdf?MOD=AJPERES

PROPUESTA DE CRITERIOS TÉCNICOS Y LEGALES PARA RESPONDER A LA VULNERABILIDAD DE INTERNET DE LAS COSAS

Por: ***Bibiana Luz Clara,***
Esteban Rivetti,
Álvaro Gamarra,
José Aráoz Fleming,
H. Beatriz P. de Gallo
Argentina

1. MARCO CONCEPTUAL

A fin de introducir al lector en la temática que se trata en este trabajo, cabe describir brevemente las dos áreas de estudio involucradas: Internet de las Cosas y Forensia Digital.

1.1 INTERNET DE LAS COSAS (IoT)

En la bibliografía consultada se encontraron múltiples definiciones de IoT, según sea el contexto en el cual se estudia. Si bien la mayoría de los autores definen IoT desde el punto de vista tecnológico, cabe considerar aquí la definición de Joyanes Aguilar et al [1] que indica que IoT es "*... la interconexión de entidades de red altamente heterogéneas con redes, siguiendo un número de patrones de comunicación como: humano-humano (H2H), humano-cosa (H2T), cosa-cosa/T2T) o cosa-cosas (T2Ts)*". A partir de los conceptos de comunicación máquina a máquina, Internet de las Cosas (IoT) también se puede definir como "*…un conjunto de tecnologías enfocadas a permitir la conexión de objetos heterogéneos a través de diferentes redes y métodos de comunicación; su principal objetivo es posicionar dispositivos inteligentes en diferentes lugares para capturar, guardar y administrar información para que ésta sea accesible a las personas desde cualquier parte del mundo…*"[2].

Por su parte, Misra et al.[3] señalan que Internet de las cosas, no es más que la combinación en la red de varios objetos físicos con electrónica, software y conectividad de red, que permite a estos objetos físicos recolectar e intercambiar datos entre varias fuentes y destinos. La idea básica o fundamental detrás de este concepto es la presencia omnipresente a nuestro alrededor de una variedad de cosas u objetos - tales como etiquetas de identificación de radiofrecuencia (RFID), sensores, actuadores, teléfonos móviles, etc. que son capaces de interactuar entre sí y cooperar con dispositivos vecinos para alcanzar objetivos comunes.

Desde el punto de vista del usuario individual, el efecto más prominente del IoT será su *visibilidad* tanto en el ámbito laboral como en el doméstico. Uno de los puntos más preocupantes referentes al tema IoT es la *seguridad y privacidad de la información*, entendiendo que –inicialmente- el contexto de internet de las cosas se presenta como un escenario vulnerable y proclive a la invasión de la vida íntima y a la comisión de delitos contra las personas.

Desde el punto de vista de la privacidad de la información, IoT involucra a múltiples partes interesadas: individuos (el sujeto de la recolección de datos), organizaciones (que son responsables de procesar los datos recolectados de los individuos) y terceros (por ejemplo, usuarios que se benefician o usan los datos recogidos o procesados). IoT promete múltiples beneficios a todos estos interesados. Para los individuos, le proporcionaría beneficios de salud y bienestar. Para organizaciones y terceros, proporcionaría información para ofrecer mejores servicios a las personas y a la sociedad en general. Sin embargo, teniendo en cuenta la creciente tendencia a recopilar datos cada vez más íntimos y personalizados, las prácticas de recolección, manipulación y procesamiento de datos de IoT plantean muchas cuestiones relativas al impacto en la privacidad de una persona desde una perspectiva jurídica (Caron et al. [4]).

El énfasis de IoT está puesto en la estructura de comunicación que permite esta interacción entre las personas y las cosas de manera directa, es decir, sin intervención humana en el proceso de transmisión que vincula todos los componentes. Desde el punto de vista de la integración de tecnologías se puede resumir la diversidad e interactividad de IoT a partir del gráfico propuesto por el autor precitado y que se señala en la Fig. 1.

Por su parte, el informe denominado "Things Matter: The user experience of the Internet of Things in Spain" presentado por Telefónica, Accenture e Ipsos [5] distingue seis grandes entornos de IoT:

- el **vehículo conectado**, que por aplicación de la telemetría implica mayor seguridad, mantenimiento eficiente, elección de las mejores rutas de circulación y acceso, y personalización de las pólizas de seguros de acuerdo a fórmulas de manejo. En el caso de los transportes de mercaderías el monitoreo constante de las cargas permite obtener mejor información y rendimientos.

- la **industria conectada**, es el sector que más se ha volcado al uso de IoT, con una producción más eficiente y competitiva para la empresa y mayor seguridad y desarrollo profesional para los empleados.

- la **tienda conectada**, la información entre el cliente y la empresa permite el ofrecimiento de promociones personalizadas a gusto del cliente a través de la información recolectada. Se mejora la experiencia del usuario y se achican los tiempos, y los costos permitiendo negocios ágiles y mayor comodidad. Significa la posibilidad de interconectar y automatizar todas las tareas con el consiguiente ahorro de mano de obra y de tiempo, simplificando los procesos productivos monitoreándolos a distancia.

- la **ciudad conectada**, para avanzar en la gestión integral del sistema urbano que permita brindar un entorno sostenible en las ciudades. La digitalización de la administración pública también mejora la calidad de vida de los ciudadanos y fomenta la transparencia.

- la **persona conectada:** la adopción de IoT para usos individuales depende del estilo de vida del consumidor, y se relaciona más a las tendencias de ocio y divertimento. Como

ejemplo puede citarse los dispositivos para medir rendimiento deportivo y localización de mascotas. En términos generales, el uso de IoT en la esfera personal es una de las categorías que más se ha incrementado en los últimos años, principalmente por la utilización masiva de teléfonos inteligentes que ponen a disposición del usuario aplicaciones inmediatas para el acceso y control de dispositivos.

- el **hogar conectado**: relacionando la comodidad y la búsqueda de seguridad para la familia, el conjunto de componentes hogareños que permiten conectarse mediante IoT ha crecido en los últimos años, haciendo posible el monitoreo de los distintos espacios de la vivienda así como el control de gastos de consumo de energía por ejemplo.

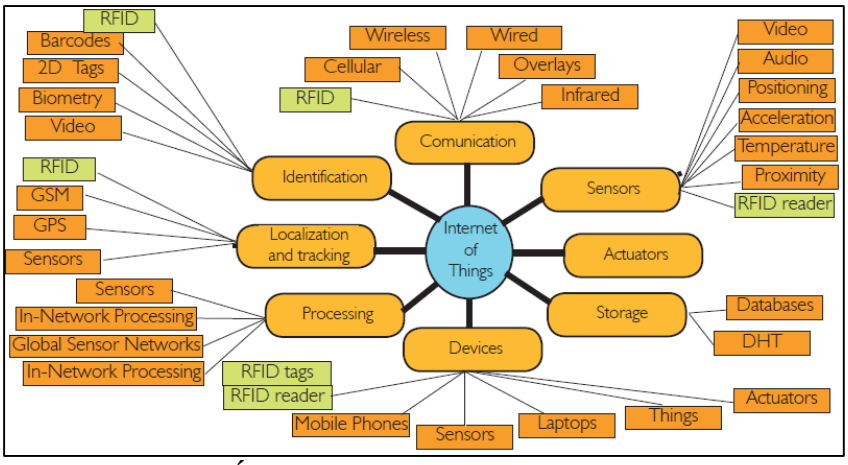


Figura 1: Categorización de Ámbitos y Tecnologías de IoT (Fte.: Joyanes Aguilar et alt ob.ct.)

Llegados a este punto es crucial hablar de la seguridad en IoT, sin la cual el sistema pierde confianza y se torna poco sostenible. Joyanes Aguilar et al. [1] destacan varias cuestiones de seguridad que deberán abordarse para hacer de IoT una tecnología segura para las personas:

- **Protocolo y seguridad de red**: la interconexión entre dispositivos de alta seguridad con otros de baja seguridad, establece un ambiente vulnerable y de fácil ingreso para las irrupciones indebidas en la red. Debería abrirse canales de comunicación mediante algoritmos criptográficos óptimos y un sistema de gestión de claves adecuado.

- **Los datos y la privacidad:** este es uno de los aspectos más sensibles respecto a la seguridad de IoT. No solo se trata de la generación de datos que cada usuario genera por sí mismo (datos de geolocalización, claves de acceso, números de teléfonos, de tarjetas de crédito, etc.) sino de la puesta a disposición de terceros o extraños de ese conjunto de datos, y ello SIN conocimiento por parte del usuario. Es posible que el propio sistema IoT adquiera información de los usuarios de manera automática. En este punto se requieren acciones tendientes a concientizar al usuario respecto de los datos que genera cada vez que se conecta a un sistema de IoT, las posibilidades de acceso indebido, el uso restrictivo de determinados servicios de la web, etc., componiendo un esquema de capacitación y culturalización en el uso de los sistemas IoT que debe ser abordado integralmente por todos los actores del sistema (proveedores de servicios, de tecnologías,

de conectividad, reguladores estatales de los servicios, normas legales de protección de datos, entre otros.).

- **Gestión de Identidad en IoT:** la gestión de identidades se refiere a la *identificación* de cada objeto de IoT, en cuando a su esencia (como ser) y su función (como servicio). Así, un objeto puede identificarse a sí mismo utilizando su identidad o sus características específicas, por ejemplo: un dispositivo que controle un determinado parámetro debe saber que el valor de ese parámetro se ajusta al usuario y su entorno específicamente. Esta visión de las cosas desde el paradigma Orientado a Objetos (POO)[1] será necesario para circunscribir la acción de cada objeto al contexto y usuario correspondiente, y en función de ello, definir los métodos de seguridad necesarios, como por ejemplo, una persona puede utilizar métodos biométricos de autenticación o un objeto dentro de una red (como un pasaporte digital o un teléfono inteligente).

- **La confianza y la gobernanza:** La confianza es fundamental para implementar IoT. Se debe definir la confianza en un ambiente dinámico y colaborativo entre todos los componentes IoT que se vinculan. Pero a esto se suma el *sentimiento de confianza* que manifieste el usuario al momento de interactuar en un sistema IoT, cuando se ve capaz de *controlar (o no) sus acciones* en el mundo virtual. Por otra parte, la gobernanza de los sistemas de IoT mediante normas de regulación legal y políticas de interoperabilidad entre los proveedores de servicios web ayudará a fortalecer la confianza en el contexto IoT, atendiendo por supuesto a no caer en la figura del "gran hermano" que todo lo ve y lo controla.

- **Tolerancia a fallos:** por supuesto que los riesgos que hoy manifiesta internet serán potenciados exponencialmente a los sistemas IoT si no se atienden debidamente. En este contexto, la tolerancia a fallos es indispensable para asegurar la confiabilidad del servicio, pero se requieren mínimamente tres acciones: a) todos los objetos debe ser seguros por si mismos tanto de hardware como de software, b) todos los objetos de IoT deberían tener la capacidad de conocer el estado de la red y sus servicios, y c) todos los objetos deberían tener la capacidad de defenderse contra fallas y ataques de intrusión.

Como observamos, esta tecnología cambia nuestra industria y por ende nuestras vidas, por lo cual será también un factor relevante adaptar la legislación a estas nuevas experiencias del modo más flexible posible, con la finalidad de que las normas no se vuelvan obsoletas antes de ser sancionadas. Focalizados en la privacidad de los datos Min et al. [6] ya advierten sobre la necesidad de que los países líderes definan políticas pertinentes y planes dirigidos a la protección de los usuarios y sus datos personales, como fundamento de la sociedad hiperconectada. Y avanzando más en este sentido, se observa también el uso de IoT en la consumación de delitos. Es decir, el contexto de ubicuidad y omnipresencia resulta atractivo para la comisión de transgresiones contra la ley, a partir de la interconectividad de

[1] Paradigma OO: proveen a los objetos como el principal medio para estructurar un sistema, en donde el mundo del problema se ve como objetos que interactúan entre así, y se modela la realidad identificando qué objetos hay en el mundo del problema, cómo son, cómo se comportan y cómo se relacionan. (Extraído de https://sophia.javeriana.edu.co/~acarrillo/POO/Material/CursoPOOConceptosOO-parteI.pdf consultado el 09/07/2018)

componentes de diferentes fuentes y destinos (celulares, GPS, sensores, cámaras de CCTV, alarmas, etc.).

Zulkipli et al. [7] definen las fuentes de amenazas en el contexto de IoT a partir de los siguientes orígenes:

- Usuario travieso: cuando accede al dispositivo, de manera desprevenida para el fabricante, e ingresa a utilidades limitadas del producto.
- Fabricante inmoral: el productor del dispositivo usa y explota las tecnologías para revelar información del usuario a extraños.
- Agresor externo: conocido también como Entidad Ajena porque no forma parte de la red de IoT y no tiene autorización para acceder, aun así, intenta obtener información confidencial y puede causar el mal funcionamiento de las entidades IoT.
- Programación Deficiente: el desarrollador de software para la aplicación IoT o los dispositivos IoT pueden escribir códigos no seguros, que permitan reconocer los datos del usuario.

Estas fuentes de amenazas pueden ser utilizadas como vía de acceso para vulnerar los sistemas de seguridad digital del usuario, estableciendo situaciones de extorsión, robo, secuestro u otros delitos informáticos.

Las áreas que más pueden verse afectadas por IoT son la privacidad y la seguridad de las personas. Por ello es fundamental tener en cuenta:
- Quien es el dueño de los datos.
- Ciberseguridad, cada vez que nos conectamos a Internet corremos riesgos de sufrir un ataque, ¿cuáles serían los mejores mecanismos de protección?
- ¿Qué políticas de privacidad estamos utilizando?, o tal vez mejor ¿hay políticas de privacidad sobre IoT?
- Control: ¿quién controla las órdenes emitidas por el objeto?
- ¿Quiénes pueden resultar afectados por los errores trasmitidos o cometidos por el objeto?

La intercomunicación de IoT se extiende horizontalmente destruyendo barreras y conectando cosas y personas que antes jamás se habían comunicado. Estos sets de aplicaciones que conectan diversas cosas al mismo tiempo, cruzan jurisdicciones, países e instituciones y diferentes legislaciones.
¿Podemos seguir aplicando los marcos legales existentes a situaciones tan diferentes? Estos temas deben ser analizados y tratados para estar preparados de antemano a los litigios que se generarán prontamente en los sistemas IoT.
Sin pretender agotar el tema, enunciamos hasta aquí las definiciones de IoT que interesan para este trabajo.

1.2 FORENSIA DIGITAL

La inclusión de las Tecnologías de la Información y de las Comunicaciones (TIC) en la sociedad ha posibilitado importantes mejoras en las actividades en general, notándose su mayor impacto en el ámbito de las comunicaciones interpersonales mediante las redes sociales, la mensajería instantánea y el correo electrónico. Pero de igual forma, así como ha

favorecido la vida de las personas, también se utiliza para el desarrollo de actividades delictivas, en las cuales las TIC participan con idéntica fuerza que en el resto de los quehaceres sociales.

Ubicados en el contexto legal, a partir de 1990 surge la necesidad de convocar a peritos informáticos para que actúen como auxiliares de la justicia cuando se presenta una prueba digital. Con el transcurso del tiempo, y la evolución de las tecnologías, esta primera acción del profesional informático que solo hacía un aporte técnico pasó a convertirse en una rama de la disciplina informática con entidad propia.

Proveniente de la Informática aplicada, el desarrollo de la *Informática Jurídica* tuvo una variante distintiva cuando se abordaron las pericias informáticas. Así, surge primeramente la *Informática Forense* y se transforma en lo que hoy se conoce como *Forensia Digital*.

A partir del año 2000, comienzan a surgir los ataques a la seguridad informática, lo que produce un crecimiento en las normas y procesos necesarios para atender la problemática de hacking e intrusión sobre los sistemas informáticos. Ya en el 2005, con la incorporación de aplicaciones web, se hace más crítica la cuestión de la seguridad y resguardo de los datos, al punto de tener que generar esquemas de seguimiento y búsqueda de vulnerabilidades. Aparecen nuevas formas de la seguridad informática (hacking ético por ejemplo) y allí se formaliza la Forensia Digital, para dar una respuesta al análisis de los incidentes de seguridad informática.

Por su parte, la Informática Forense toma para sí las herramientas y métodos de la Forensia Digital y le agrega algunos de los procedimientos propios de la criminalística como la cadena de custodia y el resguardo de la zona del delito.

Se puede tomar como definición de Forensia Digital la propuesta por Zuccardi et al.[8] que dice: "*Forma de aplicar los conceptos, estrategias y procedimientos de la criminalística tradicional a los medios informáticos especializados, con el fin de apoyar a la administración de justicia en su lucha contra los posibles delincuentes o como una disciplina especializada que procura el esclarecimiento de los hechos (¿quién?, ¿cómo?, ¿dónde?, ¿cuándo?, ¿por qué?) de eventos que podrían catalogarse como incidentes, fraudes o usos indebidos bien sea en el contexto de la justicia especializada o como apoyo a las acciones internas de las organizaciones en el contexto de la administración de la inseguridad informática*".

La Forensia Digital se aplica principalmente en dos áreas: en el ámbito de la justicia mediante las pericias informáticas con la inclusión de las evidencias digitales, y en el ámbito empresarial/institucional cuando se analizan fallas de seguridad y acciones de intrusión indebidas.

1.3 EL PROCESO DE ANÁLISIS FORENSE DIGITAL

Son varios los autores que abordan la definición del proceso de análisis forense digital, conjugando cuestiones propias de la criminalística con protocolos y normas de la ingeniería. En particular, se puede tomar la propuesta del Grupo de Investigación sobre Forensia Digital

de la UFASTA[9], quienes incorporan componentes de la ingeniería de Software y proponen el Proceso Unificado de Recuperación de Información (PURI). La Fig. 2 esquematiza este proceso:

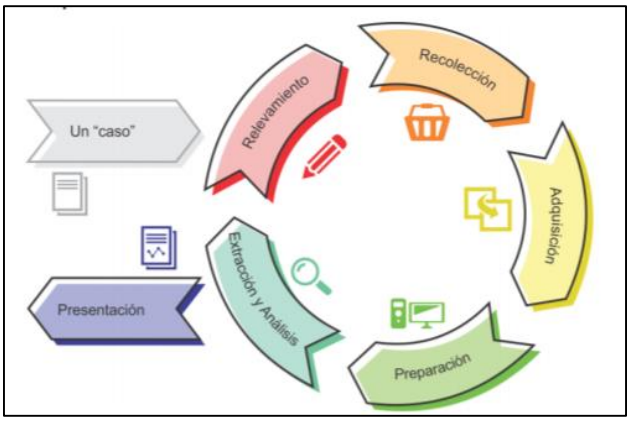


Figura 2: Fases del Proceso Unificado de Recolección de Información (PURI)

La Fase de *Relevamiento* abarca la investigación para conocer el caso e identificar los posibles objetos de interés, para considerar la documentación legal y técnica y la infraestructura de IT con que se va a trabajar. La Fase de *Recolección* abarca las acciones y medidas necesarias para obtener los equipos físicos, y/o las posibles fuentes de datos, sobre los cuales se deberá trabajar posteriormente. La Fase de *Adquisición* abarca todas las actividades en las que se obtiene la imagen forense[2] del contenido que se analizará.

La Fase de *Preparación* involucra las actividades técnicas en las que se prepara el ambiente de trabajo del informático forense, la restauración de las imágenes forenses y volcados de datos, junto con su correspondiente validación, y la selección de las herramientas y técnicas apropiadas para trabajar en la extracción y el análisis, de acuerdo al objeto origen, y a las necesidades del caso. La Fase de *Extracción y Análisis* comprende las tareas forenses de extracción de la información de las imágenes forenses, la selección de la potencial evidencia digital, y su análisis en relación al caso y a los puntos periciales o requerimientos de servicio forense. Finalmente, la Fase de *Presentación* comprende el armado de los informes necesarios y la presentación del caso en un juicio o a los solicitantes.

Hoy en día, la justicia está demandando la participación de peritos informáticos en la obtención y tratamiento de evidencias digitales que se presentan como prueba de un hecho, dado que los rastros digitales son cada vez más numerosos en los procesos investigativos.

De igual modo, demanda a los peritos informáticos un entrenamiento en la materia judicial y criminalística, particularmente respecto de los principios de mantenimiento de la cadena de custodia, no contaminación de la prueba y el uso de criterios de actuación compatibles con el derecho procesal.

[2] Una ***imagen forense*** es una copia exacta, sector por sector, bit a bit, de un medio de almacenamiento. De esta manera, es posible trabajar con la imagen de la misma manera que si se hiciera sobre el original.

1.4 Tecnologías semánticas aplicadas a la Forensia Digital

En el contexto forense, es de suma importancia vincular los datos a partir del significado de cada cosa. No se trata solo de "encontrar la evidencia digital", sino de interpretarla en el contexto de la situación, vinculándola con el resto de los componentes de la investigación (pruebas físicas, interrogatorios, marco legal y procedimental del caso, etc.).

De modo que es indispensable avanzar en la Forensia digital desde la óptica de la semántica –como elemento vinculante de todos los componentes del sistema- así como desde un marco referencial que pueda interpretarlo, es decir, una ontología. El significado de este término se entiende fácilmente a partir de la definición de De Reuver et al.[10] cuando dice que "una ontología es la descripción conceptual y terminológica de un conocimiento compartido acerca de un dominio específico. Dejando de lado la formalización e interoperabilidad de aplicaciones, esto no es más que la principal competencia del término: hacer mejoras en la comunicación utilizando un mismo sistema en lo terminológico y conceptual…".

En el caso particular de IoT, desde las tecnologías semánticas se pueden proponer varias herramientas para la comunicación con los actores no informáticos: taxonomía de conceptos, ontologías para el análisis forense basadas en la trazabilidad de la transmisión, ontologías para la interpretación de casos particulares, entre otras. Desde el proyecto de investigación encarado por el Grupo de Investigación en Informática Forense de la Facultad de Ingeniería de la UCASAL, se están abordando estos temas.

2. CASO DE ESTUDIO

El 21 de octubre de 2016 fuimos testigos de un *ataque de denegación de servicios*[3] distribuido sin precedentes, que dejó inaccesibles a grandes plataformas de Internet principalmente en Norteamérica y Europa pero con un alcance global[4]. Dentro de los damnificados, podemos citar a Amazon, Netflix, PayPal,

The New York Times y otras grandes empresas, en nuestra región el ataque afectó al diario argentino Infobae. Lo novedoso de esta acometida fue que no fue dirigida directamente a las empresas mencionadas, sino que el apuntado fue una compañía proveedora de un servicio esencial para el funcionamiento de Internet como es el DNS (Domain Name System).

El servicio DNS es el encargado de vincular un nombre de dominio, ej. www.ucasal.edu.ar con su correspondiente dirección IP para poder establecer la comunicación entre un usuario y el servidor donde se encuentra albergado el sitio en cuestión. De esta manera podemos inferir la importancia de este mecanismo dado que sin él no sería posible el uso de Internet de la manera que acostumbramos a emplear. Dada la importancia de esta "traducción del nombre de la web en una dirección IP", las empresas usuarias de Internet suelen contratar a grandes compañías proveedoras de este tipo de servicios para garantizar un inmediato tiempo

[3] *Ataque de denegación de servicios* (DDoS) es el que se realiza cuando una cantidad considerable de sistemas atacan a un objetivo único, provocando la denegación de servicio de los usuarios del sistema afectado. La sobrecarga de mensajes entrantes sobre el sistema objetivo fuerza su cierre, denegando el servicio a los usuarios legítimos.

[4] Se puede leer en https://www.infobae.com/noticias/2016/10/21/un-ataque-hacker-a-un-proveedor-de-internet-en-estados-unidos-afecta-a-twitter-y-spotify/ (consultado el 10/07/2018)

de respuesta en la vinculación dominio-IP, así también como una alta disponibilidad a las respuestas de estas consultas (lo que hace que el ingreso a la web de la empresa sea inmediato), debido a que cuentan con una constelación de servidores distribuidos globalmente.

En el caso particular de este ataque, fue dirigido a los servidores de la empresa DYN.com, y efectuado en dos fases. La primera comenzó a HS 10:10AM GMT y se prolongó por un espacio de alrededor cuatro horas y consistió en la recepción de consultas maliciosas al servicio DNS provisto por DYN con una cantidad de trafico completamente inusual lo que impidió que éste pueda responder a las consultas reales provocando la inaccesibilidad a una gran cantidad de sitios pertenecientes a sus clientes. De manera inmediata, al detectar el tráfico inusual, principalmente proveniente de Asia, América del Sur y Europa del Este, iniciaron su protocolo de respuesta y sorprendentemente el origen del ataque cambió de manera repentina afianzándose en la costa este de los Estados Unidos. En respuesta a esto, se aplicaron diversos filtros y redireccionamiento de tráfico que lograron mitigar el ataque finalizando la primera etapa del mismo.

La segunda fase se inició alrededor de las 14:50 GMT y fue más diverso a nivel mundial, con la misma técnica y extendiéndose hasta aproximadamente hs 16:00.

De acuerdo a información oficial[5], se observó tráfico entre 10 a 20 veces superior a lo recibido con asiduidad con algunas ráfagas superiores a 40 veces de lo normal llegando al orden de los 1,2 TBPS[6] y logrando de esta manera perpetuar el ataque por denegación de servicio de mayor envergadura conocido hasta el momento.

Los análisis posteriores al ataque concluyeron que el mismo fue ejecutado utilizando una red de dispositivos de Internet de las Cosas (IoT) tales como routers, grabadores de video (DVR), cámaras, monitores de bebés, etc., que fueron dominados utilizando un *malware*[7] denominado MIRAI[8] que se aprovecha de la falta de actualización y precariedad que contiene el software de base (o firmware) de estos dispositivos genéricos.
Si bien el caso descripto es de interés por que el ataque se generó vulnerando los componentes IoT, hay otros casos de ataques informáticos a instalaciones que brindan servicios vinculados a IoT, y que ponen de manifiesto el riesgo social involucrado con impacto directo en las personas, como por ejemplo:

- Ataque a los Sistemas de ventilación y aire acondicionado de edificios[9]: En 2012 un grupo de atacantes logró manipular remotamente los termostatos de un edificio de gobierno y de una planta manufacturera para cambiar con éxito la temperatura del interior. De haber ocurrido en un lugar con alta concentración de gente y sin acceso a

[5] https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/ (consultado el 10/07/2018)
[6] TBPS: Terabits por segundo
7 Malware: abreviatura de "Malicious software", término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar términos como: Virus, Troyanos (Trojans), Gusanos (Worm), keyloggers, Botnets, Ransomwares, Spyware, Adware, Hijackers, Keyloggers, FakeAVs, Rootkits, Bootkits, Rogues, etc….
[8] https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html (consultado el 10/07/2018)
[9] Se puede leer en https://www.fastcompany.com/3008148/cybercriminals-hack-factory (consultado el 10/07/2018)

ventilación natural (como un shopping por ejemplo) podría haber ocasionado situaciones de riesgo para las personas.

- Ataques a Redes eléctricas[10]: En 2013, se confirmó el robo de información de planos detallados de la red y de 71 estaciones eléctricas, ubicación precisa de dispositivos, diagramas de red y contraseñas de dispositivos de la red eléctrica gestionada por la empresa Calpine, el principal generador de electricidad de los Estados Unidos, poniendo en riesgo a las personas de todas las comunidades usuarias de este servicio.

- Ataque a una Planta acerera[11]: la Oficina Federal de Seguridad de Información de Alemania emitió un informe que confirmaba que en 2010 un grupo de *hackers* había accedido de forma no autorizada para luego impedir el apagado de uno de los hornos a la planta, lo cual provocó un daño masivo a la instalación. Los atacantes obtuvieron acceso a la planta de acero a través de la red comercial de la planta y luego se abrieron camino en las redes de producción para acceder a los sistemas de control de la planta.

- Nuevas variantes a MIRAI**:** con el correr del tiempo aparecieron redes de bots similares a MIRAI, generalmente basadas sobre su código fuente con algunas modificaciones que las vuelven más agresivas. Entre ellas podemos mencionar a Bashlight[12], Brickerbot[13] y PERSIRAI[14] todos son malware que aprovechan la vulnerabilidad de fabricación de los componentes IoT.

2.1 IMPACTO Y CONSECUENCIAS TÉCNICAS Y LEGALES DEL ATAQUE DDoS

El ataque a DYN del 21 de octubre de 2016 pone de manifiesto la vulnerabilidad de los sistemas IoT, ya que los componentes que habitualmente no se consideran informáticos sino electrónicos (grabadoras, cámaras, monitores de bebés, etc.) se fabrican con un firmware cada vez más apto para la interconexión a otros componentes, pero, con mucho descuido respecto de las normas de seguridad informática que deberían regular esa interconexión.

Analizando el impacto del ataque ocurrido, se observan algunas características que deben destacarse:

- La alta escalabilidad de los ataques. Debido a que los sistemas IoT utilizan la red de redes para la comunicación y desde un punto cualquiera de la red, el ataque se difunde rápidamente hacia nuevas conexiones de puntos no atacados inicialmente. Todos los componentes conectados a internet están expuestos a la intrusión indebida.

[10] Se puede leer en http://bigstory.ap.org/article/c8d531ec05e0403a90e9d3ec0b8f83c2/ap-investigation-us-power-grid-vulnerable-foreign-hacks (consultado el 10/07/2018)
[11] Se puede leer en https://www.wired.com/2015/01/german-steel-mill-hack-destruction/ (consultado el 10/07/2018)
[12] Se puede leer en https://krebsonsecurity.com/tag/bashlight/ (consultado el 10/07/2018)
[13]Se puede leer en https://arstechnica.com/information-technology/2017/04/brickerbot-the-permanent-denial-of-service-botnet-is-back-with-a-vengeance/ (consultado el 10/07/2018)
[14] Se puede leer en https://blog.trendmicro.com/trendlabs-security-intelligence/persirai-new-internet-things-iot-botnet-targets-ip-cameras/ (consultado el 10/07/2018)

- El crecimiento exponencial de los dispositivos IoT tanto en cantidad como en tipo de componentes. Inicialmente los sensores y actuadores eran los componentes a través del cual se conectaba un equipo electrónico a Internet, ahora están presentes en la mayoría de los equipos electrónicos, dotando de cierta *inteligencia* al dispositivo.
- Los procesos de fabricación de los dispositivos IoT no están totalmente regulados, ni cuentan con normas internacionales sobre seguridad informática de cumplimiento obligatorio.
- Las dificultades para descubrir a los autores de la intrusión ilegal, tanto en la identificación de las personas u organizaciones, como en la ubicación geográfica de los mismos.
- El cuantioso impacto económico y social que significó a los usuarios de DYN la denegación de servicios, no solo por la imposibilidad de comerciar en la web, sino también por situaciones colaterales vinculadas a la salud, la educación y la seguridad de las personas.

Desde el punto de vista del derecho, el análisis que se puede hacer también resulta de interés. El ataque perpetrado puso de manifiesto la indefensión de los usuarios que quisieron utilizar los servicios de DYN y no pudieron. Más allá de la responsabilidad comercial que le cabe a este proveedor frente a sus clientes, habría que definir el marco legal en el cual alguno de estos usuarios perjudicados pudiera demandar a quien corresponda por lo ocurrido, por ejemplo:

- ¿ante quien se realiza la denuncia? considerando la ubicuidad de internet, y atento a que los servidores están dispersos en diferentes lugares geográficos que impiden fijar la autoridad judicial competente cuando se trata un caso de estas características.
- ¿Cuál es la legislación que se aplica? el derecho internacional deberá contemplar el trabajo colaborativo entre los distintos ámbitos judiciales de los países involucrados
- ¿Hay antecedentes o jurisprudencia que permita marcar el camino a seguir? Es decir, cuanto se puede aprovechar de procesos judiciales similares, tanto en la resolución de los casos como en los aspectos menores del proceso de litigación.
- ¿los profesionales de otras disciplinas que no sean informáticos (policías, abogados, criminalistas, etc.) se encuentran capacitados para atender casos como el citado?

3. CONSIDERACIONES PARA UN CURSO DE ACCIÓN QUE PERMITA ABORDAR LA VULNERABILIDAD DE IoT

Entendiendo entonces la magnitud del desastre producido por el ataque de denegación de servicios, y siendo éste uno más de múltiples casos similares que actúan aprovechando la vulnerabilidad de los sistemas IoT, conviene identificar algunos criterios que puedan ayudar a definir un camino a seguir.

Sin la pretensión de formular una solución concreta para la problemática planteada por el uso inseguro de los sistemas de IoT, proponemos un conjunto de elementos o criterios técnicos y legales que pueden ayudar.

3.1 CRITERIOS TÉCNICOS PARA ATENDER LA VULNERABILIDAD DE IoT

Desde el punto de vista de las tecnologías IoT, los criterios a trabajar se pueden resumir considerando los distintos *actores* intervinientes: usuarios de los sistemas IoT por una parte, y proveedores de servicios y fabricantes de componentes IoT, por la otra.

3.1.1 Educación del usuario IoT

Podemos sugerir o recomendar ciertas medidas a tomar por parte de los usuarios, que habitualmente no son expertos informáticos, por lo que deben saber acerca de las vulnerabilidades de los dispositivos que utiliza y los peligros a los que se exponen.

Si bien los sistemas IoT presenta oportunidades que pueden mejorar tanto el mercado de consumo como el empresarial, es importante que tanto las personas como las empresas evalúen la *exposición al riesgo* cuando adoptan estas tecnologías.

Existe preocupación en el mercado tecnológico sobre este tema, y son varias las empresas Telco que se ocupan de asesorar al usuario final, como ejemplo, Telefónica[11] sugiere:

- Cambiar las contraseñas predeterminadas en los enrutadores domésticos y dispositivos de IoT, usando el cifrado más robusto posible al configurar redes, también asegurando la seguridad del dispositivo desde el lado de LAN
- Usar dispositivos en una red doméstica separada cuando sea factible
- Usar contraseñas seguras para cuentas de dispositivos
- Deshabilitar o proteger el acceso remoto a dispositivos IoT cuando no es necesario
- Investigar las medidas de seguridad del dispositivo del proveedor
- Modificar la configuración de privacidad y seguridad del dispositivo según sus necesidades
- Deshabilitar características que no están siendo utilizadas
- Instalar actualizaciones cuando estén disponibles

3.1.2 Políticas de seguridad de los proveedores de servicios y fabricantes de componentes IoT

Al adoptar IoT es crucial que las empresas tengan en cuenta los aspectos de seguridad desde el inicio de la iniciativa. Las mismas consideraciones de políticas de seguridad y resguardo de los datos, que las empresas implementan puertas adentro para sus activos y aplicaciones tecnológicas, debe implementarse en la provisión de servicios IoT.

Las normas de seguridad ya existen, se pueden adaptar fácilmente en la oferta de servicios de comunicación y almacenamiento de datos en la nube. Al respecto, el informe de Telefónica sugiere a los proveedores de servicios y/o fabricantes de dispositivos de IoT, la implementación de políticas de seguridad acerca de:

- Utilización de conexiones cifradas.

- Anonimización de los datos y su recopilación sólo cuando sea estrictamente necesario.
- Requerir al usuario un cambio obligatorio de las contraseñas por defecto por otras robustas y no permitir contraseñas "quemadas" en el código.
- Permitir la configuración de reglas detalladas de control de acceso.
- Implantar medidas que dificulten ataques de fuerza bruta para adivinar credenciales de acceso.
- Verificación mutua de certificados SSL y de listas de revocación de certificados.
- Implementar medidas inteligentes de fail-safe cuando la conexión o la energía del dispositivo falla.
- Realizar análisis de seguridad del código fuente y ofuscarlo si es accesible para los usuarios.

Aun considerando estas sugerencias, faltan resolver varias cuestiones técnicas, que requieren de la definición de regulaciones exigidas a los fabricantes, como por ejemplo:

- No permitir el uso de usuario y contraseña por defecto, obligando a que el usuario se haga responsable de generar las credenciales de acceso
- Se debe implementar instancias de actualización automática del firmware de los dispositivos IoT.
- Sería deseable implementar esquemas de soporte técnico para los dispositivos IoT, particularmente para aquellos componentes que se fabrican a gran escala y a muy bajo costo, permitiendo que se incorporen en arquitecturas de procesamiento seguras.

3.2 CONSIDERACIONES JURÍDICAS PARA ATENDER LA VULNERABILIDAD DE IoT

Desde el punto de vista legal, está claro que la normativa debe evolucionar, debe adecuarse a los tiempos que corren. El tratamiento de temas como el que nos ocupa siempre será ex post, la evolución tecnológica condicionará la posterior regulación normativa, pero justamente la discusión y generación de la norma debe darse en un marco temporal adecuado, acorde a la necesidad inmediata que la evolución tecnológica genera.

Las técnicas de procesamiento y tratamiento de datos, por citar un caso, que no existían hace tan solo unos quince años atrás, demandan no solo legislar en aras de proteger a los consumidores de estos objetos sino de exigir a los fabricantes adoptar medidas acordes a estas necesidades de protección. Asimismo, desde lo penal, resulta fundamental legislar nuevas sanciones para los ilícitos que se cometiesen mediante su uso.

Acorde a esta innovación tecnológica constante, deberán los legisladores de los distintos países abordar la urgente discusión que esta nueva revolución tecnológica demanda.

Temas como la recientísima aprobación del Reglamento General de Protección de Datos europeo (RGPD)[15] deben ser abordados y servir de marco comparativo para la futura legislación local o regional. Las normas más estrictas en materia de protección de datos implican que las personas tienen más control sobre sus datos personales y que las empresas se benefician de igualdad de condiciones.

Este reglamento contiene dos documentos de altísima utilidad para el tema que se trata en el presente trabajo:

- "Siete pasos para que las empresas se preparen para el Reglamento general de protección de datos (RGPD)" resumido en los siguientes puntos:

    - Verifique los datos personales que recopila y trata, el fin para el que lo hace y sobre qué base jurídica
    - Informe a sus clientes, empleados y otras personas cuando recopile sus datos personales
    - Conserve los datos personales únicamente mientras sea necesario
    - Proteja los datos personales que esté tratando
    - Conserve documentación sobre sus actividades de tratamiento de datos
    - Asegúrese de que su subcontratista respeta las normas
    - Compruebe si está sujeto a las disposiciones del RGPD
- "Guía para los ciudadanos sobre la protección de datos en la UE" resumido en los siguientes puntos:
    - Derecho a saber quién trata qué y por qué
    - Derecho a acceder a sus datos
    - Derecho a oponerse
    - Derecho a corregir sus datos
    - Derecho a borrar los datos y al olvido
    - Derecho a opinar cuando las decisiones son automatizadas
    - Derecho a trasladar sus datos

Es fundamental que el enfoque considerado por el RGPD sea revisado a la luz de su aplicación en los sistemas IoT.

Particularmente, en el caso argentino, la actualización de la ley 25.326, de protección de datos personales, debe ser necesariamente abordada y es el camino que se está recorriendo. Pensada en un mundo en donde internet no tenía la relevancia que hoy tiene, en donde la interconexión de los objetos era algo impensado, esta ley debe adaptarse a los tiempos. En el año 2000, en que fue sancionada, no se concebían las amenazas, ni vulneraciones posibles en materia de datos que la tecnología permite a la fecha. Casos como el que nos ocupa describen perfectamente esta vulnerabilidad vigente.

[15]Se puede leer en https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_es (consultado el 10/07/2018).

Es dable destacar que desde el año 2016 Argentina viene abordando esta y otras necesidades de modificación en el marco del proyecto Justicia 2020[16] del Ministerio de Justicia y Derechos Humanos de la Nación y que, en el caso citado, ya existe un anteproyecto de reforma a la ley de protección de datos personales.

En igual sentido se aprobaron, en el año 2017, los Estándares Iberoamericanos de Protección de Datos Personales[17], con el objetivo de convertirse en marco de referencia para homologar la regulación de la protección de los mismos en la región, instancia sumamente necesaria a la luz de una temática que claramente escapa de lo que un solo estado pudiese legislar al respecto.

En síntesis, temas como la debida notificación de incidentes en materia de seguridad, la comunicación de estos, las sanciones ante la no comunicación, el deber de información necesaria suficiente y eficiente cuando se introduce un nuevo objeto al mercado, el consentimiento expreso o tácito del titular de los datos cuando se trabaja con ello, deben ser necesariamente abordados y encajonados en el marco legal adecuado.

En idéntico sentido, la debida sanción penal de los ilícitos cometidos por esta vía, los consensos entre los países y el camino a la homologación normativa permitirán impedir la generalización de los mismos y minimizar su impacto.

Lo antes expuesto, sin olvidar la necesidad de adecuar la legislación procesal existente a fin de no tornar ilusorios los derechos o protecciones que la normativa de fondo regulen.

¿Qué se debería tener en cuenta para avanzar en un curso de acción que atienda situaciones como el caso citado como ejemplo? Además de generar un marco legal –de alcance internacional- que sirve de ámbito de contención para quienes son perjudicados por estos actos delictivos, se debe trabajar en:

- Conformación de espacios de trabajos internacionales e interdisciplinarios, para abordar el estudio de normas técnicas y legales que generen un ámbito seguro para la utilización de sistema IoT.
- Generación de acciones de concientización sobre la exposición al riesgo que generan los sistemas IoT dirigido principalmente a los usuarios finales, y también sobre la responsabilidad de evitar la intrusión indebida que le cabe a los proveedores de servicios y fabricantes de dispositivos IoT.
- Regulaciones para la fabricación de dispositivos IoT (sean éstos de cualquier tipo, microsensores o dispositivos de gran porte), a fin de que se ajusten a los requisitos de seguridad informática necesarios.
- Implementación de las normas de resguardo de datos y protección de la privacidad, en todas las instancias de la comunicación IoT, sean éstas provenientes de servicios de transmisión y/o almacenamiento en la nube.

[16] Se puede leer en https://www.justicia2020.gob.ar/ (consultado el 10/07/2018).
[17] Se puede leer en http://www.jus.gob.ar/datos-personales/comunicados/2017/06/22/estandares-de-proteccion-de-datos-personales-para-los-estados-iberoamericanos-(1).aspx (consultado el 10/07/2018).

4. CONSIDERACIONES PARTICULARES PARA LA FORENSIA DE IoT

Para el investigador forense la tecnología IoT plantea un gran desafío, principalmente en las fases de extracción y preservación de la prueba digital. Zulkipli et al. [7] identificaron los desafíos que plantea IoT a la Forensia Digital, entre los cuales se enuncian:

- Las herramientas y tecnologías forense generalmente no son medios aptos para identificar y analizar la infraestructura de IoT, es necesario desarrollar nuevas herramientas y protocolos de actuación pericial. Como se puede apreciar no está claro cómo proceder en estas situaciones, no existen protocolos formales de actuación y los que existen abundan en consideraciones tecnológicas pero escasamente se ajustan a los procesos normados de la justicia. Por su parte, desde el ámbito del derecho, también deben modificarse los procedimientos de obtención de pruebas digitales para ajustarlos a las arquitecturas de procesamiento distribuidos tales como *cloud computing y cloud services*.

- El proceso de análisis forense tradicional se verá afectado. Los dispositivos IoT producen una gran cantidad de datos, que se siguen generando al momento mismo de la investigación forense, requiriendo más tiempo para la identificación de la información relevante, su resguardo y preservación. Estos dos últimos pasos son los más críticos debido a que usualmente los dispositivos de IoT no se pueden desconectar para aislarlos y preservar la prueba digital. Hay otros temas que también deben estudiarse y ajustarse para actuar en la búsqueda de pruebas digitales en el contexto tecnológico de IoT: la cadena de custodia y la preservación de la escena del delito. Cuando se trata de sistemas IoT, mayormente implementados en la nube, estos dos aspectos son cruciales al momento de definir *cuándo* y *cómo* se obtiene la prueba digital. Por ejemplo: el perito debe decidir si corta la energía para no sobrescribir la evidencia con el riesgo que eso implica, o si corta el servicio de internet para no alterar la información o perderla, aunque también es posible cortar la comunicación entre si e intentar la extracción local de la evidencia en los dispositivos.

- El proceso de extracción de pruebas también se podría complicar ya que los dispositivos IoT cuentan con formatos de datos heterogéneos, protocolos e interfaces físicas involucradas. Se destaca particularmente la diversidad de dispositivos, con sistemas operativos propietarios, y la creciente capacidad de inteligencia de los sensores y actuadores. Por otro lado, existen dispositivos que trabajan en una arquitectura distribuida de modo que los datos de las actividades realizadas se encuentran distribuidos en distintos nodos y/o servicios en la nube. Este es un gran desafío para el forense que deberá analizar y determinar cuáles son los nodos de interés para la investigación, y el consecuente trámite de obtención de los datos ante proveedores del servicio que no se encuentran radicados en un único país, o a veces, no se encuentran bajo la competencia de la autoridad judicial ante quien se tramita el caso. Otra característica propia de los dispositivos IoT que también dificulta la tarea de extracción y la preservación de la prueba digital, es la capacidad de sobre escritura que tienen estos dispositivos. Esto implica que la evidencia residente en los componentes IoT es muy volátil, ocurriendo muchas veces que cuando se va a realizar la pericia el dato ya no existe.

Estos aspectos destacados, se suman a la problemática que en sí ya tiene la Forensia Digital, como ser: rigurosidad en la cadena de custodia, capacitación de los analistas forenses en estas nuevas tecnologías, normalización y estandarización de los registros (logs) de eventos, normativa legal y jurisprudencia sobre el tema.

5. CONCLUSIONES

Internet de las Cosas propone un contexto totalmente diferente al conocido hasta hoy. El procesamiento de datos pasó de un estadio *controlable* a un estadio altamente dinámico y maleable, que se ajusta automáticamente a los requerimientos del usuario. Si también consideramos los avances de la Inteligencia Artificial, Big Data y la Inteligencia Ambiental[18], se puede considerar que IoT es el inicio de una nueva forma de relacionarnos con la tecnología, que presenta muchísimos desafíos para las personas, principalmente en aquellas cuestiones relacionadas con la propia esencia del ser humano: el respeto, la dignidad, la interacción con los otros, la vida en sociedad.

Hoy los *millenniams* que constituyen la generación IoT, viven en el cambio permanente, y ya se están incorporando a la sociedad productiva de estos momentos. Por esto es necesario reconocer los cambios, adaptarse a ellos y nunca dejar de aprender. Esta constituye la característica imprescindible en estos tiempos. Si podemos aceptar que los estándares, la colaboración, la comunicación, los modelos de negocios y los modos de interacción entre nosotros y la tecnología sean abiertos y flexibles, y que la legislación también acompañe de este modo el proceso de cambio, podremos hacer de nuestro mundo un sistema colaborativo e integrador donde se puedan desarrollar soluciones agiles y acordes al entorno digital en el que estamos inmersos bajo premisas de convivencia que nos permita ser mejores personas.

6. REFERENCIAS BIBLIOGRÁFICAS

[1] CSIRT-CV, "Seguridad en Internet De Las Cosas," *Cent. Segur. TIC la Comunitat Valencia.*, p. 42, 2016.

[2] D. Betancourt, G. Gómez, and J. I. Rodríguez, "Introducción a la Internet de las Cosas." 2016.

[3] G. Misra, V. Kumar, A. Agarwal, and K. Agarwal, "Internet of Things (IoT) – A Technological Analysis and Survey on Vision, Concepts, Challenges, Innovation Directions, Technologies, and Applications (*An Upcoming or Future Generation Computer Communication System Technology*)," *Am. J. Electr. Electron. Eng. Vol. 4, 2016, Pages 23-32*, vol. 4, no. 1, pp. 23–32, 2016.

[4] X. Caron, R. Bosua, S. B. Maynard, and A. Ahmad, "The Internet of Things (IoT) and its impact on individual privacy: An Australian perspective," *Comput. Law*

[18] *Inteligencia Ambiental o Computación Ubicua es la integración de la informática en el entorno de la persona, de forma que los ordenadores no se perciban como objetos diferenciados, creando un entorno que se puede controlar desde un dispositivo móvil o un mouse.*

Secur. Rev., vol. 32, no. 1, pp. 4–15, 2016.
[5] Telefonica; Accenture; Ipsos, “Things Matter: The user experience of the IoT in Spain,” 2017.
[6] K. Min and S.-W. Chai, “A comparative analysis of personal data protection policies of leading countries in the internet of things (IoT) environment,” *Contemp. Eng. Sci.*, vol. 9, no. 13, pp. 627–633, 2016.
[7] N. H. Nik Zulkipli, A. Alenezi, and G. B. Wills, “IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things,” *Proc. 2nd Int. Conf. Internet Things, Big Data Secur.*, no. IoTBDS, pp. 315–324, 2017.
[8] G. Zuccardi *et al.*, “Evidencia Digital: Contexto, Situación, e Implicaciones Nacionales,” no. Evidencia Digital, pp. 1–17, 2006.
[9] D. I. Haydée A. *et al.*, “El rastro digital del delito Aspectos técnicos , legales y estratégicos de la Informática Forense.”
[10] M. de Reuver and T. Haaker, “Designing viable business models for context-aware mobile services,” *Telemat. Informatics*, vol. 26, no. 3, pp. 240–248, 2009.
[11] T. Detection, “Threat Detection Telefónica Trend Report Insecurity in the Internet of Things,” 2015.

PROTECCIÓN DE DATOS PERSONALES, TECNOLOGÍA Y DERECHO DEPORTIVO EN EL PERÚ: BIG DATA Y CLASIFICACIÓN AL MUNDIAL DE FÚTBOL 2018.

*Por: **Julio Núñez Ponce***
Perú

1. INTRODUCCION.

La protección de datos personales en un mundo global, tiene directa relación con el uso intensivo de la tecnología en todos los ámbitos, incluyendo el deportivo. En la presente ponencia se analiza desde el punto de vista jurídico la utilización de software, base de datos y demás tecnologías de información y comunicaciones a los procesos de clasificación al mundial de Futbol Rusia 2018, por parte de la selección peruana de futbol.

Al respecto, hay que tener en cuenta que "Big Data se refiere a los conjuntos de datos cuyo tamaño está más allá de las capacidades de la herramientas comunes de software de base de datos para capturar, almacenar, gestionar y analizar…tienen tres características principales: volumen (cantidad), velocidad (velocidad de creación y utilización) y variedad (tipos de fuentes de datos no estructurados, tales como interacción social, video, audio, cualquier cosa que se pueda clasificar en una base de datos)"[1]. Este Biga Data ha sido utilizado en el proceso de clasificación al Mundial de Futbol por parte de la Selección Peruana de Fútbol.

En la presente ponencia se analiza la protección de datos personales, la tecnología de big data y la minería de datos en su aplicación al deporte, y específicamente al caso peruano de la clasificación del mundial de fútbol; para luego, reflexionar sobre la protección de datos personales, la tecnología y el derecho deportivo.

2. LA PROTECCION DE DATOS PERSONALES y LA TECNOLOGIA DE BIG DATA y MINERIA DE DATOS.

"Big Data es un término que alude al enorme crecimiento en el acceso y uso de información automatizada. Se refiere a las gigantescas cantidades de información digital controlada por compañías, autoridades y otras organizaciones, y que están sujetas a un análisis extenso basado en el uso de algoritmos… Lo que importa es su valor potencial, que sólo las nuevas tecnologías especializadas en Big Data pueden explotar. En última instancia, el objetivo de esta tecnología es aportar y descubrir un conocimiento oculto a partir de grandes volúmenes de datos"[2].

[1] JOYANES AGUILAR, Luis: "Industria 4.0 La Cuarta Revolución Industrial". Ed. Alfa Omega. Bogotá, Colombia, 2017. Página 130.

[2] GIL GONZALES, Elena: "Big data, privacidad y protección de datos". Ed. Agencia de Protección de Datos. Madrid, España. 2016. Páginas 17-18.

En el mundo deportivo, concretamente, en el proceso de clasificación del Mundial de Futbol en Sudamérica donde han clasificado cinco países: Brasil, Uruguay, Argentina, Colombia y Perú, el uso de datos de jugadores, partidos, jugadas por medios automatizados es una realidad, cada vez más frecuente. En el Perú, el proceso de recojo de información personal para estos fines empezó el año 2015 y desde esa fecha se ha perfeccionado la gestión para un uso eficaz de estos datos. El Derecho de las Nuevas Tecnologías, se ve relacionado directamente con el cumplimiento del ordenamiento jurídico vigente en el país y con una realidad que incluye flujo transfronterizo de datos personales y transferencia de datos personales utilizando la tecnología del Big Data.

"Big Data, al igual que la nube (cloud computing) abarca diversas tecnologías. Los datos de entrada a los sistemas de Big data pueden proceder de redes sociales, logs, registros de servidores Web, sensores de flujos de tráfico, imágenes de satélites, flujos de audio y de radio, transacciones bancarias, MP3 de música, contenido de páginas web, escaneado de documentos de la administración, caminos o rutas GPS, telemetría de automóviles, datos de mercados financieros…"[3].

Esta variedad de fuentes de información que abarca el Big Data permite utilizar las redes sociales, logs, registros de servidores web donde hay datos futbolísticos, así como imágenes de satélites, donde puede obtenerse partidos de futbol, entrenamientos, jugadas especiales; asimismo, los flujos de audio y radio permiten escuchar las instrucciones, expresiones y comunicaciones que acompañan a las imágenes de los respectivos partidos o entrenamientos.

"La 36° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad[4] hace un llamado a todas las partes que utilizan el Big Data para que apliquen, entre otros, los siguientes lineamientos, al que añadimos comentarios nuestros sobre cada lineamiento:

a) *Respetar el principio de especificación de finalidad.*
La finalidad debe ser expresa y licita. Los tratamientos de datos personales y la transferencia de datos deben tener una finalidad expresa y licita. Esta finalidad debe ser especificada e informada la titular de datos. En el Big data se aplica el principio que esta especificación sobre la finalidad debe ser respetada por todos los usuarios de los datos personales. Tratándose de datos deportivos, el identificar jugadas, jugadores en partidos de futbol, transmitirlas y transferirlas debe realizarse con una finalidad lícita especificada.

b) *Limitar la cantidad de información recolectada y almacenada a un nivel que sea necesario para el propósito legítimo que pretende.*
La limitación de la información deportiva está en disonancia con la práctica del big data de recopilar información en forma masiva, de partidos, jugadas, datos de rendimiento. Sin embargo la necesidad de información debe estar en concordancia con el propósito legítimo que se pretende de utilizar esa información y datos personales para optimizar resultados en competencias deportivas como el Mundial de Futbol.

[3] JOYANES AGUILAR, Luis: Ob.cit. página 135.
[4] 36° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. 13 al 16 de octubre de 2014. Balaclava Fort. Mauricio. Resolución sobre Big data.

c) *Obtener, cuando sea apropiado, el consentimiento válido del titular de los datos en relación con el uso de información personal para fines de análisis y de creación de perfiles.*

El consentimiento valido es un tema central con respecto a la información deportiva recopilada. El consentimiento debe ser libre, previo, expreso e inequívoco e informado.

Al respecto, cabe tener en cuenta la posición de la Autoridad Nacional de Protección de Datos Personales, que afirma que: "Queda claro que para realizar el tratamiento se requiere el consentimiento del titular de los datos personales, o en su defecto, debe acreditarse que en el tratamiento se presentan algunas excepciones establecidas en la Ley de Protección de Datos personales y su Reglamento, de lo contrario, el tratamiento sin consentimiento, constituye una afectación al derecho fundamental a la protección de datos personales… del contenido de la reclamación y la contestación de la reclamación, se advierte que la realización del mencionado tratamiento implica que la reclamada ha destinado los datos personales que recopilo en el contexto de la ejecución del servicio que presta al reclamante a una finalidad distinta no autorizada. Como consecuencia de lo actuado y de lo analizado para resolver el procedimiento trilateral de tutela, se constatan conductas infractoras que esta autoridad puede sancionar…"[5]. Aplicado, este concepto a los datos deportivos opinamos que el consentimiento en forma previa, expresa e inequívoca debiera estar presente en el tratamiento de datos deportivos.

d) Ser transparentes acerca de que información se recolecta, como se procesa, con qué propósito serán utilizados y si será transferida a terceros.

Por el derecho de información en materia de protección de datos personales, el titular de los datos personales tiene derecho a ser informado en forma detallada, sencilla, expresa, inequívoca y de manera previa a su recopilación, sobre la finalidad para la que sus datos personales serán tratados, quienes son o pueden ser sus destinatarios, la existencia del banco de datos personales en que se almacenarán , así como la identidad y domicilio del titular y, de ser el caso , del encargado de tratamiento de datos personales , el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga , en especial en cuanto a los datos sensibles; la transferencia de datos personales; las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; el tiempo durante el cual se conserva sus datos personales; y la posibilidad de ejercer los derechos que la ley le concede y los medios personales para ello[6].

[5] Resolución Directoral N° 049-2016-JUS/DGDP de 7 de Junio de 2016. Procedimiento Trilateral de Tutela. La Autoridad Nacional de Protección de Datos del Perú (que inicialmente se denominaba Dirección General de Protección de Datos Personales del Ministerio de Justicia (MINJUS), actualmente es la Dirección de Transparencia y Protección de Datos Personales del MINJUS) afirma: "En el presente caso, se ha acreditado la realización de una tratamiento: la transferencia de datos y el posterior envío de publicidad comercial por parte de la empresa "Casa Helena" a la dirección del correo electrónico del reclamante, utilizando el nombre de su menor hija, y ofreciendo los servicios de confección de uniformes de la Institución Privada Innova Schools (Sede Chorillos); tratamiento realizado sin contar con consentimiento y sin que exista alguna de las excepciones reguladas en el artículo 14 de la Ley de Protección de Datos Personales (LPDP)". En: https://www.minjus.gob.pe/proteccion-de-datos-personales/

[6] Ley 29733, Ley de Protección de datos personales peruana. Art. 18. Derecho de Información del titular de datos personales.

e) Dar a las personas acceso apropiado a los datos que han sido recolectados sobre ellas y a la información y decisiones que se han tomado con esos datos. Las personas debe ser avisadas de la fuente de sus datos personales y, cuando sea apropiado, de su derecho a corregir su información, así como las herramientas para controlar esta información… "[7].

El aviso o notificación a las personas que aparecen en las imágenes deportivas, puede ser realizado en forma electrónica, lo importante es que esta comunicación esté autenticada y permita el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. APLICACIÓN DE LA TECNOLOGIA DE BIGDATA AL DEPORTE.

"Hoy en día, los nuevos datos se ponen al servicio de usos antes no conocidos, que ha sido posible desarrollar gracias al crecimiento de la capacidad de memoria de los ordenadores, los poderosos procesadores, el increíble abaratamiento de recopilar y almacenar toda esta cantidad de información, y el análisis matemáticos que provienen de la estadística tradicional. Cuando transformamos la realidad en datos, podemos transformar la información en nuevas formas de valor"[8].

Para hablar del Big data hay que darse cuenta que es una técnica que ayuda con la recogida masiva de datos y su cruce a tomar decisiones importantes, tal como se señal a en el artículo "El Big Data irrumpe en el deporte para mejorar las decisiones estratégicas" de Luis Javier Sánchez, publicado en confilegal [9]. En este artículo, Joaquín Muñoz, socio de ONTIER y responsable del área de propiedad intelectual y tecnologías, además vicepresidente de la Asociación de Derecho Deportivo de Madrid, explica: "Esto es algo que ya se viene haciendo hace años en el mundo del deporte, en menos escala que lo que supone ahora el propio Big Data". De hecho hablar de esta actividad…"supone cuantificar y recoger datos sobre las variables que intervienen en el juego con el fin de tomar decisiones: el estado de forma de los jugadores, su adecuación al estilo del entrenador, los pases completados, pases entre líneas, regates.

En definitiva, convertir la información que va más allá de los goles, tarjetas o asistencias, en algo que sirva para mejorar en la faceta deportiva", explica Salvador Carmona, especialista en Big Data y uno de los ponentes que explicará cómo el análisis de datos está transformando este deporte. Con el big data se pueden acumular datos y cruzar, de cara a tomar decisiones importantes. "Ahora esos datos se pueden tener en tiempo real, con lo cual su valor estratégico es muy importante", indica Muñoz. Este jurista nos recuerda que que los Warriors de la NBA, liga de baloncesto americana, crearon su equipo desde la estadística "vieron que necesitaban jugadores que metieran muchos triples y montaron el equipo sobre esta premisa".

---

[7] 36° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. 13 al 16 de octubre de 2014. Balaclava Fort. Mauricio. Resolución sobre Big data.
[8] GIL GONZALES, Elena: Ob.cit., página 20.
[9] SANCHEZ, Luis Javier: "El Big Data irrumpe en el deporte para mejorar las decisiones estratégicas". En Confilegal. Madrid, España 07 de mayo de 2017. En https://confilegal.com/20170507-la-aume-reclama-una-politica-de-estado

Este es un ejemplo de cómo configurar una plantilla profesional desde una buena gestión de los datos estadísticos. Para este experto, la acumulación de información de años anteriores ayudará "a tomar decisiones y ver que ha faltado para ser campeón desde el análisis de esos datos concretos." Ahora, tras su aplicación en el béisbol o la NBA, este concepto comienza a hacerse un hueco en el mundo del fútbol. "Un deporte con posesiones infinitas y reloj corrido, que es más difícil de analizar por la cantidad de datos que genera", apunta Salvador, el mismo creador de una herramienta capaz de cuantificar el marcador de un partido en función de los disparos de cada conjunto.". En definitiva, convertir la información que va más allá de los goles, tarjetas o asistencias, en algo que sirva para mejorar en la faceta deportiva", explica Salvador Carmona, especialista en Big Data y uno de los ponentes que explicará cómo el análisis de datos está transformando este deporte. Con el big data se pueden acumular datos y cruzar, de cara a tomar decisiones importantes. "Ahora esos datos se pueden tener en tiempo real, con lo cual su valor estratégico es muy importante", indica Muñoz[10].

4. EL CASO PERUANO: LA CLASIFICACION AL MUNDIAL DE FUTBOL DE RUSIA 2018.

La práctica del deporte en general constituye un derecho humano y como tal es inherente a todas las personas. Por el principio de equidad toda persona tiene igualdad de oportunidades al acceso, permanencia y trato en la práctica del deporte en general y la integración de las personas. Los valores que se promueven en la práctica deportiva son los de solidaridad, justicia, libertad, honestidad, tolerancia, responsabilidad, trabajo, verdad y pleno respeto a las normas de convivencia deportiva[11].

Conforme la Ley 29733, Ley de Protección de Datos Personales, se entiende por datos personales a "toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados". Se entiende por Datos Sensibles "datos personales constituidos por los datos biométricos que por si mismos pueden identificar al titular; datos referidos al origen racial o étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual". Se entiende por Banco de Datos Personales "Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso". Se entiende por Transferencia de datos personales "Toda transmisión, suministro o manifestación de datos personales, de carácter nacional o internacional, a una persona jurídica de derecho privado, a una entidad pública o a una persona natural distinta al titular de datos personales". Se entiende por Flujo transfronterizo de datos personales "Transferencia Internacional de datos personales, a un destinatario situado en un país distinto al país de origen de los datos personales, sin importar el soporte

[10] SANCHEZ, Luis Javier: "El Big Data irrumpe en el deporte para mejorar las decisiones estratégicas". En Confilegal. Madrid, España 07 de mayo de 2017. En https://confilegal.com/20170507-la-aume-reclama-una-politica-de-estado

[11] Cfr. Congreso dela República del Perú. Proyecto de Ley 1517/2016 –CR: "Proyecto que establece la Ley General del Deporte". En http://www.congreso.gob.pe

en que éstos se encuentren, los medios por los cuales se efectúa la transferencia ni el tratamiento que reciban".

En el Perú, se han desarrollado distintas acciones para fortalecer la cultura de protección de datos personales. A nivel normativo se dio la Ley 29733, Ley de Protección de Datos Personales en el mes de Julio del año 2011, el Reglamento el Decreto Supremo 003-2013-JUS se aprobó el 22 de marzo de 2013 regulándose entre otros temas, las funciones de la Dirección de Protección de Datos Personales del Ministerio de Justicia. Posteriormente el Decreto Legislativo 1353, modificó la Ley de Protección de Datos Personales creando la Autoridad Nacional de Transparencia y Acceso a la Información Pública, fortaleciendo el Régimen de Protección de Datos Personales y la regulación de la gestión de intereses.

Por Decreto Supremo N° 019-2017-JUS del 15 de Setiembre de 2017, se reglamentó el Decreto Legislativo 1353. Entre los temas reglamentados cabe destacar la regulación del Tribunal de Transparencia y Acceso a la Información Pública que tiene entre sus funciones "dirimir mediante opinión técnica vinculante los casos en que se presente conflicto entre la aplicación de la Ley 29733, Ley de Protección de Datos Personales y de la Ley 27806, Ley de Transparencia y Acceso a la Información Pública".

Es con este marco legislativo, que analizamos el caso Peruano del uso de los datos personales, el Big Data y las Tecnologías de la Información y Comunicaciones al Proceso de Calificación al Mundial de Futbol de Rusia del 2018. Al respecto, hay que tener en cuenta que: "Un vendaval de novedades tecnológicas llego al futbol en el vertiginoso siglo XXI. Aportes científicos y cibernéticos se empezaron a aplicar para controlar, recuperar y mejorar el estado físico de los jugadores. Asimismo, los programas informáticos desarrollaron increíbles sistemas para estudiar los partidos, las actuaciones individuales, los aciertos y desaciertos-propios y del rival- hasta permitir elaborar una minuciosa base de datos capaz de entregar un compendio detallado sobre todo lo que acontece en un partido o en un entrenamiento. En el Perú no se utilizaban esos recursos hasta que una tarde a finales de marzo del 2015, el profesor Néstor Bonillo le pidió una reunión a Juan Carlos Oblitas para solicitarle la adquisición de varios instrumentos tecnológicos. El director deportivo no le dio vueltas al asunto y le pidió un listado. Bonillo quedo satisfecho porque encontró respaldo, el mismo respaldo que había tenido cuando le hizo la propuesta al técnico Gareca"[12].

Los programas de software en el manejo de datos personales aplicables a la actividad deportiva son una realidad verificable y actual en el Perú y en otros países del mundo. Los sistemas para estudiar partidos, suponen analizar datos personales de los jugadores y entrenadores protagonistas de cada partido, focalizándose en las actuaciones individuales y haciendo una análisis valorativo de aciertos y desaciertos, o lo que da lugar a la creación, desarrollo y mantenimiento de una base de datos que puede utilizar la inteligencia de negocios, la minería de datos y otras técnicas de análisis de información para la elaboración de reportes, informes que compendian los detalles de todos los datos que revelan información que acontecen en un partido de fútbol o en un entrenamiento.

[12] JARA, Umberto: "El Camino a Rusia: La Historia Secreta de la Hazaña y sus protagonistas". Ed. Planeta.. Lima, Perú. Primera Edición. Marzo 2018. Página 77.

En este orden de ideas, se tomaron decisiones tecnológicas deportivas, que implicaron lo siguiente: "Para tener un banco de datos completo de cada jugador, el comando técnico decidió obtener información en los entrenamientos a través del uso de GPS y un software que permite comparar el desempeño del jugador en las practicas con los datos de los partidos que juega en su club o selección… Un aspecto importante es que la planificación táctica de los partidos tuvo el aporte de los datos estadísticos. Pudimos determinar cuál es el porcentaje de salida eficiente larga que tenemos, que porcentaje de salida corta, que porcentajes de pelotas ingresan al área por un sector, en qué lugar del campo se recupera más, en qué lugar del campo se recupera menos, cual es el porcentaje de recuperación de pelotas en los distintos sectores, quienes tiene mejor salto en defensa o en ataque. Lo mismo con los rivales. A dónde va el juego aéreo de los rivales en los tiros de esquina y en los tiros libres, cuales son los jugadores que vana a las distintas zonas, en qué porcentaje se repiten en cada zona. En base a todo esto, Ricardo Gareca toma decisiones"[13].

El tratamiento de datos personales descrito en el párrafo anterior, que incluyen datos estadísticos para la planificación de los partidos, implica analizar los datos de cada jugador midiendo y calificando sus acciones como la salida larga o la salida corta, la recuperación de la pelota, los tiros al arco, el grado de efectividad, etc. Lo que supone elaborar un perfil futbolístico de cada jugador en base a datos que lo identifican o lo hacen identificable. Asimismo, se sistematizado datos de relevancia grupal que coadyuva a establecer indicadores de rendimiento que facilita la planificación de jugadas y partidas en campeonatos, competencias de futbol profesional.

El sistema de información creado, debe tener en cuenta distintos criterios que sirven de base a la toma de decisiones. En este sentido se afirma que: "Ahora bien hay una precisión importante, que no hay que perder de vista. Todo el aporte de la tecnología ayuda a las decisiones, pero no define. Las tecnologías y su procesamiento estadístico aportan insumos para el trabajo de Gareca y sus asistentes…pero luego hay otros aspectos que corresponden al manejo del director técnico y su relación con los jugadores. La ventaja del material que existe en la base de datos es que Gareca podía mostrar a los jugadores evidencias y no discursos. En tal sentido, les mostraba los datos recopilados y analizados, los sentaba y les decía: Ven mira, estas son tus capacidades reales, estas son tus deficiencias"[14].

El poder elaborar un fichero personal de cada jugador sobre sus potencialidades reales de juego, tiene un aspecto motivacional importante que coadyuva a maximizar el rendimiento del jugador en un partido de futbol. Las tecnologías de información son utilizadas en el proceso de consolidar un juego definido de un equipo de futbol, que tratándose de una selección nacional como la peruana, adquiere una importancia relevante. La legislación de protección de datos personales establece principios y derechos que deben ser aplicados a estas actividades y procesos. Principios como legalidad, consentimiento, finalidad, proporcionalidad, calidad de datos y seguridad de la información deben ser tomados en cuenta y respetados. Por otra parte, derechos como el de información, acceso, rectificación, cancelación, oposición deben ser respetados y debe facilitarse los medios para que el titular de los datos personales pueda ejércelo en forma oportuna y adecuada.

[13] JARA, Umberto: Ob.cit. páginas 85 y 87.
[14] JARA, Umberto: Ob.cit. páginas 87 y 88.

5. REFLEXIONES EN TORNO A LA PROTECCION DE DATOS PERSONALES, LA TECNOLOGIA Y EL DERECHO DEPORTIVO.

El tratamiento de datos personales deportivos, descritos en el punto anterior, origina la reflexión de la importancia de la utilización del Big Data en estas actividades. "El Big Data desafía las normas de protección de datos al facilitar la re-identificación de los sujetos, ya no sólo a partir de los datos pseudónimos, sino también a partir de datos que consideramos anónimos. Es decir, las técnicas de la anonimización ya no son siempre suficientes con la llegada del Big Data"[15].

Tratándose de datos personales en el ámbito deportivo tanto de los jugadores de cada equipo, como de los rivales reales y potenciales, el Big data permite interrelacionar datos y analizarlos en forma inteligente, agregando valor y elaborando información que sirve de base para la toma de decisiones.

"Existe un gran número de puntos de vista para visualizar y comprender la naturaleza de los datos y las plataformas de software disponibles para su explotación: la mayoría incluirá una de estas tres propiedad (volumen, velocidad, variedad)…sin embargo, algunas fuentes también consideran una cuarta característica que es la veracidad…"[16].

El volumen de datos futbolísticos que incluyen imágenes desde distintos ángulos, supone un permanente proceso de captura de datos y evaluación de su importancia y pertinencia. La velocidad de acceso a los datos en tiempo real tiene también importancia, sobre todo si se trata de datos que son requeridos con urgencia para la preparación de estrategias previas a partidos de futbol. Con respecto a la variedad, un mismo movimiento de un jugador de futbol puede ser enfocado desde distintos puntos de vista, la variedad de las imágenes es también un factor Trascendente. Finalmente, la veracidad de los datos, de forma tal que pueda verificarse la fecha, lugar y congruencia de los datos con la realidad, van permitir evitar las simulaciones o imágenes falsas que pueden ser producidas con la intencionalidad de confundir o desorientar al rival.

"El Big Data implica una nueva forma de ver la información, revelando aquella que antes era difícil de extraer o que estaba oculta. En gran medida el Big Data implica una reutilización de la información. El valor de la información puede estar ligado a su capacidad para hacer predicciones acerca de acciones o eventos futuros. El Big Data puede ser percibido como un desafío para los principios clave de privacidad, en particular los principios de la finalidad y de la minimización de datos"[17].

En efecto, el Big Data tratándose de datos deportivos es una forma necesaria y novedosa de ver y tratar la información. Se reutiliza la información pero con una finalidad determinada que es definida por el entrenador y equipo técnico que utiliza esta información. Tratándose de la selección peruana de futbol y de otras selecciones nacionales que participan en

[15] GIL GONZALES, Elena: Ob.cit., página 52
[16] JOYANES AGUILAR, Luis: Ob.cit. página 135.
[17] 36° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. 13 al 16 de octubre de 2014. Balaclava Fort. Mauricio. Resolución sobre Big data.

campeonatos internacionales como el Mundial de 2018, su utilización tiene diversas utilidades. Las predicciones sobre acciones o eventos futuros son una constante en la labor de los entrenadores y equipo técnico. Coincidimos que es un aspecto clave el cumplimiento de los principios de protección de datos personales con el énfasis en el de finalidad y proporcionalidad.

"La rápida evolución tecnológica y la globalización ha planteado nuevos retos para la protección de datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha trasformado tanto la economía como la vida social…"[18]

Es en este sentido, tratándose de datos personales deportivos que la evolución tecnológica y la globalización, plantea retos a la protección jurídica, dada la magnitud, variedad, veracidad e intercambio de datos que supone su tratamiento sistemático y permanente. Confiamos que esta ponencia haya contribuido en genera interés sobre este importante tema.

6. CONCLUSIONES.

En el Mundial de Futbol de Rusia 2018 se han utilizado las Tecnologías de Información y Comunicaciones (TICs) en la competencia Deportiva, tal es el caso del Video Arbitraje (VAR) en el cual se analizan las situaciones de gol, la señalización o no de penales, la expulsión de un jugador, se evita confusiones en amonestaciones, da la potestad al árbitro de revisar jugadas y hay un análisis detallado de los datos personales producidos en un partido de futbol del Mundial en el Centro de Control donde se revisan las imágenes, para lo cual técnicos que administran el VAR reafirman o corrigen la decisión del árbitro.

Si bien esta ponencia se empezó a escribir teniendo como base la clasificación al Mundial de Futbol, se terminó de escribir al término de este importante evento. La utilización de las Tecnologías de la Información (TICs) del Video Arbitraje (VAR) se ha podido observar en los distintos partidos.

Además la preparación de los equipos y sus sistemas de información utilizados dan lugar a reflexionar sobre el Big Data, la Protección de Datos Personales en el ambiro deportivo es una necesidad a encararse desde el punto de vista del Derecho Informático y Digital para los acontecimientos que se han de suceder en el presente y en los años futuros.

BIBLIOGRAFIA

- CONGRESO DE LA REPUBLICA DEL PERU. Proyecto de Ley 1517/2016 –CR: "Proyecto que establece la Ley General del Deporte". En http://www.congreso.gob.pe

[18] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Numeral 6 de los considerandos.

-GIL GONZALES, Elena: “Big Data, Privacidad y Protección de Datos”. Protección de Datos Personales. Accesit en el Premio de Investigación de 2015. Ed. Agencia Española de Protección de Datos Personales. Madrid, España. 2016. 441 paginas.
- JARA, Umberto: “El Camino a Rusia: La Historia Secreta de la Hazaña y sus protagonistas”. Ed. Planeta.. Lima, Perú. Primera Edición. Marzo 2018. 134 páginas.
-JOYANES AGUILAR, Luis: “Industrias 4.0. La Cuarta Revolución Industrial”. Ed. Alfa Omega. Bogotá, Colombia, 2017. 471 páginas.
- SANCHEZ, Luis Javier: “El Big Data irrumpe en el deporte para mejorar las decisiones estratégicas”. En Confilegal. Madrid, España 07 de mayo de 2017. En https://confilegal.com/20170507-la-aume-reclama-una-politica-de-estado
-Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos
-Resolución sobre Big Data. 36° Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. 13 al 16 de octubre de 2014. Balaclava Fort. Mauricio
- Resolución Directoral N° 049-2016-JUS/DGDP de 7 de Junio de 2016. Procedimiento Trilateral de Tutela. En https://www.minjus.gob.pe/proteccion-de-datos-personales/

Regulación sobre TIC y los riesgos sobre la Libertad de Expresión en América Latina.

Por: ***José Adalid Medrano M.***
Costa Rica

Introducción

Las tecnologías de la información y comunicación (TIC) han transformado a la sociedad moderna, debido a la estrecha importancia que esta ha ido adquiriendo en sus actividades sociales, culturales, académicas, económicas y casi cualquier actividad realizada por el ser humano. La ubicuidad que han ido adquiriendo las TIC representa un importante reto regulatorio, ya que cualquier limitación sobre la utilización de estas puede conllevar restricciones de derechos fundamentales que son esenciales para toda democracia.

La disminución de la brecha digital ha contribuido a la proliferación de "influenciadores" de todos los estratos sociales, quienes buscan incidir en las áreas de su interés, desde el activismo social hasta la moda, pero de forma conjunta o individual colaboran en la construcción de una nueva sociedad cuya piedra angular es la libertad de expresión por medios digitales.

Para los activistas sociales, en países represivos, es esencial la utilización de seudónimos y herramientas tecnológicas que les permita mantener su identidad protegida, con el fin de escapar de la persecución de quienes se sienten incómodos con sus denuncias o artículos de opinión sobre temas que se busca ocultar.

Estrategias similares y herramientas tecnológicas también son utilizadas por delincuentes informáticos para ocultar su rastro, lo que suele tomarse como excusa para buscar la criminalización de conductas que por sí mismas no representan peligro, pero que al sancionarse penalmente puede utilizarse para perseguir a ciudadanos que le resulten incómodos para un gobierno.

El desconocimiento de la población con respecto a la terminología de las TIC o las consecuencias de criminalizar ciertas acciones puede llevarlos a aceptar sin ningún tipo de oposición legislación que pone en riesgo el ejercicio de la libertad de expresión en un país.

En países latinoamericanos como Perú, Honduras, Nicaragua y Costa Rica ya han surgido movimientos para luchar contra proyectos de ley que han considerado que podrían utilizarse para poner una mordaza en la población.

Justificación.

Esta investigación analiza los riesgos que conlleva la regulación sobre TIC en países latinoamericanos sin el debido proceso de consulta multisectorial.

Objetivos

- Analizar los riesgos predominantes en la utilización de TICS que pueden ser abordados en nuevas regulaciones.
- Identificar retos en las principales tendencias regulatorias sobre TIC.

Riesgos en la utilización de las TIC

La utilización de medios digitales conlleva riesgos de seguridad sobre los cuales la mayoría de la población no tiene conciencia, dado que la enseñanza sobre ciberseguridad no es algo generalizado, aún en la educación superior relacionadas con las TIC, lo que hace que exista una

mayor vulnerabilidad de los usuarios que suelen ser víctimas, inclusive en ataques poco sofisticados.

La lucha contra la ciberdelincuencia inicia desde la educación, ya que todo usuario debe saber qué hacer para evitar ser víctima de un delito informático o reducir los riesgos; pero también debe conocer qué debe hacer y qué no, cuando se da cuenta que ha sido víctima de un delito cometido por medios informáticos. Lo primero, con el fin de hacerle más difícil el trabajo a los ciberdelincuentes y la segunda con el fin de reducir la impunidad. Muchas víctimas de delitos informáticos borran o manipulan evidencia digital por desconocimiento y terminan facilitándole al delincuente salir impune.

Desde la perspectiva preventiva, se debe aprender a dominar los controles de privacidad que brindan las herramientas tecnológicas y así dificultar el acceso a los datos personales por parte de desconocidos. La decisión sobre qué datos y cómo deben ser tratados no es otra cosa que el ejercicio del derecho fundamental de la autodeterminación informativa[1] y este es un eje base de la seguridad informática de los individuos a nivel personal.

A continuación, se analizarán las amenazas predominantes en la utilización de las TIC.

El Phishing

Los ciberdelincuentes utilizan el engaño para poder tener acceso a datos personales de carácter confidencial o de acceso restringido con el objetivo final de atacar un sistema informático con información privilegiada obtenida, como lo puede ser una contraseña o datos del sistema que le permitan saber cómo atacarlo. Lo anterior se conoce como ingeniería social.

El "**Phishing"** lo podemos definir como un abuso informático "generalmente cometido a través del envío masivo de correo electrónico o SMS, suplantando la identidad de terceros mediante el uso de ingeniería social, con el fin de hacerse con información confidencial del usuario o instalar otro tipo de *malware"*[2].

Los usuarios suelen carecer de cultura de protección de datos personales, por lo que ante consultas por teléfono o correo electrónico, donde les requieren datos de carácter personal, los brindan en cantidades importantes, lo que le facilita el trabajo a los delincuentes. Si existiera mayor cultura digital y las personas se acostumbraran a no facilitar datos personales por vías no presenciales, la mayoría de los delitos donde se utiliza el phishing en los actos preparatorios no tendrían éxito.

En la estafa informática, el phishing se encuentra en el *iter criminis y* el delincuente busca obtener información como contraseñas y/o datos del segundo factor de autenticación que le permitan suplantarle la identidad a la víctima para realizar transferencias ilegítimas de fondos. Tomando en cuenta que los sistemas informáticos bancarios suelen ser difíciles de vulnerar, si las personas aprendieran a protegerse de ataques de ingeniería social, como el *phishing*, se podría reducir de forma significativa este tipo de delito.

Malware

En el año 2010 un artículo de la Revista Wired "*The Web is dead, long live the internet"* causó mucho revuelo ya que indicaba que la Web se encontraba muerta y que lo que seguía era un mundo de aplicaciones. Ocho años después podemos indicar que la visión de dicho artículo apuntaba al lugar correcto, ya que ahora las personas dependen de diferentes aplicaciones para distintas funciones, por lo que se han acostumbrado a instalar de forma continua aplicaciones para

[1] El derecho que tiene toda persona de decidir sobre el flujo de datos de carácter personal concernientes a su persona.
[2] GONZÁLEZ RUISÁNCHEZ, Susana, 2018, *Glosario de terminología TIC*. 1. Madrid: Abogacía Española, Consejo General, p. 45.

distintas acciones. Lo que ha llevado a los delincuentes a buscar instalar sus aplicaciones en los dispositivos de las víctimas.
Los programas informáticos maliciosos son aquellos que atentan contra el titular del sistema informático y sus fines son tan diversos como lo son las actividades delictivas. De acuerdo a Kaspersky, el 29.4% de los usuarios de computadoras fueron objeto de un ataque utilizando la web como medio de ataque en el año 2017[3].

La lucha contra el *malware* requiere de la ayuda de los desarrolladores de los sistemas operativos que utilizan miles de usuarios, ya que los ciberdelincuentes suelen aprovecharse de errores de programación o vulnerabilidades con el fin de obtener un beneficio.

Una de las formas de protegerse de este tipo de ataque es a través de la constante actualización de los sistemas, por lo que los usuarios dependen de la rápida corrección por parte de las empresas desarrolladores quienes a su vez dependen de la celeridad con que los usuarios instalen los parches de seguridad. Lo que nos deja claro que es una lucha que solo puede librarse de forma coordinada y en conjunto.

El *malware* también puede propagarse a través de la utilización de sitios web atacantes, que son aquellos que intentan explotar vulnerabilidades de los navegadores de los usuarios con el fin de obtener privilegios sobre el sistema, con lo que podrían realizar, entre otras cosas, la instalación de un programa malicioso.

El ransomware "es software malicioso que al infectar nuestro equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar nuestros archivos quitándonos el control de toda la información y datos almacenados"[4]. Es una de las amenazas más fuertes en este momento, en el año 2017, de acuerdo a Kaspersky, más de 939 722 usuarios únicos de Kaspersky Security Network fueron atacados, incluyendo más de doscientos cuarenta mil usuarios corporativos[5].

Sin embargo, para el año 2018 los programas informáticos maliciosos de minería oculta están superando al *ransomware* como la principal amenaza:

"El aumento en la cantidad de ataques con malwares mineros casi duplica las cifras registradas en 2016, que superan los 1,87 millones, pues Kaspersky Lab estima que se produjeron 2,7 millones de ataques con minería maliciosa a computadores tan solo en 2017.[6]

Por otro lado, el cibercrimen no es un área exclusiva del crimen organizado y en el caso del *malware* también es utilizado por parte de personas celosas con el fin de mantener control sobre su pareja, lo que nos aleja del cibercrimen organizado y nos lleva al cibercrimen que se realiza en el hogar.

Suplantación de identidad

Los cibercriminales crean perfiles de las personas a través de la recolección de información personal que se encuentra en fuentes disponibles al público o a través de la adquisición en el mercado, regularmente en el internet oscuro, donde se acepta como método de pago las criptomonedas, que le permiten al delincuente ocultar su identidad.

---

[3] KASPERSKY SECURITY BULLETIN: OVERALL STATISTICS FOR 2017, 2018, KASPERSKY, P. 5
[4] ¿Qué es un Ransomware?, Panda Security (en línea), . *[Accedido 18 de Julio, 2018]. Disponible en:* https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/
5. KASPERSKY SECURITY BULLETIN: OVERALL STATISTICS FOR 2017, 2018, KASPERSKY. P. 11
[6] *RIVERO, JACKELINE, 2018, Kaspersky Lab: mineros ocultos sustituyen al ransomware como modelo de negocios de cibercriminales | CriptoNoticias [online]. 2018. [Accedido 18 de Julio, 2018]. Disponible en: https://www.criptonoticias.com/seguridad/kaspersky-lab-mineros-ocultos-sustituyen-ransomware-modelo-negocios-cibercriminales/*

Con los datos personales de las víctimas les pueden suplantar la identidad por medios electrónicos con fines distintos, desde el acoso cibernético hasta la estafa informática.
El robo de datos personales también puede utilizarse para crear un perfil falso en redes sociales para engañar menores de edad y así seducirlos, obtener documentos de índole íntima y/o buscar un encuentro físico con el menor, con el fin de abusarle o violarle[7].

A través de la utilización de una cantidad importante de datos personales de una persona se puede lograr realizar montajes en video o audio de personas con las que se logra un montaje creíble para terceros que quien se encuentra realizando acción en video es la persona que está sufriendo lo que se conoce como *deepfakes* y que algunos expertos advierten que este abuso informático podría ayudar en la manipulación de las próximas elecciones de los Estados Unidos:

> «Un reciente estudio titulado 'Inteligencia artificial y seguridad internacional' indica cómo los DeepFakes, una técnica de inteligencia artificial (IA) utilizada para crear imágenes o videos falsos de gente real, representa una de las mayores amenazas de esta tecnología.
>
> Según la explicación de los autores del estudio, los sistemas de inteligencia artificial *"son capaces de generar grabaciones de voces sintéticas con sonido realista"* de cualquier individuo del cual exista suficiente registro para entrenar a la inteligencia artificial.
>
> Los videos generados por DeepFakes son normalmente fáciles de detectar por cualquier persona, no obstante, el avance de esta tecnología va tan rápido que en menos de cinco años podría llegar a engañar a cualquier ojo u oído sin entrenamiento para detectar estas falsedades».[8].

Para luchar contra flagelos como el citado supra lo más importante es que las personas cuiden sus datos personales, para no darles material a los delincuentes para que puedan realizar estos montajes tan creíbles y por lo tanto dañinos.

Noticias falsas

En los últimos años han surgido acusaciones serias de manipulación del electorado con noticias falsas, lo que ha dejado expuesto a las plataformas tecnológicas por el poco esfuerzo que han puesto en el combate de los llamados *fake news*, debido a que esta técnica ha podido ser utilizada por gobiernos extranjeros para incidir en un resultado.

El caso más emblemático es el de las elecciones de los Estados Unidos en el año 2016, donde se piensa que existió una manipulación del gobierno ruso, lo que le ayudó a Donald Trump a llegar al poder, como lo relata la BBC Mundo:

> "Trece ciudadanos y tres compañías rusas fueron acusadas formalmente este viernes por el Departamento de Justicia de Estados Unidos de interferir en las elecciones presidenciales de 2016. Se les acusa de "violar las leyes criminales para interferir en los comicios de EE.UU. y los procesos políticos", señaló la oficina del fiscal especial Robert Mueller, quien investiga la presunta interferencia rusa en la campaña.

[7] Conducta conocida por su nombre en inglés *Child Grooming.*
[8] Expertos advierten que los DeepFakes podrían influenciar las elecciones de Estados Unidos en 2020, TekCrispy [En línea]. *[Accedido 18 de Julio, 2018]. Disponible en: https://www.tekcrispy.com/2018/07/12/expertos-advierten-deepfakes-influencia-elecciones-estados-unidos/*

> Entre sus operaciones, figuran la comunicación de "información despectiva sobre Hillary Clinton, denigrar a otros candidatos como Ted Cruz y Marco Rubio, y apoyar a Bernie Sanders y al entonces candidato Donald Trump"[9].

Recientemente también salieron a relucir las estrategias utilizadas para difundir las noticias falsas de acuerdo a los intereses de sus objetivos, a través del tratamiento ilegal de datos personales de estos. Las controversiales acciones consistieron en lo siguiente:

> "Un modelo de psicología y un algoritmo de extraordinaria precisión sirvieron a Cambridge Analytica para analizar los perfiles de millones de usuarios de Facebook e intentar influenciar en sus votos.
> Alexander Nix, exjefe de la compañía británica, dijo que había logrado hacer un perfil de personalidad de "cada adulto en Estados Unidos" y de esta forma había conseguido influenciar en el resultado de las elecciones que convirtieron a Donald Trump en presidente de Estados Unidos.
> El modelo de los cinco grandes rasgos de personalidad, que se utiliza en psicología, le sirvió de base."[10].

La responsabilidad ha recaído sobre la plataforma tecnológica quien para la fecha de los hechos permitía que con el consentimiento de un usuario de la red social se recopilaran datos personales de sus amigos, lo cual es una flagrante vulnerabilidad y violación de las diferentes leyes de protección de datos personales donde Facebook tiene presencia.

Al mismo tiempo, Facebook nunca se cercioró que las empresas que creaban aplicaciones que capturaban datos personales, a través de su plataforma, cumplían con los términos de servicio de la red social, por lo que esto fue aprovechado para realizar actos de captación de datos personales a gran escala.

Acoso digital.

La ubicuidad de la tecnología en la sociedad moderna y la dependencia tecnológica que va generando en los ciudadanos hace que estas vayan formando parte de nuestra realidad, por lo que todo lo que suceda en el mundo virtual tenga un efecto importante sobre las personas.

En el caso del acoso por medios electrónicos puede generar un impacto psicológico en las víctimas bastante fuerte, debido a que dependiendo de los recursos tecnológicos con los que cuente el acosador, así hará notar su presencia alrededor de la víctima, quien confundirá el acoso digital con peligro en el mundo físico.

El acoso digital puede realizarse a través de acciones que encuadran en un tipo penal informático, por lo que pueden perseguirse penalmente, pero también pueden realizarse a través de abusos informáticos que no se encuentran tipificados en el Código Penal, por lo cual las víctimas pueden sentirse desprotegidas cuando se presentan este tipo de acciones.

En el caso de España, la Ley Orgánica 1/2015 reformó al Código Penal e introdujo el acoso incesante a una persona en el artículo 172 ter que reza lo siguiente:

---

[9] El Departamento de Justicia de Estados Unidos acusa a 13 ciudadanos rusos de interferir en las presidenciales de 2016, 2018. *BBC News Mundo* [en línea],.. *[Accedido 18 de Julio, 2018]*. *Disponible en:* https://www.bbc.com/mundo/noticias-internacional-43092239 .

[10] Cómo el algoritmo de Cambridge Analytica analizó la personalidad de millones de usuarios de Facebook, BBC News Mundo [en línea], *[Accedido 18 de Julio, 2018]*. *Disponible en:* https://www.bbc.com/mundo/media-43655680

«1. Será castigado con la pena de prisión de tres meses a dos años o multa de seis a veinticuatro meses el que acose a una persona llevando a cabo de forma insistente y reiterada, y sin estar legítimamente autorizado, alguna de las conductas siguientes y, de este modo, altere gravemente el desarrollo de su vida cotidiana:

1. ª La vigile, la persiga o busque su cercanía física.
2. ª Establezca o intente establecer contacto con ella a través de cualquier medio de comunicación, o por medio de terceras personas.
3. ª Mediante el uso indebido de sus datos personales, adquiera productos o mercancías, o contrate servicios, o haga que terceras personas se pongan en contacto con ella.
4. ª Atente contra su libertad o contra su patrimonio, o contra la libertad o patrimonio de otra persona próxima a ella.

Si se trata de una persona especialmente vulnerable por razón de su edad, enfermedad o situación, se impondrá la pena de prisión de seis meses a dos años.
2. Cuando el ofendido fuere alguna de las personas a las que se refiere el apartado 2 del artículo 173, se impondrá una pena de prisión de uno a dos años, o trabajos en beneficio de la comunidad de sesenta a ciento veinte días. En este caso no será necesaria la denuncia a que se refiere el apartado 4 de este artículo.
3. Las penas previstas en este artículo se impondrán sin perjuicio de las que pudieran corresponder a los delitos en que se hubieran concretado los actos de acoso.
4. Los hechos descritos en este artículo sólo serán perseguibles mediante denuncia de la persona agraviada o de su representante legal.»

Sobre este tipo penal el autor CÁMARA Sergio, indica "Las conductas de stalking afectan el proceso de formación de la voluntad de la víctima en tanto que la sensación de temor e intranquilidad o angustia que produce el repetido acechamiento por parte del acosador le lleva a cambiar sus hábitos, sus horarios, sus lugares de paso, sus números de teléfono, cuentas de correo electrónico e incluso de lugar de residencia y trabajo. Se protege asimismo el bien jurídico de la seguridad. Esto es el derecho al sosiego y a la tranquilidad personal. No obstante solo adquirirán relevancia las conductas que limiten la libertad de obrar del sujeto pasivo, sin que el mero sentimiento de temor o molestia sea punible. Por último hemos de advertir que, aunque el bien jurídico principalmente afectado por el *stalking* sea el de la libertad, también pueden verse afectados otros bienes jurídicos como el honor, la integridad moral o la intimidad, en función de los actos en que se concrete el acoso"[11].

En opinión de las autoras DAVARA Laura y DAVARA Elena, este artículo viene a dar cabida "a todas aquellas actuaciones -molestas y altamente dañinas- que, sin duda, causan un menoscabo en la víctima, tanto a lo que respecta a su propia libertad como a su dignidad y seguridad. Y es que, tal y como establece el propio artículo, las acciones llevadas a cabo con objeto de acosar incesantemente llevan aparejada la alteración grave del desarrollo de la vida cotidiana"[12].

En la resolución 416/2017 de la Audiencia Provincial de la Coruña el tribunal ahonda sobre este tipo penal:

«Ya respecto al tipo penal explica el Tribunal Supremo que "Con la introducción del art. 172 ter CP nuestro ordenamiento penal se incorpora al creciente listado de países que cuentan con un delito con esa morfología. La primera ley antistalking se aprobó en California en 1990. La iniciativa se fue extendiendo por los demás estados confederados hasta 1996 año en que ya existía legislación específica no solo en todos ellos, sino también

[11] ARROYO CÁMARA, S, La primera condena en España por acecho o stalking. Quadernos de criminología: revista de criminología y ciencias forenses, Sociedad Española de Criminología y Ciencias Forenses, España, Nº. 35, 2016, p. 40.
[12] DAVARA Elena, DAVARA Laura, Delitos Informáticos, primera edición, Editorial Aranzadi, España, 2017, p. 177

un delito federal. Canadá, Australia, Reino Unido, Nueva Zelanda siguieron esa estela a la que se fueron sumando países de tradición jurídica continental: Alemania (Nachstellung), Austria (behrrliche Verfolgung), Países Bajos, Dinamarca, Bélgica o Italia (atti persecutori). En unos casos se pone más el acento en el bien jurídico seguridad, exigiendo en la conducta una aptitud para causar temor; en otros, como el nuestro, se enfatiza la afectación de la libertad que queda maltratada por esa obsesiva actividad intrusa que puede llegar a condicionar costumbres o hábitos, como única forma de sacudirse la sensación de atosigamiento."

En los intentos de conceptualizar el fenómeno del *stalking* desde perspectivas extrajurídicas -sociológica, psicológica o psiquiátrica- se manejan habitualmente, con unos u otros matices, una serie de notas: persecución repetitiva e intrusiva; obsesión, al menos aparente; aptitud para generar temor o desasosiego o condicionar la vida de la víctima; oposición de ésta... Pues bien, es muy frecuente en esos ámbitos exigir también un cierto lapso temporal. Algunos reputados especialistas han fijado como guía orientativa, un periodo no inferior a un mes (además de, al menos, diez intrusiones). Otros llegan a hablar de seis meses.

Esos acercamientos metajurídicos no condicionan la interpretación de la concreta formulación típica que elija el legislador. Se trata de estudios desarrollados en otros ámbitos de conocimiento dirigidos a favorecer el análisis científico y sociológico del fenómeno y su comprensión clínica. Pero tampoco son orientaciones totalmente descartables: ayudan en la tarea de esclarecer la conducta que el legislador quiere reprimir penalmente y desentrañar lo que exige el tipo penal, de forma explícita o implícita.

No es sensato ni pertinente ni establecer un mínimo número de actos intrusivos como se ensaya en algunas definiciones, ni fijar un mínimo lapso temporal. Pero sí podemos destacar que el dato de una vocación de cierta perdurabilidad es exigencia del delito descrito en el art. 172 ter CP, pues solo desde ahí se puede dar el salto a esa incidencia en la vida cotidiana. No se aprecia en el supuesto analizado esa relevancia temporal -no hay visos nítidos de continuidad-, ni se describe en el hecho probado una concreta repercusión en los hábitos de vida de la recurrente como exige el tipo penal.»

Como puede verse la fórmula utilizada por el Código Penal español es limitada en el sentido que excluye acciones que podrían afectar el bien jurídico a pesar de que la misma no se dé de una forma reiterativa pero con la suficiente fuerza para afectar el bien jurídico penalmente.

Problemática de la regulación de las TIC

Como hemos analizado, existen diferentes acciones que representan riesgos para los usuarios que deben ser reguladas, pero que si la tarea se le da a un legislador que responde a sus propios intereses, o a los de terceros, puede poner en riesgo la libertad de expresión, al sancionar acciones que pueden ser realizadas por activistas, periodistas o investigadores, pero que son incorporadas como delitos en una reforma al código penal.

Por lo anterior, toda legislación que busque regular las TIC debería ser consultada con la sociedad civil, especialistas locales e internacionales, organismos internacionales especializados en la materia, colegios profesionales afines y demás partes interesadas, con el fin de que puedan pronunciarse sobre la propuesta.

La libertad de expresión es el pilar de toda sociedad moderna y el ejercicio de la misma a través de medios tecnológicos se ha convertido en la forma predominante y la más efectiva, por lo que cada vez que se pretende regular las TIC existe mucha preocupación de que se busquen formas de censurar a la población.

Índice de Libertad de Prensa y Regulación.

En un país que no goce de libertades para que la población pueda expresarse libremente, se presentará problemas en la regulación de situaciones que presentan grandes retos para la sociedad moderna, al poder surgir sospechas de que se quiere brindar más herramientas al gobierno para que ejerza mayor control sobre la población. Por lo anterior, si no se realiza un proceso de consulta multisectorial se podría perder la paz y el orden en el país, en el caso de que la sociedad civil pueda detectar previamente anomalías en la propuesta de regulación o en el peor de los casos, simplemente se apruebe la normativa con portillos que pueden utilizarse en contra de derechos fundamentales.

La comunidad internacional debe estar alerta cuando países latinoamericanos con una democracia frágil avancen hacia una nueva regulación de las TIC vinculados con los siguientes temas:

- Leyes de protección de datos personales y derecho al olvido.
- Delitos relativos de la propiedad intelectual
- Delitos informáticos.

Un país que reprime a la prensa y a los ciudadanos que adversan el gobierno, puede querer utilizar regulación de las TIC en contra de los disidentes y de esta forma mantener un control sobre la información que circula en su territorio.

Protección de datos personales.

Una ley de protección de datos personales que no sea revisada por organismos internacionales, consultada con la sociedad civil y especialistas locales e internacionales, podría contener sanciones que podrían utilizarse en contra de diarios digitales o personas que publiquen denuncias en redes sociales.

Se debe comprender que la mayoría de denuncias que hace la ciudadanía incorporan de alguna u otra forma datos personales, por lo que es claro que no se puede obtener el consentimiento de los titulares de los datos personales para hacer las respectivas publicaciones y si no se incorporan excepciones importantes para que se pueda prescindir del consentimiento expreso en casos donde los datos sean de acceso irrestricto u obtenidos de fuentes públicas, podría ser utilizado como mordaza contra la población.

Es importante que en Latinoamérica se avance hacia una cultura de protección de datos personales, sin embargo, toda legislación sobre la materia debe tener garantías de que la misma no va a ser utilizada en contra del derecho de libertad de prensa o libertad de expresión.

Toda legislación no solo debe ser respetuosa de derechos fundamentales sino que también debe adecuarse al contexto político y social de un país, por lo que en países con democracias más frágiles la normativa de protección de datos personales debe ser más clara y a través de reglas transparentes proteger a los medios de comunicación tradicionales y no tradicionales de la censura que se podría imponer con una legislación abierta.

El derecho al olvido, que tiene base en el derecho a la calidad de información, lo que implica que todo dato personal debe ser veraz, **actual**, exacto y adecuado al fin, le da derecho a toda persona a que un dato que no sea actual no le afecte. Una normativa sobre derecho al olvido con portillos, podrían permitirle a un político “olvidar” hechos cubiertos en la prensa, para que así sus actos de corrupción sean borrados.

Delitos relativos a la propiedad intelectual.

Si bien es cierto mucho se ha avanzado sobre normativa de propiedad intelectual, la misma no necesariamente fue diseñada para un mundo moderno donde la mayoría los ciudadanos utilizan los medios sociales para expresarse.

Una reforma sobre la materia que permita una protección más expedita de los derechos de autor en plataformas digitales, en el contexto latinoamericano, puede utilizarse para obtener mecanismos para traerse abajo contenidos que no sean de agrado del gobernante de turno. Lo anterior no significa que no deban brindarse los mecanismos para que los autores puedan proteger sus obras, sino que debe garantizarse que los ciudadanos gocen de excepciones que le permitan ejercer el derecho de libertad de expresión y acceso a la información.

Dentro de las excepciones que debe brindarse se encuentran, lo que en el derecho anglosajón se conoce como el uso justo y extendido al uso de obras pero con fines de parodia o humor.

Como lo indica el autor CORREA, Carlos "Bajo el derecho de autor angloamericano, las excepciones se formulan caso por caso, y se fundamentan en la aplicación de principios generales amplios. **Estas excepciones se refieren a actos de "trato justo" o "uso justo", tales como copiar con fines de investigación, enseñanza, periodismo, critica, parodia y actividades realizadas por bibliotecas.** Un buen ejemplo es la doctrina estadounidense del "uso justo", la que sólo provee lineamientos legislativos generales y concede un amplio margen a los tribunales para interpretar lo que puede ser permisible en instancias específicas. **Se define el "uso justo" como una norma racional que se basa en la equidad y que permite que se usen materiales protegidos en ciertas condiciones, sin el consentimiento del titular del derecho"[13]**

En la actualidad, existe una cultura del meme, donde los ciudadanos se expresan mediante este tipo de imágenes que suelen utilizar contenido protegidos por los derechos de autor, sin autorización del titular de la obra, sin fines de lucro y en ejercicio del derecho de libertad de expresión desde fines meramente humorísticos hasta críticos hacia un tema de interés general.

Recientemente en el Parlamento Europeo se estuvo discutiendo una propuesta de la Comisión Europea para reformar las normas comunitarias europeas sobre derechos de autor, que en medios sociales se denunció sobre el riesgo hacia la cultura del meme. En el portal de noticias 20 Minutos lo explican bien: "El famoso artículo 13 de esta propuesta, es el que pasaría más factura al Internet que ahora conocemos. Si entra en vigor, YouTube, Instagram, Twitter y eBay deberán instalar filtros automáticos y algoritmos para evitar que sus usuarios compartan contenidos protegidos por derechos de autor. La finalidad de este artículo, por tanto, es localizar el material que viole las leyes del copyright…Según las leyes de propiedad intelectual vigentes se puede intervenir judicialmente ante la denuncia del propietario del copyright. Las plataformas online solo pueden borrar contenidos por este motivo solo si el autor de ellos lo denuncia. Con la nueva normativa no haría falta denunciarlo.

La propuesta de la Comisión Europea actuaría como un mecanismo de censura previa. ¿Dónde quedarían los memes? En principio en España estarían protegidos, de hecho si alguna publicación de este tipo supusiera conflicto, un juez podría sentenciar que la vulneración no existe debido al Derecho de Parodia que existe en nuestro país. En cambio, si la ley de copyright sale adelante, quien revisaría los contenidos sería un filtro informático y no un juez. Se presume, por tanto, que explicar el Derecho de Parodia a un algoritmo programado, para que no termine censurado, sería algo más complicado"[14]

[13] CORREA, Carlos, Uso justo en la era digital, 2004, Libros y ensayos N 79, Buenos Aires, p. 143.

[14] Lo que debes saber sobre la nueva normativa de copyright que se votará en el Parlamento Europeo, 20 Minutos [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: https://www.20minutos.es/noticia/3386718/0/normativa-copyright-parlameto-europeo-internet-derechos-autor/#xtor=AD-15&xts=467263

Debido a la presión ejercida en medios digitales y la campaña de concientización se logró que el Parlamento Europeo finalmente rechazara la propuesta con 318 votos en contra frente a 278 apoyos y 31 abstenciones, Con este resultado, se bloquea el inicio de las negociaciones por parte del Consejo de la UE y se envía a la ley sobre el copyright a un nuevo proceso de modificación en la que habrá que debatir un nuevo texto, que se volverá a votar del 10 al 13 de septiembre.[15]

Delitos Informáticos

Un delito informático es toda aquella acción delictiva informática dirigida a vulnerar la confidencialidad, integridad y disponibilidad de los sistemas o datos informáticos, o la autodeterminación informativa y/o la identidad en medios electrónicos.

Con la reducción de la brecha digital se incrementan los abusos informáticos[16], lo que genera el debate sobre si deben sancionarse penalmente dichas conductas, y existe un peligro sino se realiza un análisis previo sobre quiénes son los sujetos activos y si esto no puede atentar contra derechos fundamentales de los ciudadanos.

De las conductas criminales que representan mayores retos en su sanción penal son: propagación de malware, suplantación de identidad, acoso digital y noticias falsas.

Acoso digital y delitos contra el honor.

El reto al regular esta conducta se encuentra en la definición de la misma, la cual debe darle herramientas a las víctimas de acoso, sin que al mismo tiempo pueda ser utilizado por políticos o gobernantes interesados en denunciar a disidentes que hacen denuncias, las cuales puedan considerar como acoso en línea, pero no necesariamente configuren un delito de difamación, injuria o calumnia.

La fórmula encontrada por el legislador español, parece tener un buen balance, que permite que no pueda utilizarse en contra de la libertad de expresión, sin embargo, podría darse el caso que en un país latinoamericano se busque una fórmula más amplia que le permita en algún momento ser utilizado en contra de personas que realizan crítica abierta a un gobierno.

En el caso de los delitos contra el honor, los cuales en muchos países latinoamericanos son delitos de acción privada, se suele utilizar un argumento sobre la posible viralización de estos por encontrarse en medios sociales, lo que para algunos políticos debería generar una pena agravada.

En Costa Rica, en el presente año, un diputado cristiano presentó un proyecto de ley en este sentido. Dicho proyecto ha tenido muchas críticas por sus falencias técnicas y en un editorial del diario La Nación se levanta la voz sobre el riesgo que esto representa: "Una iniciativa del diputado Jonathan Prendas, del Partido Restauración Nacional, propone elevar las penas aplicables a los delitos contra el honor cuando sean cometidos mediante las redes sociales. El planteamiento no tiene sentido y entraña importantes peligros para la libertad de expresión"[17]. El proyecto tiene pocas posibilidades de convertirse en ley de la República, sin embargo, llama la atención la propuesta y el argumento utilizado.

[15] El Parlamento Europeo rechaza la nueva ley comunitaria sobre el copyright, El Economista [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: http://www.eleconomista.es/tecnologia/noticias/9254494/07/18/El-Parlamento-Europeo-rechaza-la-nueva-ley-comunitaria-sobre-el-copyright-.html

[16] El abuso informático, en sentido estricto, es aquella conducta no ética, cometida vía ordenador, la cual no cuenta con los elementos necesarios para ser considerada como delito. En sentido general, los delitos informáticos son a su vez abusos de la informática, pero no todo abuso informático puede considerarse delito.

[17] Editorial: El honor en las redes sociales , La Nación [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: https://www.nacion.com/opinion/editorial/editorial-el-honor-en-las-redes-sociales/O7KB44GURFDHBOSHCUFQTZCHJM/story/

En Nicaragua, en el presente año, el gobierno ha utilizado como excusa la lucha contra el flagelo del acoso digital para buscar controlar las redes sociales. Sobre esto, el medio de comunicación nicaragüense La Prensa informa: "Las redes sociales (Facebook, Twitter, Youtube, entre otras) medios masivos utilizados por los nicaragüenses para hacer denuncia social, están siendo amenazadas por el Gobierno del presidente designado por el Consejo Supremo Electoral, Daniel Ortega, y funcionarios públicos, que pretenden controlarlas bajo el argumento de combatir el ciberacoso y garantizar la seguridad ciudadana[18].

Esto nos deja claro que causas nobles como la lucha contra acciones que golpean a la ciudadanía puede ser utilizado por los gobiernos de turno para favorecer sus agendas de represión contra la libertad de expresión.

Malware

La propagación del malware, como fenómeno, representa un reto desde el campo regulatorio, aunque no sea una acción que sea realizada por activistas sociales, ni involucre un ejercicio de la libertad de expresión, pero sí que puede utilizarse en contra de los ciudadanos, en el caso que se regule la instalación de programas informáticos maliciosos por parte de las autoridades.

La instalación de *malware* con fines de investigación judicial no solo debe ser algo que se encuentre expresamente regulado por ley, sino que se debe delimitar en qué tipo de delitos puede realizarse la misma, ya que si no se restringe se podría prestar para abusos en contra de ciudadanos.

En México «de acuerdo con el reportaje "Gobierno espía: vigilancia sistemática a periodistas y defensores de derechos humanos", entre enero de 2015 y julio de 2016 ocurrió una serie de ciberataques en contra de comunicadores y activistas mexicanos.

El documento fue realizado por Artículo 19, R3D, Red en Defensa por los Derechos Digitales y Social Tic, Tecnología digital para el cambio social, apoyados por Citizen Lab. Los afectados, según el informe, son al menos 12 comunicadores y activistas que investigaron casos de corrupción gubernamental. También incluye a abogados que asisten a familiares de los 43 estudiantes desaparecidos de la Escuela Normal de Ayotzinapa, así como al hijo menor de edad de la periodista Carmen Aristegui. De acuerdo con el documento la empresa que diseñó el *malware* condiciona su venta a que se utilice únicamente para vigilar criminales, o prevenir amenazas de seguridad nacional»[19].

En este caso, vemos como la instalación de *malware* se realizó por parte de las autoridades del gobierno mexicano, de forma clandestina y sin que mediara autorización de un juez, lo que es todavía más preocupante y nos deja clara la importancia de estar vigilantes ante cualquier propuesta de regulación sobre TIC.

En la lucha contra la ciberdelincuencia especializada en propagar malware, no se debería tampoco sancionar el desarrollo de programas informáticos maliciosos, debido a que esta es una acción que de forma regular realizan los especialistas de empresas de seguridad para el estudio de este tipo de ataques. Pero sí debería incorporarse como delito la instalación y propagación de programas informáticos maliciosos.

[18] Gobierno de Ortega amenaza con controlar las redes sociales en Nicaragua, La Prensa [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: https://www.laprensa.com.ni/2018/03/12/nacionales/2390099-gobierno-de-ortega-apunta-canones-contra-redes-sociales

[19] Cómo es Pegasus, el software capaz de vigilarte usando la cámara y el micrófono de tu teléfono en el centro de un escándalo de espionaje en México, BBC Mundo [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: https://www.bbc.com/mundo/noticias-america-latina-40336088

Noticias falsas

Las noticias falsas suelen utilizarse con distintos fines, pero el común denominador entre los diferentes tipos de *fake news* es el daño a la sociedad al generar confusión al relatar hechos que son total o parcialmente falsos. Por su peligrosidad para cambiar el comportamiento de la población, es que a nivel mundial se busca luchar contra este flagelo y en muchos casos se piensa en sancionar penalmente este tipo de acciones, lo que conlleva riesgos para la libertad de expresión en países represivos o con presidentes sin mucha conciencia sobre la importancia de la libertad de expresión

En el caso del presidente de los Estados Unidos busca sancionar a los medios de comunicación que emitan noticias que se consideren falsas[20]. Acá es importante aclarar que para el presidente Trump, las *fake news* no necesariamente son noticias de hechos falsos, sino con un enfoque que no es de su agrado.

En Malasia hay un proyecto de ley que busca sancionar las noticias falsas, «se trata de la iniciativa "Anti *fake news* 2018" del gobierno del primer ministro, Najib Razak, que establece multas de unos US$123.000 y penas de hasta seis años de cárcel por crear, publicar o diseminar **noticias "total o parcialmente falsas" que afecten al país o a sus ciudadanos**.

"Esta ley tiene como objetivo proteger al público ante la proliferación de noticias falsas, garantizando al mismo tiempo la libertad de expresión, según lo previsto en la constitución federal", dijo la ministra de Leyes, Azalina Othman Said. El gobierno espera así frenar las "informaciones maliciosas" tanto de medios locales como extranjeros, incluido aquello compartido en blogs y redes sociales. La medida ha sido fuertemente criticada por opositores y activistas, que la consideran **un nuevo instrumento de censura** estratégicamente aprobado a puertas de las nuevas elecciones generales»[21].

Este es un claro ejemplo de cómo propuestas de regulaciones sobre TIC deben ser discutidas ampliamente junto con la sociedad civil, organismos internacionales, especialistas locales e internacionales, así como todas las partes interesadas en la materia. Si bien es cierto, Malasia tiene la propuesta más radical sobre el tema, no es el único que lo está valorando, ya que países como Francia y Alemania también han iniciado la discusión sobre cómo crear normativa para combatir las noticias falsas.

CONCLUSIONES

La falta de conocimiento sobre el funcionamiento de las TIC, aunado con los deseos de ejercer control sobre el flujo de informaciones que circulan en un país y así reprimir el pensamiento disidente, requiere mucha vigilancia internacional para evitar represión estatal.

Toda propuesta legislativa que pretenda regular la materia debería cumplir con lo siguiente:

- **Consulta multisectorial:** sociedad civil, organismos internacionales, especialistas locales e internacionales, empresa privada y grupos interesados.
- **Análisis constitucional**: debe pasar por un análisis constitucional con el fin de asegurarse que la misma no sea restrictiva de derechos fundamentales, como el de libertad de expresión y acceso a la información.

[20]Trump sugiere penalizar a cadenas de televisión para evitar "noticias falsas", 20 Minutos [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: https://www.20minutos.es/noticia/3158504/0/trump-sugiere-penalizar-cadenas-television-noticias-falsas/

[21]El país que castiga con hasta 6 años de cárcel a quienes difunden noticias falsas, BBC Mundo [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: https://www.bbc.com/mundo/noticias-43628414

- **Analizar el contexto nacional:** no deben realizarse copias de otras legislaciones con una realidad distinta a la del país, ya que una norma abierta en un país democrático puede no resultar perjudicial de derechos fundamentales, pero en un país represivo puede resultar en la represión de disidentes.

Bibliografía

GONZÁLEZ RUISÁNCHEZ, Susana, 2018, *Glosario de terminología TIC*. 1. Madrid: Abogacía Española, Consejo General, p. 45.

CORREA, Carlos, Uso justo en la era digital, 2004, Libros y ensayos N 79, Buenos Aires, p. 143.

DAVARA Elena, DAVARA Laura, Delitos Informáticos, primera edición, Editorial Aranzadi, España, 2017, p. 177

ARROYO CÁMARA, S, La primera condena en España por acecho o stalking**,,** Quadernos de criminología: revista de criminología y ciencias forenses, Sociedad Española de Criminología y Ciencias Forenses, España, Nº. 35, 2016, p. 40

El Departamento de Justicia de Estados Unidos acusa a 13 ciudadanos rusos de interferir en las presidenciales de 2016, 2018. *BBC News Mundo* [en línea], *[Accedido 18 de Julio, 2018]*. *Disponible en:* https://www.bbc.com/mundo/noticias-internacional-43092239 .

RIVERO, JACKELINE, 2018, Kaspersky Lab: mineros ocultos sustituyen al ransomware como modelo de negocios de cibercriminales, CriptoNoticias [online]. 2018. [Accedido 18 de Julio, 2018]. Disponible en: https://www.criptonoticias.com/seguridad/kaspersky-lab-mineros-ocultos-sustituyen-ransomware-modelo-negocios-cibercriminales/

KASPERSKY SECURITY BULLETIN: OVERALL STATISTICS FOR 2017, 2018. , KASPERSKY. p. 5-11

Expertos advierten que los DeepFakes podrían influenciar las elecciones de Estados Unidos en 2020, TekCrispy [En línea], *[Accedido 18 de Julio, 2018]. Disponible en: https://www.tekcrispy.com/2018/07/12/expertos-advierten-deepfakes-influencia-elecciones-estados-unidos/*

Cómo el algoritmo de Cambridge Analytica analizó la personalidad de millones de usuarios de Facebook, BBC News Mundo [en línea], *[Accedido 18 de Julio, 2018]. Disponible en:* https://www.bbc.com/mundo/media-43655680

El Parlamento Europeo rechaza la nueva ley comunitaria sobre el copyright, El Economista [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: http://www.eleconomista.es/tecnologia/noticias/9254494/07/18/El-Parlamento-Europeo-rechaza-la-nueva-ley-comunitaria-sobre-el-copyright-.html

El país que castiga con hasta 6 años de cárcel ha quienes difunden noticias falsas, BBC Mundo [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: https://www.bbc.com/mundo/noticias-43628414

Trump sugiere penalizar a cadenas de televisión para evitar "noticias falsas", 20 Minutos [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: https://www.20minutos.es/noticia/3158504/0/trump-sugiere-penalizar-cadenas-television-noticias-falsas/

Cómo es Pegasus, el software capaz de vigilarte usando la cámara y el micrófono de tu teléfono en el centro de un escándalo de espionaje en México, BBC Mundo [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: https://www.bbc.com/mundo/noticias-america-latina-40336088

Gobierno de Ortega amenaza con controlar las redes sociales en Nicaragua , La Prensa [en línea], *[Accedido 18 de Julio, 2018]*, Disponible en: https://www.laprensa.com.ni/2018/03/12/nacionales/2390099-gobierno-de-ortega-apunta-canones-contra-redes-sociales .

REPRESENTACIÓN Y PROCESAMIENTO DEL CONOCIMIENTO DEL OPERADOR PARA APOYAR LA TOMA DE DECISIONES EN CASOS LEGALES.

Por: ***Luis Raúl Rodríguez Oconitrillo***
Universidad de Costa Rica, San José, Costa Rica

Introducción

En este artículo se presenta un modelo matemático de representación y procesamiento del conocimiento legal de la percepción del juez, para el apoyo a la toma de decisiones jurídicas óptimas. El modelo se diseña utilizando dos tipos de capas de lógica y una interfaz cognitiva que las comunique. Implementa un proceso cognitivo legal que permite generar los constructos necesarios para formas de estructuras de conocimiento complejas. Utiliza matemática ordinaria de forma poco ordinaria, manteniendo un diseño y procesos simples, pero sin omitir detalles sobre los fundamentos cognitivos, enfocados a resolver problemas jurídicos complejos.

La sección II describe el fondo y la complejidad cognitiva jurídica, necesidades y antecedentes de esta investigación. Incluye la descripción de elementos jurídicos que el modelo de representación de la percepción debe de considerar. También se describen trabajos relacionados tanto a nivel de modelos como de sistemas que puedan implementar modelos de representación, encontrando que son insuficientes para satisfacer las necesidades de un modelo de representación y procesamiento de la percepción del juez.

En la sección III se describe el modelo mediante un sistema de símbolos y ecuaciones sobre la percepción del juez y la forma de representar el conocimiento. Se describe un Proceso Cognitivo Legal (PCL), una Capa de Lógica Legal Auto-epistémica (CLAE) y otra Capa de Lógica Legal No Expresiva (CLNE) que son fundamento para las ecuaciones de la percepción, estructuras complejas, y cálculos geométricos sobre elementos jurídicos. Al final del artículo se derivan algunas conclusiones y se discute el trabajo futuro.

El Problema: fondo, especificaciones y trabajo relacionado

El modelo inicia con el análisis 398 casos relacionados a la declaración judicial de abandono en el Juzgado de Niñez y Adolescencia del Primer Circuito Judicial de Costa Rica, luego se analizan 110 casos comprendidos entre los años 2001 al 2017 provenientes de los Tribunales de Familia y de la Sala Constitucional de la Corte Suprema de Justicia de Costa Rica.

Junto con la información anterior, se recopila e intercambia información sobre las operaciones judiciales con: magistrados de la Sala II de la Corte Suprema de Justicia de Costa Rica, distintos jueces de las ramas Laboral, Civil, Penal y Familia, y con distintos profesionales judiciales tales como: auxiliares, médicos y peritos psicológicos. Esto es la base del modelo de cognitivo jurídico aquí presentado.

El análisis mostró la necesidad, dentro de la operación judicial, de contar con un mecanismo de interpretar datos jurídicos en la lógica judicial para poder derivar inferencias de ellas seleccionando elementos dentro de los ámbitos legales del dominio jurídico. También identificó que dicho mecanismo debe de considerar lógica deóntica que especifica Carlos ALCHOURRÓN, lógica doxástica comentada por Angus MACINTYRE junto con lógica temporal expuesta por Luciano FLORIDI.

La forma en que el juez o magistrado piensa sobre los aspectos de un caso legal dentro de la operación judicial es a lo hemos llamado aquí la percepción de un juez o magistrado. Los jueces deben de contar con información pertinente y oportuna, que según su experiencia, son

indispensables para tomar decisiones sobre casos legales. Todo lo anterior mediante un modelo de representación y procesamiento del conocimiento legal.
1) Pregunta de Investigación: Basado en el análisis, existe la siguiente pregunta: ¿es posible construir un sistema de información basado en investigación de operaciones que pueda procesar las percepciones de los jueces y reutilizar dicha información para ayudar a otros jueces a tomar decisiones bien informadas?

Esta pregunta nos lleva a considerar el enfoque de Investigación de Operaciones (IO) para apoyar la toma de decisiones de un juez en el fallo de una sentencia. IO se basa en la aplicación del análisis científico para manejar problemas, dando a los responsables de la toma de decisiones: una plataforma cuantitativa frente a la incertidumbre, riesgos, relaciones complejas y forma de resolver intereses encontrados de los que menciona Philip MORSE.

Los enfoques de IO, como tales, han dominado esferas económicas, industriales y de negocios, más no así esquemas de conocimiento jurídico. En esta investigación desarrollamos una visión novedosa de IO, ya que se aplica al entorno legal de un país. Por otra parte, el objetivo más importante de la IO es la óptima toma de decisiones y desarrollo de las actividades, que en este caso serían jurídicas.

2) El fondo: El conocimiento usado en las operaciones para resolución problemas sociales se basa en la toma de decisiones legales que hace un juez usando su percepción. Estas decisiones y su impacto operacional implican la expresión de 1/3 del poder de un país a través de la resolución de un caso en disputa, debido a que un poder judicial es uno de los 3 poderes de un estado democrático. Entonces las decisiones de los jueces expresan la potestad de imperio BINGHAM que tiene un país, la cual les es delegada y depositada en dichas decisiones. El producto de sus decisiones es la sentencia y a su vez el servicio es la paz social.

Las decisiones en entornos legales se han enfocado tradicionalmente en el uso de sistemas de información que recuperen información principalmente de forma textual, proveniente de grandes y extensos volúmenes de datos, relativa a leyes, decretos, reglamentos, tratados internacionales y jurisprudencia. Otros se orientan a organizar y clasificar información.

Con dichos sistemas tampoco es posible recolectar, representar y procesar los aspectos que un juez considere relevantes sobre un caso y que sean vitales para la toma de decisiones bien informadas basándose en modelos de procesamiento del conocimiento.

Existen tecnologías de información y comunicación dentro del Sistema Judicial de Costa Rica que durante décadas han operado brindando archivos de información a usuarios comunes, abogados, jueces y magistrados sobre situaciones legales que necesitan ser decididas, pero ninguna operación judicial utiliza sistemas de información que permitan extraer y procesar datos sobre la percepción de un juez respecto un caso legal.

Ni en los sistemas anteriores, ni en las herramientas encontradas en la literatura actual, se evidencia alguno que provea un medio satisfactorio de extraer y procesar conocimiento útil para la toma de decisiones, así como ninguno de ellos enfoca el problema de cómo tratarse dentro de Investigación de Operaciones de tal forma que ayude a resolver conflictos y problemas de la sociedad que menciona John WARFIELD.

Los requisitos para las operaciones jurídicas, que un modelo de cognitivo legal debe considerar para brindar apoyo a la toma de decisiones legales, que en nuestro caso son los niños abandonados, son: (1) identificar elementos jurídicos es decir, datos sobre los hechos y las pruebas contenidos en el archivo que fue adquirido de una fuente judicial; (2) asociaciones, es decir, descripciones de cómo estos datos pueden relacionarse entre ellos; y (3) inferencias legales, es decir, una descripción de cómo procesar el conocimiento para que sea útil empleando. La sentencia de un caso debe ser declarada en términos de fundamentos de hecho y derecho.

Es precisamente en este punto la captura, representación y procesamiento del conocimiento jurídicos proporciona un enorme beneficio al sistema jurídico en su conjunto, pues permite gestionar el mismo de manera más eficaz y eficiente.
3) La percepción de un juez de una situación legal: La percepción de una persona sobre una situación se forma sobre la base de datos sensorial recolectada que menciona Edward SMITH y Stephen KOSSLYN, y el principal producto de ese proceso es un constructo que describe aspectos relevantes de la situación y que puede usarse para responder preguntas pertinentes sobre la misma al aplicarse algún tipo de lógica.

Entonces, la lógica deóntica es aplicada cuando el juez utiliza ideas y normas jurídicas junto con las experiencias jurídicas. La lógica doxástica es aplicada cuando se evalúa lo que el juez pueda creer de los hechos contenidos en testimonios, declaraciones juradas, peritajes y manifestaciones entre otros, y que el juez valora o no, como ciertas. La lógica temporal es aplicada al evaluar los recursos de revocatoria, apelación en subsidio, nulidad concomitante, procesos de revisión, emplazamientos y prescripciones entre otros. Pero para obtener la información de dichas lógicas se requiere una transformación de la información contenida en un expediente jurídico para lograr una interpretación epistemológica aceptable desde el punto de vista legal y obtener un constructo de la percepción legal.

Un modelo de representación que use la percepción de los jueces, respecto a los elementos de un caso jurídico debe de considerar 3 factores fundamentales: (1) vínculos entre elementos, (2) efecto de un elemento hacia otro e (3) importancia del elemento respecto a otros. Estos factores permiten identificar elementos relevantes con atributos de un caso y simultáneamente identifica rasgos que puedan generar una violación o no a un valor jurídico a tutelar.

4) Especificación del Problema: Con el fin de resolver un conflicto legal, el juez usa su propia interpretación respecto a los hechos, pruebas, principios y peticiones de las partes con el fin de tomar una decisión y resolver una situación jurídica. La representación histórica de lo que las partes solicitan y justifican acerca de una situación conflictiva, es lo que se conoce como el expediente, junto con las decisiones del juez. Sin embargo, el conocimiento acerca de cómo y por qué un juez toma una decisión en particular se pierde en el proceso y en el tiempo. Lo único que se incorporada en el expediente, respecto a las decisiones del juez, es la descripción del fundamento jurídico y referencia a los hechos probados y no probados, y usando básicamente esos elementos el juez toma decisiones. Esto indica claramente que un juez no tiene orientación sobre todas las posibles relaciones pertinentes a la cantidad y diversidad de elementos de un caso jurídico. Esto es indicador de una percepción holística sin un análisis detallado que puede inducir a error si no se considera los vínculos, efectos, importancias y relaciones de los elementos jurídicos.

Si bien es cierto el tema central sobre el conocimiento es su representación y procesamiento legal, en la investigación de operaciones, el modelo matemático a proponer debe de ser sostenible o aplicable en el tiempo para mantener decisiones óptimas. Aquí encontramos, que para hacerlo sostenible, se tiene que capitalizar el conocimiento concepto que trabaja Riccardo VIALE y Henry ETZKOWITZ, que para nosotros es legal. Si el conocimiento se pierde en el proceso y en el tiempo, no es posible crear reales estructuras ontológicas (informáticas) y epistemológicas completas y adecuadas.

Dicho esto, nuestro problema consiste en proporcionar una respuesta a la pregunta de investigación mencionada anteriormente, aquí se replanteada como una pregunta al problema: ¿en el proceso de toma de decisiones, existe un modelo matemático que represente y procese la percepción y experiencias de un juez en tiempo real, que ayude a filtrar e interpretar datos oportunos y relevantes de un caso legal?

5) Trabajo Relacionado: Algunos trabajos relativos a la representación del conocimiento y al diseño propuesto aquí, son descritos brevemente en ésta sección.

Pompeu CASANOVAS expone el uso de la Web Semántica para representar del dominio legal considerando las limitaciones de un caso para que el usuario las tome en su decisión. Otros modelos usan lenguajes descriptivos (DL) junto con ontologías de alto nivel (Upper Ontology) para mostrar un modelo conceptual de los eventos de un crimen como lo muestra Federico GONÇALVES DE FREITAS. Existen otros que tratan de enfocarse en el uso de estándares y emplear medios de descripción declarativa en lenguaje natural como Semántica en Vocabulario de Negocios y Reglas de Negocios (SBVR) y generar una representación del conocimiento usando fundamentos del Lenguaje de Remarcado Extensible (XML) a través de LegalRulML tal y como lo trabaja Xing WANG. También hay otros que mezclan ingeniería de requerimientos (RE) y reglas de normas legales para representar el conocimiento legal en el estudio de flujos de trabajo jurídicos tal y como lo indica Guido BOELLA. Unos usan Lógica Conceptual Atributiva con Complementos (ALC) basándose en lógica descriptiva para representar reglas legales tal y como lo trabaja Edward HAEUSLER. Existen otros que usan Marcos de Descripción de Recursos (RDF) con metadatos basado en Lenguaje de Marcado Extensible (XML) para representar el conocimiento tal y como lo usa M.P EBENHOCH. Ninguna de las formas de representación y procesamiento de conocimiento legal brindaron solución o contribución para responder al problema propuesto.

Para extender aún más la búsqueda fijamos la mirada a sistemas de información y herramientas que podrían mostrar formas de representar y procesar el conocimiento legal. Pero de igual forma en ninguno de ellos se encontró alguna solución o contribución para satisfacer nuestros requerimientos. Tal es el caso de (1) JUEZ que lo describe William BAIN, que trabaja sobre casos de asalto y asesinato. Utiliza justificaciones o la falta de ellas como métrica. GREBE el cual menciona Riccardo VIALE, utiliza documentaciones de los litigantes sobre los hechos y los casos para determinar y explicar las consecuencias de las decisiones. Vincent ALEVEN menciona a CATO, el cual plantea un entorno educativo para estudiantes de derecho el cual (1) organiza de argumentos, (2) obtiene diferencias entre los casos, y (3) evalúa la relevancia de los casos precedentes. Tom BINGHAM menciona a HYPO, el cual usa un razonamiento basado en casos legales utilizando argumentos exitosos o fallidos de situaciones legales basado en Common Law y no Continental Law.

Hasta éste punto, los modelos y sistemas anteriores revisados: (1) no usan, aclaran o identifican expresamente alguna lógica deóntica, doxástica y temporal en los procesos jurídicos y entorno al juez. (2) No hay una representación y procesamiento matemático de un caso legal considerando los atributos de los elementos jurídicos del expediente desde el punto de vista del juez. (3) No hay una representación y cálculo matemático, a través de factores, de la precepción del juez. (4) No hay comparación de atributos específicos entre jueces sobre los elementos legales, por ejemplo, sobre un valor jurídico a tutelar, que explique el cómo dos jueces, "A quo" y "A quem", caracterizan ese valor, tomando en cuenta el vínculo, efecto e importancia de dicho valor legal, no hay evidencia de que existan. (5) No consideran una metodología específica de procesamiento jurídico que inyecte el cómo y el porqué de la forma de pensar de un juez sobre un aspecto jurídico. (6) No están explícitamente diseñados en asistir a la toma de decisiones de los jueces, en sus operaciones jurídicas. (7) No permiten obtener o evaluar la relevancia de un atributo de un caso o de un caso en sí mismo. (8) Muchos solo se centran en conceptos para representación ontológica y semántica a través de diferentes lenguajes. (9) No proveen formas episódicas del caso (estado del caso en diferentes instancias judiciales), conforme los jueces trabajan, por lo tanto no es posible analizar las diferencias entre episodios iniciales, medios y avanzados del caso jurídico. (10) No permiten identificar y resolver conflictos entre jueces de diferentes jerarquías, inferior ("A quo") y superior ("A quem"), respecto a las decisiones tomadas en la sentencia. Debido a que un juez superior puede anular parcial o totalmente las decisiones en las sentencias del juez inferior, y tener la relación entre elementos jurídicos del por qué lo hizo, es vital. (11) No consideran, en el modelo, la filtración de información ruidosa, parcial e irrelevante del expediente

del caso, o de aquella que las partes en conflicto quieran inyectar. (12) Están diseñados para diferentes sistemas legales y no ofrecen una forma de poder representar o procesar el conocimiento para normativas de Ley Común (Common Law) y Ley Continental (Continental Law). (13) Se centran en las reglas de argumentación, usadas por los litigantes, no por los jueces. (14) No ofrecen un modelo de representación de la memoria basado en un modelo matemático de representación del conocimiento legal, que evalúe la incorporación de elementos jurídicos nuevos al caso a través del tiempo.

Por su parte, es bueno recalcar que las mismas desventajas de las referencias anteriores, facilitan un nuevo punto de vista sobre la desambiguación semántica, y por lo tanto se consideran para el análisis de requerimientos en nuestro enfoque. También dichos enfoques se consideran como forma de reducir la brecha entre las fuentes de informaciones textuales, sobre todo no estructuradas, y la especificación semántica de sus contenidos.

El modelo: símbolos, representación del conocimiento

El modelo se enfoca en representar y procesar el conocimiento de la percepción del juez de forma que genere información idónea para la toma de decisiones óptimas. El modelo tiene dos capas y una interfaz; utiliza matemática ordinaria de forma poco ordinaria, manteniendo un diseño lo más simple posible, pero sin perder detalle de los fundamentos cognitivos, orientado a resolver problemas jurídicos complejos.

La primera, es una capa de lenguaje gráfico como el que define Jianhui LUO, pero en nuestro caso es lenguaje gráfico expresivo el cual implementa lógica modal en donde se incluyen la lógica deóntica, lógica doxástica y la lógica temporal, especificada como Lógica Legal Deóntica-Doxástica-Temporal (LOL-DEDOTE), con la cual juez interactúa, esta capa se denomina Capa de Lógica Legal Auto-Epistémica (CLAE) debido a que puede expresar conocimiento o la falta de conocimiento sobre situaciones del caso legal. Esta primera capa se encarga de suplir el medio de expresividad fácil y compacta de los elementos jurídicos que el juez manipula tales como hechos, normas, pruebas, hechos probados entre otros es decir contiene los cuantificadores legales y entidades legales de los elementos del caso. La primera capa contiene los constructos legales conformados por los elementos jurídicos. La segunda capa indicada como Capa de Lógica Legal No Expresiva (CLNE), usa lógica proposicional, y se encarga del procesamiento de conectivas jurídicas, constantes normativas y variables jurídicas con valores de cierto o verdadero, con el propósito de generar los pre-constructos legales. Un reconstructo es un constructo legal en proceso de formación.

La capa CLAE se conecta e intercomunica con CLNE a través de una Interfaz Legal Cognitiva (ILC). La interfaz toma de la primera capa los elementos jurídicos y los envía a la segunda capa para construir el pre-constructo; cuando el pre-constructo es terminado se convierte en constructo y es enviado a la primera capa para ser usado por el juez.

La interfaz funciona usando principios de la dinámica de sistemas, definidos por David LUENBERGER, para poder representar estructuras complejas de un caso legal. La dinámica usa un pensamiento sistémico, definido por Patrick HESTER, pero en nuestro caso es jurídico para resolver dos cosas: (1) problemas de relaciones entre los pre-constructos legales, y (2) la asignación de propiedades a los pre-constructos. Asimismo, la dinámica de sistemas, para llevar acabo la ejecución del pensamiento sistémico, implementa un proceso cognitivo legal de pasos bien definidos, Figura 3, indicado como Proceso Cognitivo Legal (PCL), que desde la fase 1 a la 8 tiene dos propósitos: (1) identificar el elemento, (2) y saber el qué, por qué, cuándo y cómo usar el elemento jurídico.

Proceso Cognitivo Legal

El proceso cognitivo cuenta con una retroalimentación de pre-constructos entre la fase Estructura de Representación Cognitiva y la fase Resolución de Problemas Legales con el objetivo de generar

la estructura ontológica legal y la semántica de los constructos legales finales en forma de un grafo acíclico dirigido usado por el juez. Éste grafo es un diagrama de influencia (DI), tal y como lo define Michael RICHTER, en la toma de decisiones bien informadas por parte del juez. Por tanto, es el producto de las capas y la interfaz usando el proceso cognitivo (PCL).

Las relaciones del DI son los arcos, los elementos jurídicos son los nodos del diagrama. El constructo sería un conjunto específico de nodos y sus arcos, donde cada nodo y arco cuenta con atributos. Los atributos son estructurados en forma de vectores llave-valor, ejemplo: (estado niño, abandonado) y (estado parental, ausente).

Los constructos pueden organizarse en estructuras complejas dentro del DI. Dichas estructuras son la agrupación de un conjunto de conceptos legales, todos juntos forman un caso y un caso pertenece a un contexto legal específico en el dominio del discurso. Un ejemplo de concepto legal es Abandono de un Niño y un ejemplo de contexto legal es el área de Familia.

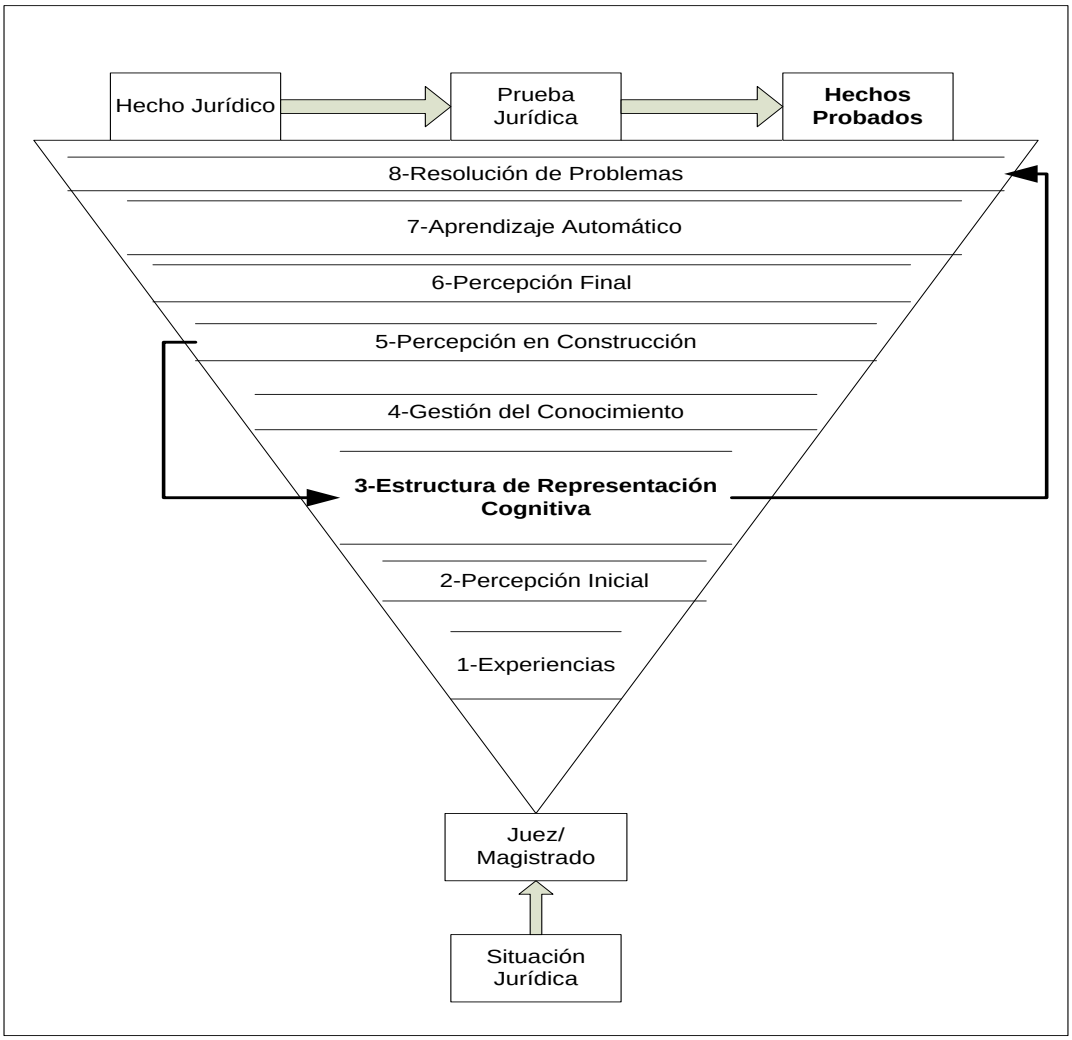


Figura 3. Proceso Cognitivo Legal

1) Ecuaciones de la Percepción: En nuestro modelo, para construir un sistema de símbolos que pueda representar el conocimiento del dominio del discurso, empleamos las dos las capas y la interfaz mencionados anteriormente. El análisis y modelamiento de los elementos jurídicos se hace mediante para generar el constructo, esto significa la utilización de un principio sistemático [20, p. 133] legal, creando constructos en forma de estructuras complejas, a partir de elementos atómicos legales; aquí empleamos el principio local-global [20, p. 96] llamado Incorporación de Elementos Atómicos Cíclicos (IEC).

En este punto, el proceso cognitivo es sistemático y retroalimentado. Lo que hace falta es un componente que se encargue de ensamblar los elementos jurídicos del constructo, este componente es un operador de construcción [20, p. 96-103] y es llamado Contructor Jurídico (CJ) indicado en la ecuación 1. En dicha ecuación, la estructura compleja E_c representa la estructura sistémica, o sea una estructura de constructos, A_i es la unidad atómica o elemento jurídico del constructo, *I* representa el índice de elementos jurídicos, *Cj* es el constructor jurídico de la estructura sistemática. Entonces la estructura compleja es igual a que un constructor jurídico ensamble las unidades atómicas jurídicas, tal que, cada valor del subíndice de la unidad pertenezca a un conjunto específico de índices de unidades.

$$E_c = Cj(\sum_{i=1}^{n} A_i | i \in I) \qquad (1)$$

Ahora, usando la ecuación 1, podemos representar el conocimiento jurídico de un caso legal mediante la ecuación 2; la variable *Pc* es la percepción del juez, enfocada a un contexto determinado *Cx* y a la sumatoria de los constructos legales Cn_i más las relaciones de los constructos Rc_i (sean relaciones entre conceptos del constructo o entre constructos) menos los datos no útiles del caso DnU_i (que pueden estar en el expediente físico). Con los DnU_i se podría establecer una razón entre el tamaño del expediente físico y los datos reales usados en el caso.

$$Pc = \left\{ Cx, \sum_{i=1}^{n} ((Cn_i + Rc_i) - DnU_i) \right\} \qquad (2)$$

2) Detalles de las Ecuaciones de la Percepción: En la ecuación 2 requiere la existencia un contexto jurídico *Cx*. Entonces, la ecuación 3 muestra que debe existir al menos un contexto tal que su índice *j* pertenezca dentro un índice contextual *J* superior, por ejemplo Familia e *I* a un valor en ese contexto.

$$Cx = \{\exists\ Cx_j | j \in J, I\} \qquad (3)$$

El ensamblaje de las unidades atómicas de los constructos y sus relaciones se representan en la expresión 4, donde cada constructor Cn_i y la suma de las relaciones Rc_i implican una sumatoria del vector de atributos $\vec{V_i}$, el cual esta compuesto del par de vectores de atributos y del vector de las relaciones dentro de los elementos atómicos del constructo, más el vector de los elementos atómicos insertados después de la sentencia $\overrightarrow{Aid_i}$, menos el vector de los elementos atómicos restados después de la sentencia $\overrightarrow{Ard_i}$, más el vector de las relaciones entre constructos (si existen), menos el vector de los elementos atómicos no útiles del expediente $\overrightarrow{DnU_i}$.

$$(Cn_i + Rc_i) \Rightarrow \sum_{i=1}^{n} \vec{V_i} = (\vec{A_i}, \vec{Ra_i}) + (\vec{Aid_i}) - (\vec{Ard_i}) + (\vec{Rc_m}) - (\vec{DnU_i}) \qquad (4)$$

Las adiciones y las sustracciones de la ecuación 4 se deben a los ajustes que cada estructura de constructos sufre según sea los recursos legales[1] aplicados. Las validaciones de las estructuras de constructos y sus cambios, están hechas por los propios jueces dentro del PLC, mediante las revisiones que hace el juez superior al juez inferior según su jerarquía.

3) Ecuaciones de Elementos del Constructo: Como se mencionó anteriormente, aplicando el PLC usando la CLAE y la CLNE junto con la ILC se obtienen las estructuras complejas de constructos para generar el DI. Ahora veremos cómo se constituyen los elementos jurídicos (nodos) y las relaciones entre ellos (arcos) dentro de los constructos.

Para ensamblar los nodos, el modelo les asigna un peso, que representa geométricamente el diámetro del nodo si lo hacemos en forma de círculo, y un orden de ingreso; de ser necesario el juez los puede cambiar.

Para los arcos, se usan los factores mencionados anteriormente: vínculo, efecto e importancia. Cada factor tiene un valor de medida y un valor de utilidad, ambos valores son número reales de dimensión finita dentro de un espacio euclidiano con vectores normados. Entonces la medida de un factor es un valor dentro de una escala continua finita, mientras que la utilidad de ese factor describe un valor virtual [20, p. 141].

Para aclarar lo anterior indicamos, que el factor vínculo, describe la utilidad de enlace entre elementos jurídicos. El factor efecto, describe la utilidad de impacto, mientras que la importancia describe la utilidad de relevancia. Para explicar mejor los valores de medida y la utilidad pensemos en un caso donde haya una prueba, dicha prueba genera un vínculo entre un hecho y otro, pero hay poco enlace, debido a que no hay suficiente prueba. Por su parte, pensemos ahora que el Hecho 1 afecta al Hecho 2, sin embargo dicho efecto no conlleva el suficiente impacto para considerarlo dentro del caso. Ahora, considere que pueden existir un conjunto de elementos, todos ellos de alta importancia, pero solo uno es más relevante que el resto del conjunto.

Aclarado lo anterior, indicamos que cuando dos factores se interrelacionan, se produce la medida y la utilidad del tercer factor, es decir, la medida y la utilidad de un factor es producto de función de los valores la medida y utilidad de los otros dos factores.

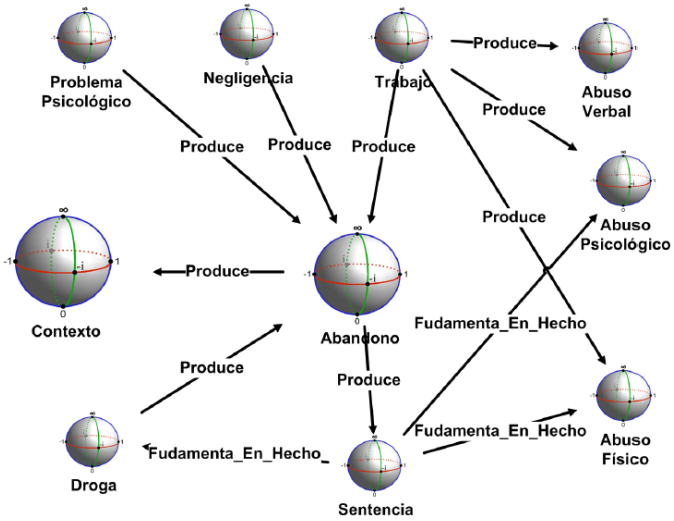


Figura 4. Diagrama de influencia cognitiva.

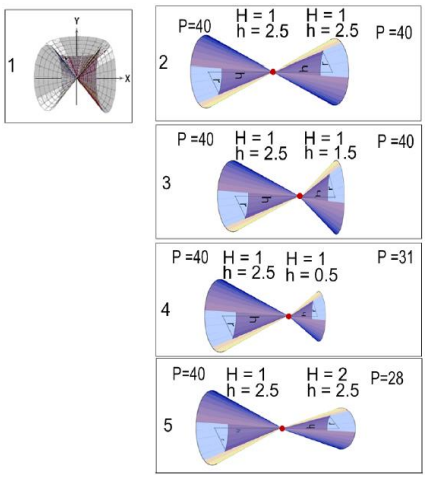


Figura 5. Simulación de resultados

[1] Los recursos pueden ser: revocatoria, apelación en subsidio, nulidad concomitante, revisión y aclaración según el contexto. Cada uno puede ser ejecutado por las partes, fiscales, defensores. Los recursos expresan la inconformidad y el derecho de reclamar en cada episodio del proceso jurídico.

La interrelación se logra utilizando funciones pitagóricas simples como la ecuación 5, donde el impacto *H* de un atributo es igual al resultado la raíz cuadrada del cuadrado del vínculo h^2 más el peso del atributo divido entre dos $P/2$ al cuadrado. El valor de utilidad del impacto es un atributo virtual que es establecido a la hora de construir la relación.

$$H = \sqrt{h^2 + (P/2)^2} \qquad (5)$$

En la ecuación 6 vínculos se obtiene del resultado de la raíz cuadrada del cuadrado del impacto sumado al producto de la división del peso entre dos y elevado al cuadrado.

$$h = \sqrt{H^2 + (P/2)^2} \qquad (6)$$

Ahora es adecuado indicar los pasos básicos al ensamblar un DI como el especificado en la

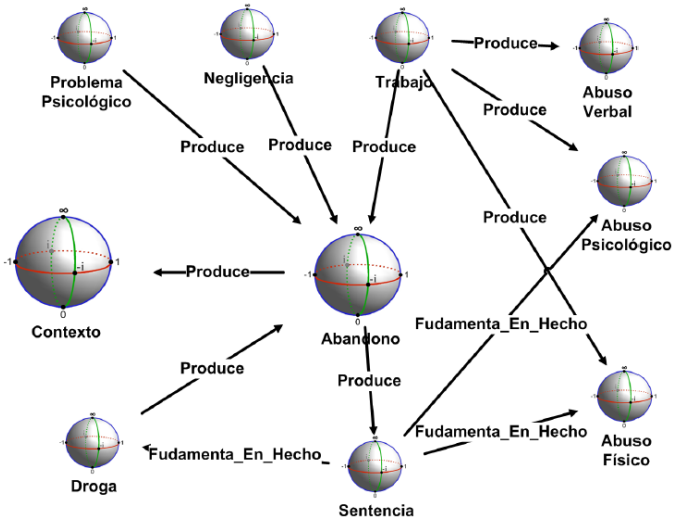


Figura 4; primero se identifican el concepto legal, luego los hechos relacionados a dicho concepto legal, posteriormente el resto de los elementos jurídicos de ser necesario; luego se indican los esos de los elementos. Segundo, se crean las relaciones semánticas (arcos) entre dichos atributos de los hechos, asignado el grado de impacto y el grado de vinculación a cada relación. Aquí juega un rol fundamental el *CJ* para obtener la medida de los factores, debido a que el juez podría no indicar ningún valor para los factores y solo enfocarse en hacer relaciones entre nodos. Si no se ingresa ningún valor para los factores el *CJ* toma para la importancia el orden, para el vínculo un valor derivado de la relevancia, y con ello calcula el tercer factor tanto para la medida como para la utilidad.

4) Interacción de los Elementos del Constructo: El *CJ* considera los pesos de los elementos su orden, junto con el vínculo, impacto e importancia para establecer las relaciones entre un elemento y otro en las estructuras del constructo. Pero para entender la forma dimensional de los nodos, se necesita la explicación e interpretación de la figura 3 en conjunto con la figura 2.

Primero, observando el DI de la figura 2, podemos explicar que los elementos como drogas, negligencia, problemas psicológicos y el trabajo generan el abandono de un niño. El trabajo se relaciona con elementos sobre abuso físico, verbal y psicológico indicando la generación de violencia sobre el menor de edad, además del abandono. Debido a que es un caso jurídico real, se ha simplificado el DI omitiendo las leyes, para efecto explicativos. En todo caso, de querer necesitarlas, basta con crear un nodo que represente la norma correspondiente y relacionarla mediante un arco con otro nodo, de igual forma aplica para las pruebas.

Luego la figura 3 los conos representan la proyección de un nodo hacia otro nodo, desde el centro del primero hasta cubrir el tamaño total del segundo nodo. La base del cono sería la circunferencia del segundo nodo, la altura h es el vínculo entre un nodo y otro, el radio r del segundo nodo representa el peso P del segundo nodo, el efecto de la relación sería la línea de la generatriz del cono. Para este ejemplo, se le asignan diferentes valores al peso P, efecto H y vínculo h para observar el cambio orático en la forma del cono, que constituye los nodos y los arcos.

Tomando cualquiera de los elementos jurídicos la figura 2, por ejemplo droga y luego ubicarlo en centro de alguno de los bloques del 1 al 5 de los pares de conos de la figura 3, se puede apreciar cómo se proyectaría sobre otro.

5) Aplicación del Espacio Euclidiano en Elementos del Constructo: La medición de las influencias dentro del constructo y entre constructos, se realiza usando principios sistemáticos [20] basado en geometría, cálculo de ángulos y valores de los atributos de las relaciones y los elementos jurídicos.

En la figura 4 los factores de impacto y el vínculo deben siempre de formar un ángulo respecto al peso de un elemento jurídico *P*, sea éste uno en un triángulo rectángulo. En caso que el ángulo $< 90°$ fuera agudo, y no forme un triángulo rectángulo, implica obtener una proyección ortogonal de los valores de impacto *H* de la relación y peso del elemento jurídico *P* con respecto al vínculo *h* de la relación. Esta proyección ortogonal de igual manera está definida en un espacio euclídeo. Esto significa que siempre podemos obtener los valores aun cuando el triángulo formado no sea rectángulo.

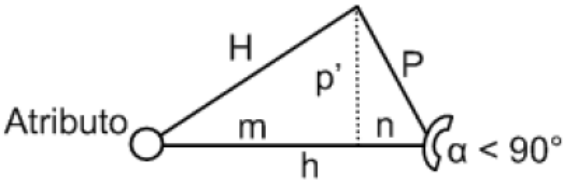


Figura 6. Ortogonalidad de Elemento Jurídico con ángulo α < 90°.

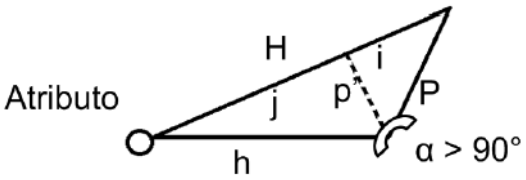


Figura 7. Ortogonalidad de Elemento Jurídico con ángulo α > 90°.

En la figura 4 la proyección ortogonal del impacto *H* es el vínculo *m*, y la proyección ortogonal del peso *P* sería el vínculo *n*.

El cambio de los factores y el peso del elemento jurídico se puede obtener de la expresión 7, donde se indica que para todo ángulo generado que sea menor de 90 existe por lo menos un valor del impacto H_i y un valor de peso P_i tal que el subíndice de cada uno pertenece a un conjunto de índices *I*, tales que cada impacto H_i implica un cambio en el vínculo que genera la proyección ortogonal *(h - n) = m* y cada peso P_i implica un cambio en el vínculo que genera la proyección ortogonal *(h - m) = n* lo que implica una función de cambio en el vínculo *h*. Hay que notar, que con solo aumentar de valor de vínculo *h* en la Figura 6, y manteniendo el impacto *H* y el peso *P* constantes, se produciría el mismo efecto que se genera al dejar fijo el vínculo *h* y disminuir el valor del impacto de la relación y del peso del elemento jurídico.

$$\forall\ \alpha < 90\ \exists\ H_i, P_i | i \in I : H_i \rightarrow ((h - n) = m), \quad P_i \rightarrow ((h - m) = n) \Rightarrow f : h \tag{7}$$

Ahora, cuando el ángulo no forma un triángulo rectángulo y más bien se genera un ángulo obtuso, la proyección ortogonal del peso *P* del elemento jurídico es el impacto *i* de la relación, mientras que la proyección ortogonal del vínculo *h* de la relación sería el impacto *j* de la misma relación, tal y como se muestra en la Figura 7.

Cuando el peso de un atributo y su impacto cambian aumentando sus valores, se puede presentar un cambio en el ángulo del triángulo rectángulo original, el cual puede es expresado en la expresión 8.

$$\forall\ \alpha > 90\ \exists\ H_i, P_i | i \in I : h_i \rightarrow ((H - i) = j), \\ P_i \rightarrow ((H - j) = i) \Rightarrow f : H \qquad (8)$$

La expresión 8 indica que para todo ángulo generado que sea mayor de 90° existe por lo menos un valor del impacto H_i y un valor de peso P_i tal que el subíndice de cada uno pertenece a un conjunto de índices *I*, tales que cada vínculo h_i de la relación implica un cambio en el impacto de la misma relación, que genera la proyección ortogonal *(H - i) = j* y cada peso P_i implica un cambio en el impacto que genera la proyección ortogonal *(H - j) = i* lo que implica una función de cambio en el impacto *H*. Hay que recalcar, que con solo disminuir de valor de vínculo *h* en la Figura 7, y manteniendo el impacto *H* de la relación y el peso *P* del elemento jurídico constantes, se produciría el mismo efecto que se genera al dejar fijo el vínculo *h* y se aumentara el impacto y el peso, de la relación y el elemento respectivamente.

6) Propagación de Pesos de Atributos: Los pesos de los atributos son reajustados cuando se inserta o se modifica alguno de su lista de índices, la expresión 9 indica que existe por lo menos un atributo A_i tal que su subíndice pertenece a un índice superior *I* finito, tal que para todo peso P_i del elemento que tenga su índice mayor o igual al resultado de la resta entre el índice superior menos el índice actual *I - i*, implica una función de cambio *f :* de pesos del elemento que es mapeada desde el peso con índice actual más uno *P(i+1)* hasta el peso con índice final P_i. Entonces, el cambio de pesos cuando un elemento es modificado o insertado siempre se va a ser el actual y todos lo de rango superior a él.

$$\exists A_i | \in I : \forall P_i \geq (I - i) \Rightarrow f : P_{i+1} \rightarrow P_I \qquad (9)$$

El cambio de pesos en los elementos significa también que la inserción de un solo elemento a un caso, puede cambiar la dinámica sistémica legal desde el punto de vista semántico, entre los elementos de mayor peso, y con ello el caso en sí mismo.

Trabajo futuro

El trabajo a futuro incluye varias áreas de incursión. Las principales son (1) crear una adaptación de los estados de la memoria del modelo que permitan identificar la interacción entre los diferentes estados de los constructos, (2) poder incluir en etapas posteriores del procesamiento del conocimiento lógica difusa y redes bayesianas con el propósito de refinar los procesos constructivos del conocimiento, y (3) crear un perfil de pruebas implementando el modelo de representación del conocimiento en una herramienta informática.

Conclusiones

El análisis, diseño y fabricación de la representación y procesamiento del conocimiento, en el área jurídica, presentó fuertes retos, pero nos permitió contar con un modelo de representación cognitivo efectivo pero simple, con el objetivo de (1) a portar seguridad jurídica en el procesos legales, (2) permitir a los jueces contar con un modelo de toma de decisiones óptimas, (3) poder capitalizar el conocimiento, (4) contar con un modelo simbólico de sobre el cual el conocimiento jurídico pueda funcionar.

Reconocimientos

Queremos agradecer especialmente a los Magistrados, miembros de la Segunda Corte de la Corte Suprema de Justicia de Costa Rica, jueces y funcionarios judiciales, por su interés en este proyecto, por sus comentarios sobre borradores anteriores de este trabajo y por su compromiso de brindar apoyo a nuestro equipo. De igual forma al Programa de Doctorado en Ciencias de la Computación e Informática de la Universidad de Costa Rica por la oportunidad de generar conocimientos en nuevas áreas en dicha disciplina.

Bibliografía

ALCHOURRÓN, Carlos and BULYGIN, Eugenio. 1987. *<<Introducción a la metodología de las ciencias jurídicas y sociales.>>*. Buenos Aires : Astrea, 1987. 340.
ALEVEN, Vincent. 2003. *<<Using Background Knowledge in Case-based Legal Reasoning: A Computational Model and an Intelligent Learning Environment>> en Journal Artificial Intelligence - Special issue on AI and law.* s.l. : Elsevier Science Publishers Ltd., 2003. 0004-3702.
BAIN, William. 1986. *<<Judge: A Case-based Reasoning System>> en ACM Machine Learning: A Guide to Current Research.* s.l. : Kluwer Academic Publishers, 1986. 0-89838-214-9.
BINGHAM, Tom. 2010. *<<The Rule of Law>>*. London, England : Penguin Group, 2010. 978-0-14-196201-6.
BOELLA, Guido, et al. 2014. *<<A critical analysis of legal requirements engineering from the perspective of legal practice>> en 2014 IEEE 7th International Workshop on Requirements Engineering and Law (RELAW).* s.l. : IEEE, 2014. 978-1-4799-6325-6.
CASANOVAS, Pompeu, et al. 2016. *<<Semantic Web for the Legal Domain: The next step>> en Semantic Web Springer.* s.l. : Semantic Web, 2016. Vol. 7. 1570-0844 (P).
EBENHOCH, M.P. 2001. *<<Legal knowledge representation using the resource description framework (RDF)>> en 12th International Workshop on Database and Expert Systems Applications.* s.l. : IEEE Xplore, 2001. 0-7695-1230-5.
FLORIDI, Luciano. 2004. *<<The Blackwell Guide to the Philosophy of Computing and Information>>*. Massachusetts, USA : Blackwell, 2004. 9780631229186.
GONÇALVES DE FREITAS, Frederico, AZEVEDO, Ryan and RODRIGUES, Cleyton. 2016. *<<An Ontology for Property Crime Based on Events from UFO-B Foundational Ontology>> en 2016 5th Brazilian Conference on Intelligent Systems.* s.l. : IEEE, 2016. 978-1-5090-3566-3.
HAEUSLER, Edward, DE PAIVA, Valeria and RADEMAKER, Alexandre. 2011. *<<Intuitionistic Description Logic and Legal Reasoning>> en 2011 22nd International Workshop on Database and Expert Systems Applications.* s.l. : IEEE Xplore, 2011. 2378-3915.
HESTER, Patrick and Adams, Kevin. 2014. *<<Systemic Thinking: Fundamentals for Understanding Problems and Messes.>>*. s.l. : Springer International, 2014. 3319076280.
LUENBERGER, David. 1979. *<<Introduction to Dynamic Systems: Theory, Models, and Applications.>>*. s.l. : John Wiley & Sons, Inc., 1979. 0471025941.
LUO, Jianhui, et al. 2005. *<<Graphical models for diagnosis knowledge representation and inference>> en IEEE Autotestcon, 2005.* s.l. : IEEE Xplore, 2005. 0-7803-9101-2.
MACINTYRE, Angus, SHEPHERDSON, John and SCOTT, Dana. 1992. *<<Godel's Incompleteness Theorems (Oxford Logic Guides)>>*. New York : Oxford University Press, 1992. 0-19-504672-2.
MORSE, Philip and KIMBALL, George. 1951. *<<Methos of Operation Research>>*. New York : The Thechnology Press of Massachusetts Institute of Technology and John Wiley & Sons, INC., 1951.
RICHTER, Michael and WEBER, Rosina. 2013. *<<Case-Based Reasoning: A Textbook>>*. s.l. : Springer Publishing Company, Incorporated, 2013. 364240166X.
SMITH, Edward and kOSSLYN, Stephen. 2007. *<<Cognitive Psychology: Mind and Brain>>*. Edinburgh Gate, England : Prentice Hall, 2007. 1-292-02235-3.

VIALE, Riccardo and ETZKOWITZ, Henry. 2010. <<*The Capitalization of Knowledge: A Triple Helix of University-Industry-Government*>>. Northampton, MA/Cheltenham : Emerald Group Publishing Limited, 2010. 978-1848441149.
WANG, Xing, et al. 2016. <<*Representation of Chinese criminal law in the semantic web*>> *en 2016 12th International Conference on Natural Computation, Fuzzy Systems and Knowledge Discovery (ICNC-FSKD).* s.l. : IEEE, 2016. 978-1-5090-4092-6.
WARFIELD, John. 1977. <<*Redesigning the Future, a Systems Approach to Societal Problems*>> *en IEEE Transactions on Systems, Man, and Cybernetics.* s.l. : IEEE, 1977. 0018-9472.

RIESGOS DEL PANÓPTICO LABORAL A TRAVÉS DE LA TECNOVIGILANCIA.

Por: ***Dr. Felipe Miguel Carrasco Fernández***
Investigador.
Universidad Popular Autónoma del Estado de Puebla (UPAEP) México.

Introducción.

Existe un vínculo o correspondencia entre la innovación tecnológica desarrollada por la sociedad y el Estado de gobierno de ésta así como el tipo de sociedad y los derechos de las personas.

La sociedad de la información y comunicación generada por la tercera revolución industrial y caracterizada por el desarrollo de las tecnologías de información y comunicación ha generado una sociedad de control con la finalidad de prevenir los riesgos que en la misma se puedan presentar; por lo tanto, las relaciones laborales entre empleador y trabajador tienen dichas características, así en la actualidad nos encontramos ante nuevos paradigmas en el Derecho del trabajo derivada de la implementación de la tecnología informática y de comunicación con fines de vigilancia y control de sus deberes y obligaciones laborales.

Por lo tanto, al no existir un marco jurídico regulatorio especifico de los límites de la tecnovigilancia en el ámbito laboral su aplicación se ha dejado a códigos de conducta empresarial, recomendaciones, directrices y una muy escasa legislación ambigua en el mejor de los casos, en consecuencia de esto nos encontramos ante la presencia de la casuística por parte de los tribunales al resolver los conflictos derivados de la tecnovigilancia en el ámbito laboral. Lo anterior genera incertidumbre jurídica para ambas partes.

2.- Impacto de las nuevas tecnologías en el ámbito laboral

Las transformaciones que asociamos a la globalización no pueden entenderse sin tener en cuenta el desarrollo tecnológico masivo que se produce en la totalidad de los ámbitos de la actividad económica. Para Rosenberg la tecnología nos marca los límites de lo posible, nos define lo que podrá hacerse y, por tanto, también aquello que no podrá realizarse.[1]

La principal revolución de las TIC's tiene que ver con la construcción de la sociedad del conocimiento por su parte Castells, dice que la capacidad de las TIC para generar, gestionar, transmitir y compartir información, hace posible la intensa producción de nuevo conocimiento científico-técnico y su utilización de forma casi instantánea a lo largo y ancho del planeta. Hace que las economías se centren en el conocimiento y la información como bases de productividad y de competitividad, tanto para empresas como para regiones, ciudades y países.[2]

La tecnología constituye un elemento importante en la configuración de las condiciones de vida y de trabajo. Las transformaciones tecnológicas afectan de distintas formas a la actividad laboral. Por lo tanto, en una sociedad altamente especializada, en la que los avances informáticos llegan prácticamente a todos los ámbitos, también las nuevas tecnologías empiezan a ocupar un lugar muy destacado en el desarrollo de la prestación laboral.

[1] Rosenberg citado por Camino Beldarrain, Vicente. "Tecnología y globalización económica", Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades, Año 14, Nº 27. Primer Semestre de 2012. Visible en: http://alojoptico.us.es/Araucaria/nro27/monogr27_3.pdf p. 102.
[2] Ídem. p. 103

Las relaciones laborales como lo afirma Carrasco, en la actualidad se denominan postmodernas indican la prioridad del capital sobre el trabajo y la sustitución de la mano de obra por la tecnología.[3]
Como lo establece Selma: La realidad productiva genera formas atípicas de servicios dependientes respecto de los que el sistema tradicional de indicios deviene insuficiente. Unas veces porque el ejercicio del poder de dirección llega a ser tan flexible que se confunde fácilmente con la autonomía plena, y otras, porque sin variar la intensidad del control empresarial, cambia la forma de manifestarse hacia el exterior.[4]

Respecto del impacto de estas tecnologías en las relaciones laborales Kahale: Realiza una reflexión en los sistemas de las relaciones laborales y la evolución que podría tomar el ordenamiento laboral en los próximos años, aportando soluciones o las vías de escape a las que debe llegar el Derecho del Trabajo en un futuro, partiendo desde el impacto de las tecnologías en las relaciones laborales; la relación existente entre los trabajadores y representantes de los trabajadores con las nuevas tecnologías; los conflictos que dimanan del uso de la tecnología en las relaciones laborales, y la gran necesidad de una regulación legal específica del tema.[5]

En consecuencia estamos en presencia de un conjunto de problemas jurídicos hasta ahora inexistentes. En la actualidad existe la problemática de que para tener acceso al trabajo se necesita estar capacitado en nuevas tecnologías o para permanecer en el.

Hoy la realidad nos acerca a cambios de paradigmas en lo que tiene que ver con el propio derecho frente al desarrollo de las Tecnologías de Información y Comunicación, como lo enuncia Stella Rodríguez, la idea de protección se enfrenta con los reclamos de miles de personas que proclaman un uso democrático de la red y de todos los bienes que existen en ella.[6]

3- Panóptico Laboral.
Se transita de la sociedad de la información a la sociedad de control en virtud del incremento en los sistemas de verificación y vigilancia en las relaciones laborales a través de la innovación tecnológica creándose un sistema panóptico laboral lo cual constituye un nuevo paradigma del derecho del trabajo del posmoderno.

La implementación de sistemas de videovigilancia en la sociedad actual como lo afirma Rojas: Parece admitirse en lo que se refiere a salvaguardar la seguridad de la ciudadanía, pues confiere veracidad a los hechos y permite reconstruir la realidad. Pero al mismo tiempo, otra mirada al respecto puede desvelar que dichos sistemas pueden perfectamente responder a una estructura cuyo objetivo es la posibilidad de establecer un mecanismo de control de sus habitantes.[7]

Hoy se hace realidad aquel famoso modelo de sociedad ortopédica que formulaba el Panóptico benthiano, como lo manifiesta Medina Castillo, estaba representado como un edificio de forma circular en medio del cual había un patio con una torre en el centro, estaba dividido el anillo en pequeñas celdas que daban al interior y al exterior y en cada una de ellas había, por ejemplo, un obrero trabajando. En la torre central había un vigilante y como cada celda daba al mismo tiempo

[3] Carrasco Fernández, Felipe Miguel. "Derecho del trabajo y nuevas tecnologías". Editorial Porrúa México. 2016. p. 49
[4] Selma Penalva, Alejandra. "Las Peculiaridades prácticas del Control en la Empresa". Visible en: http://www.telework2010.tic.org.ar/papers/Pino%20Estrada%20spanish.pdf, p. 36.
[5] Kahale Carrillo, Djamil Tony. "Las Nuevas Tecnologías en las Relaciones Laborales: ¿Avance o Retroceso?". En Revista de Derecho, julio, número 025, de la Universidad del Norte, Barranquilla, Colombia. Visible en: http://redalyc.uaemex.mx/pdf/851/85102508.pdf p. 291
[6] Stella Rodríguez, Gladys. "El software libre y sus implicaciones jurídicas". Revista de Derecho, Núm. 30, Diciembre, 2008, pp. 164-169. Universidad del Norte. Barranquilla, Colombia. Visible en: http://www.redalyc.org/pdf/851/85112306007.pdf p. 166
[7] Rojas, Jesús. "Mecanismos de videovigilancia en la sociedad de la información". UOC Papers, Revista sobre la Sociedad del Conocimiento. No. 5, 2007, Universidad Oberta de Cataluña. Visible en: http://www.uoc.edu/uocpapers/5/dt/esp/rojas.pdf p. 31

al exterior y al interior, la mirada del vigilante podía atravesar toda la celda sin que quedara ningún lugar oculto y, por consiguiente, todo lo que el individuo hacía estaba expuesto a la mirada del vigilante, que, a su vez, veía sin ser observado.
Las posibilidades técnicas actuales permiten esa función panóptica de un modo ampliado, al generar en la conciencia de los individuos la necesidad de autocontención, convencidos de la imposibilidad de escapar al omnipresente ojo del vigilante tecnológico que ni parpadea, ni se fatiga, ni descansa.

En la esfera productiva el control se manifiesta en un doble aspecto, por un lado, en la producción y por otro en los productores. Las características de las nuevas tecnologías aplicadas a la industria permiten, en primer lugar, la sustitución del control periférico, discontinuo y parcial que anteriormente se confiaba a la actividad humana, caso de los controladores fabriles (agentes de métodos, encargados, capataces) que, cronómetro en mano, recorrían la planta tomando tiempos; para pasar a un sistema de control centralizado y objetivo realizado por las máquinas.

Mientras el sistema de control tayloriano utilizaba al capataz como un agente represivo que apremiaba a los obreros, les presionaba para que aumentaran sus rendimientos, los nuevos sistemas de control tecnológico están incorporados a la misma maquinaria productiva. La utilización, por ejemplo, de lo que se ha denominado software in accounting permite, previa identificación personal del operador, memorizar el número de operaciones efectuadas por el mismo, el número de errores cometidos, el tiempo empleado para cada operación, el tiempo total de trabajo y la frecuencia y la duración de las interrupciones en la actividad.

Además de ello, los sistemas de organización del trabajo que propician las nuevas tecnologías, permitiendo el trabajo en grupos auto organizados, islas productivas, constituyen una expresión nueva del control, en este caso, autocontrol.

Modalidad perfeccionada del panóptico laboral donde ya no es precisa la existencia de controles externos, humanos o tecnológicos; es el mismo grupo el que controla la actividad de cada uno de sus componentes. Autocontrol que es posible, entre otros medios, mediante la fijación de sistemas retributivos al grupo, en el lugar de cada trabajador y, haciendo depender la cuantía de sus salarios de los rendimientos productivos alcanzados, al modo del conocido sistema de salario a destajo, tan usual, por ejemplo, en la construcción.[8]

Para Cillario, el trabajador podrá ser vigilado y controlado por el empresario, respecto al cumplimiento de sus obligaciones y deberes laborales, mediante las medidas que este considere oportunas, sin que exista la posibilidad recíproca, predicable de cualquier otra relación contractual, de que los trabajadores puedan adoptar similares medidas para efectuar el control del cumplimiento por parte del empresario de sus correspondientes deberes y obligaciones laborales.[9]

Michel Foucault al referirse a la tecnología desarrollada entre los siglos xvi y xix cuyo objetivo era el control de los sujetos: la inspección de los individuos no debe cesar y la mirada está por doquier en movimiento.

Por lo tanto, la sociedad de control para Ricaurte, se sostiene sobre un andamiaje económico, político, jurídico, militar y discursivo que, a través de la infraestructura tecnológica, se inscribe en la intimidad y cotidianidad del sujeto: sus relaciones, su trabajo, sus comunicaciones, su consumo.[10]

[8] Medina Castillo, J. Enrique. "Las nuevas tecnologías en las relaciones laborales. Del empleo a la participación en la innovación". Visible en: file:///C:/Users/Propietario/Downloads/archivoPDF%20(2).pdf p. 8
[9] Cillario citado por Medina Castillo, J. Enrique. Op. Cit. p. 9
[10] Ricaurte Quijano, Paola; Nájera, Jacobo y, Robles Maloof, Jesús. "Sociedades de control: tecnovigilancia de Estado y resistencia civil en México". Teknokultura, Revista de Cultura digital y Movimientos sociales. Vol. 11, No 2, 2014. Visible en: http://teknokultura.net/index.php/tk/article/view/224/pdf p. 263

4.- Nuevos paradigmas derivados de la tecnovigilancia en el ámbito laboral.

La tecnovigilancia ha propiciado el análisis de sol derechos del empleado en relación a la privacidad e intimidad hasta el grado de poder ser invasiva en el desempeño del trabajo.
Un dispositivo de vigilancia como lo expone Lyon tiene la finalidad de establecer una rutina enfocada a la observación de detalles personales, con el propósito de influenciar, administrar, cuidar y controlar a una población determinada (o a parte de ella), transformando lo observado en datos que, además, pueden ser procesados.[11]

El punto de inflexión entre el derecho del trabajo y el derecho de las tecnologías de información y comunicación han generado nuevos paradigmas que deben ser atendidos por el primero en la sociedad actual la cual tiene la característica de ser multiétnica, pluricultural en la sociedad de la información y en la sociedad de control.

Los paradigmas son las marcas que identifican y caracterizan a eras o etapas en la historia y las ciencias. A decir de Khun los paradigmas son en las ciencias, explicaciones duraderas a fenómenos y que resisten el embate permanente de nuevos paradigmas que pugnan por ocupar el lugar de los paradigmas vigentes.[12]

En consecuencia los nuevos paradigmas del derecho del trabajo derivados del tecnovigilancia en las relaciones laborales consisten en responder a la nueva situación de utilización de los controles de tecnovigilancia e informáticos para encontrar el respeto de los derechos del trabajador sin que implique violación a la intimidad o desequilibrio a los derechos fundamentales de éstos y que permita el control empresarial a través de esta tecnologías de información y comunicación en las relaciones laborales. Este clima favorece, como lo indica Cardona Rubert, el protagonismo de la autonomía individual y de los códigos unilaterales de conducta, como el método preferido por algunas empresas, en cuanto a la regulación de la utilización de los medios informáticos.

La cuestión que se plantea con los códigos éticos de conducta unilaterales es el de su aceptabilidad. En principio, los códigos de conducta, siempre y cuando su contenido sea regular y ajustado a Derecho, constituyen una manifestación del poder de dirección del empresario, admitida por el ordenamiento jurídico.[13]

La justificación del sector empresarial al uso de la tecnovigilancia en las relaciones laborales reside en eficacia y rentabilidad, control de calidad en la prestación del servicio laboral y a los clientes, así como preservar bienes de la empresa, por lo tanto, se debe cumplir con la legislación que permita por una parte al empresario lograr dicha finalidad y a los trabajadores el respeto y garantía de los derechos fundamentales.

La proyección de las nuevas tecnologías sobre las relaciones laborales individuales, plantean un mismo orden de cuestiones, que pueden sintetizarse en dos como lo expone Cardona Rubert:

—Límites del uso extra-laboral de los medios informáticos por los trabajadores
—Facultad de vigilancia y control empresarial de dicho uso.

[11] Lyon citado por Ricaurte Quijano, Paola; Nájera, Jacobo y, Robles Maloof, Jesús. Op. Cit. p. 277
[12] Aguirre, Carlos Dionisio. "Sociedad de la Información, Nuevos paradigmas, Nueva economía". Derecho Informático en Iberoamérica. Editorial Popocatépetl. México. 2010. p. 81
[13] Cardona Rubert, María Belén. "Las relaciones laborales y el uso de las tecnologías informáticas". Lan Harremanak: Revista de Relaciones Laborales, Nº Extra 1, 2003, Ejemplar dedicado a: Segundas Jornadas sobre cuestiones de actualidad del Derecho del trabajo y de la Seguridad Social de la Escuela universitaria de Relaciones laborales de la UPV/EHU. 2003. Visible en: file:///C:/Users/Propietario/Downloads/Dialnet-LasRelacionesLaboralesYElUsoDeLasTecnologiasInform-786247%20(1).pdf p. 160

El empleado, por su lado, sabiendo o no si el empleador practica el monitoreo, debe siempre utilizar de manera racional, sin abusos, las herramientas tecnológicas puestas a su disposición por el empleador para el desarrollo exclusivo de las actividades laborales.[14]

Para Terán, la ética en el ámbito laboral se reduce en el ejercicio de conductas de buena fe, justas, correctas, lícitas, racionales y razonables, por parte de los sujetos del contrato de trabajo o sea empleador y trabajador. Busca el equilibrio en las relaciones entre el mandante y el mandado. Sin ella, no existiría la armonía en el trabajo, así como la puerta del liberalismo seria evidente.[15]

Es sabido que la obtención del control empresario presenta tanto alternativas de medios como de modos, así por ejemplo contralores al azar de los correos electrónicos de los trabajadores son por lo general suficientes para la función empresaria, en cuyo supuesto un control total de toda la correspondencia electrónica no tendría en principio justificación ya que el fin empresario puede obtenerse de un modo menos invasivo.

La sociedad de la información y comunicación generada por la tercera revolución industrial ha desarrollado a la vez una sociedad de control con la finalidad de prevenir riesgos en las relaciones laborales. Los nuevos paradigmas del derecho del trabajo derivado de la tecnología constituyen el nuevo reto pero a la vez deben preservar los derechos fundamentales del empleado y permitir el control, vigilancia y supervisión del empresario dentro del centro del trabajo y fuera de él en todo lo relacionado al trabajo contratado.

Conclusiones.

1. La sociedad postmoderna ha generado un sistema con características de panóptico en el ámbito laboral a través de la tecnovigilancia.
2. La tecnovigilancia constituye nuevos paradigmas y el reto es el respeto de los derechos del trabajador sin que implique violación a la intimidad o desequilibrio a los derechos fundamentales de estos, pero que a la vez permita el control empresarial a través del uso de tecnología.

Bibliografía

- Aguirre, Carlos Dionisio. "Sociedad de la Información, Nuevos paradigmas, Nueva economía". Derecho Informático en Iberoamérica. Editorial Popocatépetl. México. 2010.
- Camino Beldarrain, Vicente. "Tecnología y globalización económica", Araucaria. Revista Iberoamericana de Filosofía, Política y Humanidades, Año 14, Nº 27. Primer Semestre de 2012. Visible en: http://alojoptico.us.es/Araucaria/nro27/monogr27_3.pdf
- Cardona Rubert, María Belén. "Las relaciones laborales y el uso de las tecnologías informáticas". Lan Harremanak: Revista de Relaciones Laborales, Nº Extra 1, 2003, Ejemplar dedicado a: Segundas Jornadas sobre cuestiones de actualidad del Derecho del trabajo y de la Seguridad Social de la Escuela universitaria de Relaciones laborales de la UPV/EHU. 2003. Visible en: file:///C:/Users/Propietario/Downloads/Dialnet-LasRelacionesLaboralesYElUsoDeLasTecnologiasInform-786247%20(1).pdf
- Carrasco Fernández, Felipe Miguel. "Derecho del trabajo y nuevas tecnologías". Editorial Porrúa México. 2016.
- Kahale Carrillo, Djamil Tony. "Las Nuevas Tecnologías en las Relaciones Laborales: ¿Avance o Retroceso?". En Revista de Derecho, julio, número 025, de la Universidad del Norte, Barranquilla, Colombia. Visible en: http://redalyc.uaemex.mx/pdf/851/85102508.pdf

[14] Vargas Basilio, Aíslan. "Perspectiva ética del monitoreo electrónico en el ámbito empresarial". Derecho Informático Empresarial. Editorial Popocatépetl. México. 2013. p. 57

[15] Terán citado por Vargas Basilio, Aíslan. Op. Cit. p. 58

- Medina Castillo, J. Enrique. “Las nuevas tecnologías en las relaciones laborales. Del empleo a la participación en la innovación”. Visible en: file:///C:/Users/Propietario/Downloads/archivoPDF%20(2).pdf
- Ricaurte Quijano, Paola; Nájera, Jacobo y, Robles Maloof, Jesús. “Sociedades de control: tecnovigilancia de Estado y resistencia civil en México”. Teknokultura, Revista de Cultura digital y Movimientos sociales. Vol. 11, No 2, 2014. Visible en: http://teknokultura.net/index.php/tk/article/view/224/pdf
- Rojas, Jesús. “Mecanismos de videovigilancia en la sociedad de la información”. UOC Papers, Revista sobre la Sociedad del Conocimiento. No. 5, 2007, Universidad Oberta de Cataluña. Visible en: http://www.uoc.edu/uocpapers/5/dt/esp/rojas.pdf
- Selma Penalva, Alejandra. “Las Peculiaridades prácticas del Control en la Empresa”. Visible en: http://www.telework2010.tic.org.ar/papers/Pino%20Estrada%20spanish.pdf
- Stella Rodríguez, Gladys. “El software libre y sus implicaciones jurídicas”. Revista de Derecho, Núm. 30, Diciembre, 2008, pp. 164-169. Universidad del Norte. Barranquilla, Colombia. Visible en: http://www.redalyc.org/pdf/851/85112306007.pdf
- Vargas Basilio, Aíslan. “Perspectiva ética del monitoreo electrónico en el ámbito empresarial”. Derecho Informático Empresarial. Editorial Popocatépetl. México. 2013.

Blockchain, Bitcoin y Monedas Virtuales: el cambio de Paradigma en los Sistemas de Pago Electrónico

***Mariliana Rico Carrillo*[1]**

1. Introducción

En la actualidad no hay nada más cierto que el respaldo del dinero, tanto el de curso legal como el electrónico es virtual, ya que ninguna de las dos forma de pago cuenta con un respaldo físico que garantice su valor. Al no existir las tradicionales reservas en oro vinculadas con la emisión de los billetes y monedas bancarios, la confianza en el medio de pago reside en el Estado a través de la autoridad emisora de la moneda. La expresión dinero fiduciario[2] es empleada para referirse al nivel de confianza que infunde el sujeto que respalda la emisión de la moneda; en su momento éste fue uno de los cambios de paradigma más importante en la concepción tradicional del dinero, pero la evolución de la representación del dinero la hemos visto también en otras épocas de la historia de la humanidad, con la aparición de los títulos valores, las transferencias de fondos, los sistemas de pagos electrónicos y otros avances vinculados directamente con el desarrollo de las nuevas tecnologías.

El presente trabajo está dedicado a estudiar las implicaciones que produce el nuevo cambio de paradigma en los sistemas de pago como consecuencia de la aparición del *bitcoin* y la tecnología *blockchain*; como veremos, esta nueva concepción del dinero radica una vez más en la confianza que rodea la emisión del medio de pago, aunque en este caso no se trata de un metal o de un Estado sino de la propia tecnología y de la actuación de los sujetos que participan en la emisión, circulación e intercambio de lo que se conoce como monedas virtuales o criptomonedas.

En el desarrollo de la investigación, abordaré el estudio de otro instrumento de pago que ha nacido gracias a los avances de las operaciones comerciales electrónicas en Internet: el dinero electrónico como sustituto del dinero de curso legal. La importancia de este análisis es fundamental al momento de establecer la diferencia entre este mecanismo de pago y las monedas virtuales.

3. Internet y el desarrollo de los sistemas de pago

El comercio electrónico en Internet y la necesidad de diseñar instrumentos de pago adecuados a este entorno ha producido un importante avance en los sistemas de pago electrónico (en adelante SPE)[3] gracias a la creación de medios de pago como *PayPal* y el

[1] Catedrática de Derecho Mercantil de la Universidad Católica del Táchira. Profesora visitante de la Universidad Carlos III de Madrid. Secretaria General de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI)

[2] El dinero fiduciario es la moneda que un gobierno ha declarado legal, sin estar respaldada por un producto físico. El valor del dinero fiduciario se deriva de la relación entre la oferta y la demanda y de la confianza en la autoridad emisora, más que del valor del respaldo material del dinero. El dinero fiduciario comenzó a dominar en el siglo XX, a partir 1971 con las políticas monetarias del presidente estadounidense Richard Nixon que pusieron fin a la época de las reservas en oro.

[3] Un sistema de pago se define como un conjunto de instrumentos, procedimientos y reglas para la transferencia de fondos entre los participantes del sistema. Por lo general, se basa en un acuerdo entre el participante y el operador del sistema, donde la transferencia de fondos se realiza utilizando una infraestructura técnica acordada. El calificativo "electrónico" se añade para destacar que la circulación y representación del dinero se materializan a través

dinero electrónico, concebido como un sustituto de los tradicionales billetes y monedas bancarios.

Los SPE involucran el estudio de dos componentes básicos: la transferencia electrónica de fondos (TEF), como el sistema que permite efectuar el movimiento del dinero, y los instrumentos de pago electrónico (IPE), entendidos como los dispositivos que permiten a los usuarios emitir las órdenes de pago para activar la TEF, entre los que se encuentra el dinero electrónico.

En Europa, el dinero electrónico ha sido objeto de regulación en dos normas vinculantes, la Directiva 2000/46CE sobre entidades de dinero electrónico y su ejercicio, modificada por la Directiva 2009/110/CE del Parlamento Europeo y del Consejo de 16 de septiembre de 2009 sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades (Directiva EDE). Al ser considerado un servicio de pago, también es de aplicación la Directiva 2015/2366 sobre servicios de pago en el mercado interior, conocida como la Directiva PSD2 por sus siglas en inglés *Payment Service Directive* y por ser la segunda directiva que se ocupa de regular estos servicios[4].

3.1. El dinero electrónico como sustituto del dinero de curso legal

De acuerdo con las previsiones del artículo 2 de la segunda Directiva EDE, el concepto del dinero electrónico se refiere a un valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor, se emite al recibir fondos del titular, con el propósito de efectuar operaciones de pago y es aceptado por una persona distinta del emisor.

De esta definición se derivan las características básicas de esta nueva forma de pago: 1) la emulación del dinero tradicional, 2) el almacenamiento del dinero en un soporte electrónico, 3) la aceptación por empresas distintas del emisor, y 4) su emisión por un valor igual a los fondos recibidos (valor a la par).

Un elemento fundamental en el esquema de funcionamiento del dinero electrónico es su conversión a dinero de curso legal, que se establece con la finalidad de mantener la confianza de los titulares y usuarios de este IPE. Para lograr esta conversión, la Directiva EDE establece la obligación de reembolso a las entidades emisoras de dinero electrónico (EDE), quienes deben pagar el valor nominal equivalente en dinero de curso legal al titular del mismo en cualquier momento que éste lo solicite.[5]

Al concebirse como una emulación del dinero fiduciario, la emisión de dinero electrónico es una actividad altamente regulada y corresponde exclusivamente a las EDE,

---

de técnicas electrónicas. Para un estudio amplio sobre los sistemas de pago electrónico, sus aplicaciones y funcionamiento en Internet *vid*. RICO CARRILLO, Mariliana: *El pago electrónico en Internet. Estructura operativa y régimen jurídico,* Thomson Reuters Aranzadi, Madrid, 2012.

[4] Esta directiva entró en vigor en las legislaciones nacionales de los Estados miembros de la UE a partir del 13 de enero de 2018 y derogó la anterior Directiva 2007/64/CE. Fue aprobada con la finalidad de proporcionar la base jurídica para seguir avanzando en el desarrollo de un mercado interior más integrado de pagos electrónicos en la UE y busca lograr una apertura de los mercados de pagos para permitir que entren nuevos actores y aumente la competencia, ofreciendo más opciones y mejores precios a los consumidores. Vid. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=LEGISSUM:2404020302_1 (última consulta: 15 de julio de 2018)

[5] Un estudio amplio de las características del funcionamiento del dinero electrónico puede consultarse en MARTÍNEZ NADAL, A: *Dinero electrónico: aproximación jurídica*, Civitas, Madrid, 2003.

quienes deben cumplir unos requisitos específicos con el objeto de ser autorizadas para funcionar como tales. Es importante mencionar que las EDE se consideran entidades de crédito y como tales están sometidas a un régimen de supervisión específico y que el artículo 18 del referido texto legal prohíbe en forma expresa la emisión de dinero electrónico a cualquier persona física o jurídica que no cuente con la respectiva autorización.

En cuanto a la naturaleza jurídica del dinero electrónico como un sustituto del dinero de curso legal, es importante destacar desde una óptica jurídica los conceptos no son del todo identificables, ya que sólo el dinero de curso legal es de obligatoria aceptación como medio de pago; en este sentido y al igual que sucede con los otros medios de pago alternativos al dinero fiduciario, será el acreedor quien debe aceptar, previamente a la operación, el pago mediante dinero electrónico, sin que esté obligado a ello.

Otra característica distintiva del dinero electrónico, de acuerdo con el concepto legal, es el almacenamiento del valor monetario en un soporte electrónico previamente a la emisión del dinero. El soporte electrónico puede ser un instrumento tangible (el chip de una tarjeta, p. ej.) o la memoria del disco duro del ordenador. Esto implica que para la generación del dinero electrónico es necesario tener abierta una cuenta bancaria en una institución financiera, ya que son los fondos de esa cuenta los que permiten la emisión de dinero electrónico.

Es importante tener en cuenta estos elementos (regulación, emulación del dinero de curso legal, reembolso, provisión de fondos, control y supervisión de la actividad y del doble gasto) para poder establecer las diferencias con el *bitcoin* y otras monedas virtuales y determinar la naturaleza jurídica de estos nuevos instrumentos de pago.

3.2. *PayPal* y los sistemas de pago P2P

Los servicios de pago P2P (*Person to Person*) permiten el envío de dinero entre cuentas de correo electrónico mediante transferencias de fondos gestionadas por empresas privadas. *PayPal* es una de las empresas que más éxito ha tenido en Internet en el ámbito de los pagos P2P.

La infraestructura de este tipo de servicios es suministrada por empresas especializadas comúnmente denominadas *Payment Services Providers* (PSP) que se encargan de gestionar el pago. El sistema tiene su base en el uso del correo electrónico como medio de notificación de las transacciones. Para poder realizar pagos a través de este mecanismo, es necesario registrarse en la web del PSP, suministrar una dirección de correo electrónico y los datos de una cuenta bancaria o de una tarjeta donde se cargará el monto de la operación, esto implica que la intervención de las entidades financieras es imprescindible a efectos de concretar la operación, por lo tanto es un mecanismo directamente vinculado con el sistema financiero.

El éxito de *PayPal* se debe a la facilidad y comodidad del servicio para los usuarios, quienes sólo necesitan suministrar una cuenta de correo electrónico y un número de cuenta bancaria; a la seguridad de la transacción, que es garantizada por el PSP y al bajo coste de las operaciones. En la actualidad las empresas como *PayPal* están sujetas

a la aplicación de la Directiva PSD2 en su función de proveedores de servicios de iniciación de pagos (PISP).[6]

4. La intermediación como característica diferenciadora de los sistemas de pago electrónico de primera y segunda generación

Como bien puede observarse, tanto el dinero electrónico como *Paypal* requieren la presencia de un tercero para gestionar los pagos, cuya intermediación infunde confianza en los usuarios. La intermediación predominante en estos sistemas de pago (tanto en el dinero electrónico, los IPE en general y los sistemas de pago P2P) nos permite distinguir una primera generación de SPE, cuya base es la centralización de la confianza en una tercera parte, de una segunda generación, caracterizada por la descentralización y la ausencia de terceros de confianza.

Esta segunda generación ha surgido como consecuencia del uso de la tecnología *blockchain,* que ha cambiado significativamente el paradigma tradicional de la confianza. Aunque el modelo centralizado continúa en uso y sigue siendo predominante, *blockchain* permite realizar pagos descentralizados, gracias al empleo monedas virtuales, donde la confianza reside en la propia tecnología y en la participación de los usuarios e intervinientes en la transacción, es por ello que hablamos de una segunda generación de SPE, cuyo estudio desarrollamos en los siguientes apartados.

5. Blockchain y bitcoin: una nueva revolución

El *bitcoin* y la tecnología *blockchain* han producido toda una revolución en los pagos en Internet, determinada por el uso de un "ecosistema" [7] de tecnologías ha dado origen a lo que hemos denominado la segunda generación de SPE, caracterizada por el uso de medios de pago basados en sistemas de confianza descentralizados y privados, lo cual marca una notable una diferencia con los tradicionales SPE centralizados y públicos, al excluir la actuación de los intermediarios financieros.

La primera moneda virtual en aparecer en el mercado y que ha causado un mayor impacto en la economía es el *bitcoin*, cuyo uso y funcionamiento se basa en la tecnología conocida como *blockchain* (cadena de bloques en español), que permite realizar pagos electrónicos sin la intervención de un banco, una empresa de tarjetas de pago o un intermediario como *PayPal*.[8]

El protocolo *blockchain* es difundido en el año 2009 tras las publicación del documento técnico "*Bitcoin: a Peer to Peer Electronic Cash System*" cuya autoría se atribuye al japonés Satoshi Nakamoto. La idea de Nakamoto se centra en el diseño de un

[6] Un servicio de iniciación de pago se define como aquél que permite iniciar una orden de pago a petición del usuario del servicio de pago, respecto de una cuenta de pago abierta con otro proveedor de servicios de pago. Estos servicios se basan en el acceso directo o indirecto de los PSIP a las cuentas del ordenante. En el ámbito del comercio electrónico proporcionan un soporte lógico que sirve de puente entre el sitio web del comerciante y la plataforma bancaria en línea del proveedor de servicios de pago gestor de cuenta del ordenante, con el fin de iniciar pagos por transferencia a través de Internet. (*Vid*. considerando 27 de la Directiva PSD2).

[7] En los distintos documentos que han analizado el funcionamiento de las MV se usa el término "ecosistema" para hacer referencia a la combinación de distintas tecnologías y a la presencia categorías nuevas y específicas de actores que no estaban presentes en los sistemas de pago tradicionales.
Vid. EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes- a fuerte análisis*, February 2015, p. 3. Disponible en https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf (última consulta: 14 de junio de 2018)

[8] TAPSCOTT D. y A. TAPSCOTT: *Blockchain Revolution*, Penguin Ramdom House, LLC, New York, 2016 p. 6.

SPE basado en el uso de la criptografía y la tecnología *peer to peer*, eliminando de esta manera la intermediación financiera, con la finalidad de ofrecer una alternativa de pagos frente a los tradicionales SPE.

Aunque la tecnología *blockchain* ha sido definida de diversas maneras, técnicamente es un protocolo que combina diversos servicios de confianza (criptografía, firmas digitales, sellos de tiempo) y establece un conjunto de reglas que aseguran la integridad de la transacción a través de la intervención de distintos sujetos, sin que ninguno de ellos pueda calificar como una tercera parte de confianza.

El concepto de moneda electrónica expuesto por Nakamoto se fundamenta en el uso de la firma digital basada en criptografía de clave pública. El protocolo define el funcionamiento de una cadena de firmas digitales donde una persona transfiere un valor monetario a otra en forma cronológica, mediante la firma de un *hash* de una transacción previa y la incorporación de la clave pública del próximo propietario, agregándolas al final de la operación, de modo que cuando los beneficiarios de la transacción accedan posteriormente a las firmas puedan verificar la cadena de propiedad.[9]

Blockchain permite que todas las transacciones sean verificadas y registradas en un bloque que está directamente vinculado con el bloque anterior, creando la respectiva cadena que otorga un carácter irreversible a las operaciones (inmutabilidad), que a su vez son validadas por la mayoría de los participantes en la red. En este caso el consenso de las partes es el elemento fundamental que avala la seguridad de la transacción.

A diferencia de lo que sucede con las instituciones financieras, se trata es una red de acceso público y una nueva forma de colaboración *peer to peer*, esto implica cualquiera puede acceder a los registros en cualquier momento y que no existe una tercera parte que certifique las operaciones. En el ámbito de los medios de pago es una plataforma que se distingue por la inclusión y la disminución del costo de la transacción (en comparación con las tradicionales TEF y los SPE de primera generación), ya que no requiere cuentas bancarias, aprobaciones de crédito u otras inversiones, elementos característicos de la intermediación financiera que aunque aportan seguridad, aumentan el costo de la transacción.

7. Los esquemas de monedas virtuales

La irrupción del *bitcoin* y otras monedas virtuales ha llamado la atención de las autoridades europeas, principalmente del Banco Central Europeo (BCE) como catalizador de los sistemas de pago y de la Autoridad Bancaria Europea (ABE) como ente supervisor de las actividades financieras. Ambas instituciones han elaborado distintos documentos a efectos de estudiar el funcionamiento de las monedas virtuales, tomando en cuenta principalmente las implicaciones del uso del *bitcoin* en el sistema financiero.

Los informes del BCE se refieren en forma amplia a los esquemas de monedas virtuales y datan de 2012[10] y 2015[11]. Estos documentos tratan diversos aspectos relacionados con los nuevos medios de pago, incluyendo la relevancia de los esquemas

[9] NAKAMOTO, Satoshi "*Bitcoin: a Peer to Peer Electronic Cash System*", disponible en https://bitcoin.org/bitcoin.pdf (última consulta: 14 de junio de 2018)
[10] EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes*, October 2012, *op.cit.*
[11] EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes- a further analysis*, February 2015, *op. cit.*

de monedas virtuales para los bancos centrales donde se analizan los riesgos para la estabilidad financiera y de los sistemas de pago. Los trabajos de la AEB también están orientados a analizar el funcionamiento de las monedas virtuales, su infraestructura técnica, sujetos participantes, potenciales riesgos y beneficios. Sus conclusiones se recogen en el dictamen titulado *Opinion on "virtual currencies",* de julio de 2014.[12]

En este apartado nos dedicamos al estudio de las monedas virtuales, tomando como base los informes del BCE y las conclusiones del dictamen de la AEB de 2014, que como veremos más adelante, han sido tomadas en cuenta en la redacción de la quinta Directiva en materia de prevención del blanqueo de capitales y la financiación del terrorismo[13], aprobada en mayo de 2018[14].

7.1 Precisiones terminológicas y conceptuales

La expresión moneda virtual (*virtual currency*) se usa en forma genérica para diferenciar esta forma de pago del dinero electrónico como sustituto del dinero de curso legal.

Existen distintos tipos de monedas virtuales, unas son de uno abierto, otras limitadas a una comunidad determinada, algunas son de flujo unidireccional y otras de flujo bidireccional[15]. El término criptomoneda (*cryptocurrency*) se refiere a un tipo específico de monedas virtuales como el *bitcoin*, que son descentralizadas y de uso bidireccional[16], características que se derivan del uso de la tecnología *blockchain*.

Antes de examinar las diferentes definiciones, insistimos que jurídicamente no estamos hablando de dinero electrónico, ni mucho menos de dinero de curso legal, en el sentido que no existe una institución financiera que respalde su emisión. Las monedas virtuales (en adelante MV), son medios de pago de carácter privado, cuya delimitación conceptual es importante para conocer sus implicaciones jurídicas, para saber de qué estamos hablando y cuál sería la regulación aplicable (si es que existe alguna) o para saber qué es lo que en el futuro se va a regular.

Uno de los primeros conceptos lo encontramos en el Informe del BCE de 2012 que define estos instrumentos monetarios como "…un tipo de dinero digital no regulado, emitido y generalmente controlado por sus desarrolladores, utilizado y aceptado entre los miembros de una comunidad virtual específica." En el texto de este documento se

---

[12] EUROPEAN BANKING AUTHORITY (EBA) *Opinion on "virtual currencies*", July 2014. Disponible https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (última consulta: 15 de julio de 2018)

[13] Directiva (UE) 2018/843 del Parlamento Europeo y del Consejo de 30 de mayo de 2018 por la que se modifica la Directiva (UE) 2015/849 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifican las Directivas 2009/138/CE y 2013/36/UE.

[14] La Directiva destaca que el anonimato de las monedas virtuales permite su uso indebido con fines delictivos como sistemas de financiación alternativa para los grupos terroristas que pueden ser capaces de transferir dinero hacia el sistema financiero de la UE o dentro de las redes de monedas virtuales ocultando transferencias o gozando de cierto grado de anonimato en esas plataforma (*Vid*. considerandos 8, 9 y 10 de la citada directiva).

[15] En cuanto a los diferentes tipos de esquemas de MV, los informes del BCE advierten la presencian de tres: 1) los esquemas cerrados, que carecen de vínculo con la economía real; 2) los esquemas de flujo unidireccional, donde las monedas se pueden comprar a un tipo de cambio específico pero no pueden ser canjeadas; y 3) los esquemas de flujo bidireccional, que permiten a los usuarios comprar y vender MV de acuerdo con las tasas de cambio y se usan para la compra de bienes y servicios virtuales y reales. En este caso, las MV son similares a cualquier otra moneda convertible con respecto a su interoperabilidad en el mundo real. Esta categoría es la que se identifica con el término "criptomonedas". *Vid*. EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes,* October 2012, O*p. cit.*

[16] EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes- a further analysis,* February 2015, *op. cit.*

diferencian los distintos tipos de MV y se advierte que la definición se formula de manera abierta, en el entendido que puede ser adaptada en el futuro si las características fundamentales de su funcionamiento cambian.

En su dictamen de 2014, la ABE define las MV como una "…representación digital de valor no emitida por un banco central o autoridad pública, ni necesariamente vinculada con el concepto de dinero fiduciario, que es utilizada por personas físicas o jurídicas como un medio de intercambio y puede transferirse, almacenarse o intercambiarse por medios electrónicos". La importancia de esta última definición es notable por sus efectos en la futura regulación de las MV, de hecho, ha sido incorporada en la Directiva de prevención de utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo.

La influencia del dictamen de la ABE también la podemos observar en el informe del BCE de 2015, que se refiere a los avances de las MV e indica que el BCE ha estado examinando el desarrollo de estos SPE para analizar su relevancia en los sistemas de pago minoristas. Los lineamientos de la ABE están presentes en este nuevo informe al indicar que las MV como el *bitcoin*, no son formas de dinero tal como se definen en la literatura económica, sino "...una representación digital de valor, no emitida por un banco central, institución de crédito o institución de dinero electrónico, que en algunas circunstancias se puede utilizar como una alternativa al dinero."

Como bien puede observarse, tanto el BCE como la ABE y la propia Comision Europea concuerdan al conceptualizar las MV como una representación digital de valor de carácter privado, aceptada como una alternativa de pago. En los siguientes epígrafes nos dedicamos a estudiar los principales rasgos distintivos de esta nueva forma de pago y su diferencia con el concepto de dinero electrónico analizado anteriormente.

7.2. Características de los esquemas de monedas virtuales

a) La descentralización como elemento fundamental

La descentralización es el elemento fundamental que caracteriza el funcionamiento de las MV. Tradicionalmente, la confianza en los sistemas de pago y en las operaciones electrónicas encuentra su base en la intervención de los denominados terceros de confianza. Estos terceros de confianza son de la más variada índole y van desde los intermediarios financieros tradicionales hasta las empresas especializadas en SPE como *Paypal*. En estos casos se habla de modelos de confianza centralizados, donde la seguridad reside en una determinada persona o institución.

En los SPE de segunda generación, los usuarios compran y venden las MV entre ellos sin ningún tipo de intermediación, ya que la confianza la proporciona la propia red a través de la infraestructura tecnológica. La información distribuida entre los diversos usuarios y la presencia de los denominados "mineros"[17] aportan seguridad y confianza. En los modelos descentralizados, la tecnología *blockchain* y la confianza en la red sustituye a los bancos e intermediarios financieros.

[17] Los "mineros" son los sistemas informáticos que validan las transacciones. El proceso de minería se lleva a cabo a través de equipos extremadamente rápidos que pueden realizar cálculos matemáticos complejos con la finalidad de verificar la validez de las transacciones. *Vid*. EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes*, October 2012, *op. cit*., p. 23

b) La criptografía como elemento de seguridad y la inmutabilidad de la transacción

En materia de pagos efectuados a través de medios electrónicos, la criptografía ha adquirido singular importancia en los últimos años, gracias a su uso en los sistemas de pago propios de las operaciones bancarias y financieras, con la finalidad de lograr la identificación entre el receptor y el emisor del mensaje y mantener la confidencialidad de la información[18].

Los sistemas de cifrado asimétrico permiten la generación de firmas digitales, que es el mecanismo de seguridad que utiliza el protocolo *blockchain*. Para generar una firma digital el emisor dispone de dos claves matemáticamente relacionadas entre sí: una pública que debe revelar y publicar y otra privada que debe mantener en secreto. La clave privada sirve para firmar digitalmente un mensaje y garantiza la autenticidad, la integridad y el no repudio. En el sistema ideado por Nakamoto cada propietario de MV dispone un par de claves que se almacenan localmente en un archivo electrónico, esto significa que la pérdida del archivo implicará la pérdida de las MV.

Las técnicas criptográficas permiten a las partes realizar las transacciones sin la intervención de terceros confiables, de manera que ellas mismas pueden verificar la cadena de bloques desde su origen hasta el final. Las operaciones se registran en un bloque que está directamente vinculado con el bloque anterior, creando la respectiva cadena que otorga el carácter de inmutabilidad a las transacciones. Todo esto sucede gracias al empleo de la criptografía.

Las transacciones firmadas se envían a la red, lo que significa son públicas y aunque no se proporciona información sobre las partes involucradas, se pueden rastrear.[19] La información queda registrada de manera permanente y es replicada de forma distribuida en los distintos servidores que forman parte de la red. La inmutabilidad está directamente relacionada con la prevención del doble gasto, es decir, evitar que se copie o falsifique una moneda, especialmente si se considera que no existe un intermediario que valide las transacciones.

c) La presencia de nuevos actores

El uso de la tecnología *blockchain* implica la presencia de nuevos actores en el mecanismo de pago. Al igual que en la economía real, en una economía virtual hay una amplia gama de actores económicos que intervienen en las transacciones de diferentes maneras[20].

En el esquema del funcionamiento de las MV básicamente encontramos los siguientes participantes: 1) los creadores originales del sistema que permite emitir las monedas

[18] El propio BCE ha destacado la importancia del uso de técnicas criptográficas en el ámbito de los pagos a través de Internet, en el Informe sobre Dinero Electrónico de 1998 se menciona la criptografía como el medio idóneo para autenticar las transacciones y proteger la confidencialidad e integridad de la información en los instrumentos de dinero electrónico. Vid. EUROPEAN CENTRAL BANK (ECB) *Report on Electronic Money*, August 1998, *Op. cit.*

[19] A través de la tecnología *blockchain*, cuando una persona envía una moneda se registran todos los datos de la transferencia: dirección de red desde la que salen las MV, la dirección de envío, cantidad y momento exacto de la transacción. A través de la dirección de red se puede rastrear la transacción, aunque esta siga siendo anónima, ya que lo que se identifica es la dirección de red y no el usuario. La Directiva 5AMLD se refiere a la dirección de red como la dirección de las monedas virtuales. Para combatir los riesgos relacionados con ese anonimato, el considerando 9 indica que las Unidades de Inteligencia Financiera (UIF) nacionales deben tener acceso a la información que les permita vincular las direcciones de las monedas virtuales con la identidad del propietario de la moneda virtual.

[20] *Vid.* EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes*, October 2012, *op. cit.*,

(inventores), que son los individuos u organizaciones que desarrollan la infraestructura técnica que soporta la red; 2) los usuarios que intercambian, adquieren o invierten las monedas; 4) los mineros, que resuelven los *hashes* y validan las transacciones a efectos de impedir el doble gasto y la falsificación de las monedas, recibiendo a cambio pequeñas cantidades de MV; 5) los proveedores que ofrecen billeteras digitales a los usuarios para almacenar sus claves criptográficas de MV y los códigos de autenticación que permiten realizar las transacciones, denominados en la terminología jurídica "proveedores de servicios de custodia de monederos electrónicos".

Al lado de estos sujetos se encuentran las entidades que participan en el intercambio de MV por dinero fiduciario, transferencias de fondos, otros medios de pago (tarjetas, dinero electrónico), u otras monedas virtuales, en el supuesto que éstas sean convertibles[21], los intermediarios que ponen en contacto a las distintas personas que desean comprar o vender en los distintos mercados donde se cotizan las MV, y los proveedores de bienes y/o servicios aceptantes de MV.

Como explicaremos en el siguiente epígrafe, la aprobación de la Directiva sobre prevención de blanqueo de capitales, somete a los proveedores de servicios de cambio de MV por monedas fiduciarias y a los proveedores de servicios de custodia de monederos electrónicos al cumplimiento de los requisitos de supervisión y vigilancia indicados en la norma comunitaria.

d) Su uso como medio de pago

Las MV pueden utilizarse como medio de pago para obtener bienes y servicios. El grado de aceptación varía de un esquema a otro y depende de los participantes del mercado (es decir, de su red de aceptación) ya que su uso puede ser amplio o estar limitado a una comunidad específica de individuos[22].

En esencia, los esquemas de MV funcionan de manera muy similar a los sistemas de pago minoristas, excepto por el hecho que los intermediarios financieros no están involucrados en el proceso de pago. En los esquemas de MV están presentes los tres elementos principales de un sistema de pago minorista: 1) se utiliza un instrumento de pago que debe ser aceptado entre las partes, 2) el procesamiento y la compensación implican una instrucción de pago entre el acreedor y el deudor, y 3) los débitos y créditos se liquidan en la cuenta del usuario[23].

e) Su uso como mecanismo de inversión

Las MV no sólo pueden usarse como medios de pago, también pueden utilizarse como mecanismo de inversión. En esta función, las operaciones de compraventa o intercambio de MV pueden producir ganancias o pérdidas patrimoniales, y estar sujetas a impuesto, ya que generan una alteración en la composición del patrimonio del contribuyente, como veremos más adelante.

---

[21] Algunos esquemas de MV son convertibles (o abiertos) y, por lo tanto, se pueden intercambiar por dinero fiduciario a un tipo de cambio, mientras que otros no son convertibles (o cerrados), es decir, son específicos de una comunidad en particular y no pueden intercambiarse. *Vid*. EUROPEAN BANKING AUTHORITY (EBA) *Opinion on "virtual currencies*", July 2014, Op. *cit.* p. 13.

[22] EUROPEAN BANKING AUTHORITY (EBA) *Opinion on "virtual currencies*", July 2014, Op. *cit*.

[23] *Vid*. EUROPEAN CENTRAL BANK (ECB), *Virtual Currency Schemes*, October 2012, *op. cit*.

7.4. Las monedas virtuales en la Directiva sobre prevención de blanqueo de capitales

Durante el mes de mayo de 2018 fue aprobada la quinta Directiva sobre prevención de utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo, (conocida por sus siglas en inglés 5AMLD).[24] Esta norma es el primer texto legal de carácter vinculante a nivel comunitario que establece un marco jurídico aplicable al funcionamiento de las plataformas de cambio de MV, al someter a su regulación a los proveedores de servicios de cambio de MV por monedas fiduciarias y a los proveedores de servicios de custodia de monederos electrónicos[25].

Una de las novedades más importantes de esta Directiva es precisamente la inclusión de estos proveedores en su ámbito de aplicación, por lo tanto, como entidades obligadas están sometidas al deber de aplicar medidas preventivas y de notificar toda transacción sospechosa relacionada con las MV, de forma similar a como lo están las instituciones financieras respecto a las actividades sospechosas derivadas del uso de medios de pago tradicionales.

Otro aspecto a destacar de esta Directiva es la incorporación en un texto jurídico vinculante del concepto de MV elaborado por la AEB. El artículo 1 de la 5AMLD modifica el texto de su predecesora, la Directiva 2015/89 (4AMLD) con la finalidad de añadir el concepto de MV, que a efectos legales se entiende como una:

> ….representación digital de valor no emitida ni garantizada por un banco central ni por una autoridad pública, no necesariamente asociada a una moneda establecida legalmente, que no posee el estatuto jurídico de moneda o dinero, pero aceptada por personas físicas o jurídicas como medio de cambio y que puede transferirse, almacenarse y negociarse por medios electrónicos.

7.3. Naturaleza jurídica

La aparición de estas nuevas formas de representación de valor y la ausencia de una regulación integral han planteado problemas a la hora de determinar la naturaleza jurídica de las MV, en particular del *bitcoin*.

En Europa, los diferentes documentos analizados por las instituciones financieras (el BCE y la AEB) concuerdan en que las monedas virtuales son una representación digital de un valor monetario no emitido por una autoridad central y aceptado como alternativa de pago. De acuerdo con el contenido de estos informes, las MV se configuran como una especie de SPE que involucra un conjunto de instrumentos, procedimientos y reglas para la transferencia de fondos entre sus participantes.

En el año 2015, la naturaleza jurídica del *bitcoin* fue analizada por el Tribunal de Justicia de la Unión Europea (TJUE) en el caso C 264/14, a efectos de la aplicación de la Directiva que regula el impuesto al valor agregado (IVA)[26]. En esta oportunidad, el TJUE

[24] *Fifth Anti/Money Laundering Directive*

[25] Estos proveedores permiten el acceso a los distintos esquemas de MV y son definidos en la Directiva 5AMLD como una entidad que presta servicios de salvaguardia de claves criptográficas privadas en nombre de sus clientes, para la tenencia, el almacenamiento y la transferencia de monedas virtuales.

[26] En razón de esta calificación, el TJUE considera que la operaciones en *bitcoins*, en su condición de *divisa virtual* están exentas del IVA en virtud de la disposición sobre las operaciones relativas a «las divisas, los billetes de banco y

calificó al *bitcoin* como una divisa virtual que se utiliza para realizar pagos entre particulares en Internet y en determinadas tiendas en línea y se puede adquirir y vender sobre la base del tipo de cambio[27]. Para determinar la aplicación de esta norma comunitaria, el TJUE estimó que las operaciones de cambio de divisas tradicionales por unidades de la divisa virtual *bitcoin* (y viceversa) son prestaciones de servicios realizadas a título oneroso en el sentido de la Directiva de IVA, ya que consisten en cambiar distintos medios de pago.

Como indicamos en el apartado anterior, la Comisión Europea ha seguido las orientaciones del BCE y la AEB al determinar, en la Directiva sobre prevención de blanqueo de capitales de 2018, que las MV son una representación digital de valor no emitida por ninguna autoridad pública.

En España, la Dirección General de Tributos (DGT) también ha analizado las funciones del *bitcoin* y otras MV como medios de pago y como mecanismos de inversión. En la resolución vinculante V2846-15, de 1 de octubre de 2015, la DGT califica al *bitcoin* como un medio de pago e indica que este tipo de MV "…por sus propias características deben entenderse incluidas dentro del concepto «otros efectos comerciales» por lo que su transmisión debe quedar sujeta y exenta del IVA"[28]. En su función de medio de inversión, la resolución vinculante V0808-18 de la DGT de 22 de marzo de 2018[29], determinó que las operaciones de compraventa o intercambio de criptomonedas como *bitcoin*, *litecoin* y *ripple*, dan lugar a una ganancia o pérdida patrimonial, en la medida que generan una alteración en la composición del patrimonio del contribuyente[30]. El *bitcoin* también ha sido aceptado por el Registro Mercantil como aporte de capital en la constitución de sociedades anónimas.[31]

Independientemente de los pronunciamientos de los distintos organismos oficiales, es importante aclarar que aunque actualmente la regulación de las MV es escasa, se han comenzado a dar los primeros pasos para incluirlas en el ámbito de aplicación de algunos instrumentos normativos como ha sucedido con la reciente aprobación de la Directiva 5AMLD.

---

las monedas que sean medios legales de pago». El artículo 135 de la Directiva IVA de 2006 exonera de su aplicación, entre otras a:

> …las operaciones, incluida la negociación, relativas a las divisas, los billetes de banco y las monedas que sean medios legales de pago, con excepción de las monedas y billetes de colección, a saber, las monedas de oro, plata u otro metal, así como los billetes, que no sean utilizados normalmente para su función de medio legal de pago o que revistan un interés numismático.

[27] Disponible en https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150128es.pdf (última consulta: 15 de julio de 2018)

[28] Disponible en https://www.iberley.es/resoluciones/resolucion-vinculante-dgt-v2846-15-01-10-2015-1432915 (última consulta: 15 de julio de 2018)

[29]Disponible en https://www.iberley.es/resoluciones/resolucion-vinculante-dgt-v0808-18-22-03-2018-imputacion-temporal-irpf-compraventa-monedas-virtuales-1476129 (última consulta: 15 de julio de 2018)

[30] La resolución indica textualmente lo siguiente:

> … en la venta de monedas virtuales, la alteración patrimonial habrá de entenderse producida en el momento en que se proceda a la entrega de las monedas virtuales por el contribuyente en virtud del contrato de compraventa, con independencia del momento en que se perciba el precio de la venta, debiendo, por tanto, imputarse las ganancia o pérdida patrimonial producida al período impositivo en que se haya realizado dicha entrega.

[31]*Coinffeine* es la primera empresa española cuyo capital social está constituido íntegramente en *bitcoins* a modo de aportación no dineraria. Para un análisis detallado del procedimiento de constitución de esta sociedad anónima y la forma de realizar los aportes en *bitcoin vid*. FERNÁNDEZ BURGUEÑO, PABLO: "Retos legales del bitcoin, ethereum y los smart contracts", en *Hacia una Justica 2.0 volumen X*, Actas del XX Congreso Iberoamericano de Derecho e Informática, volumen II, 2016 pp. 345-356.

El hecho que las MV no puedan asimilarse al dinero de curso legal implica que su aceptación no es obligatoria sino consensuada, esto significa que el acreedor de una obligación de pago puede rechazarlas y que corresponde a las partes mutuamente involucradas en la transacción acordar el pago mediante MV.

8. Consideración final: las monedas virtuales frente al dinero electrónico

A efectos de evitar tratar las MV como un tipo específico de dinero electrónico, es necesario establecer la distinción entre estos dos mecanismos de pago. Los SPE basados en el uso MV difieren sustancialmente de los esquemas de dinero electrónico en diversos aspectos, en los que destacan la forma de emisión, la intervención de las entidades financieras, la vinculación con el dinero de curso legal y la determinación del valor de la moneda.

Una de las diferencias fundamentales entre estos dos SPE es que las MV no tienen como contraparte física el dinero de curso legal, como sucede con el dinero electrónico, por lo tanto, los sujetos participantes y el régimen jurídico es notablemente diferente. Las MV no involucran la participación de los actores financieros tradicionales, el emisor generalmente es una empresa privada no financiera, es por ello que las normas de regulación y supervisión del sector financiero no son aplicables. En los esquemas de MV el control íntegro lo asume el emisor, quien gobierna la red y administra la emisión y circulación del dinero.

En cuanto a la vinculación con el dinero de curso legal, en el dinero electrónico existe la obligación de reembolso impuesta por ley a las EDE, lo que significa su convertibilidad obligatoria en dinero fiduciario. La circulación del dinero electrónico es restringida, es por ello que al recibirlo, su titular lo debe remitir a la entidad emisora para proceder a su convertibilidad. En las MV no necesariamente existe tal vinculación, ya que éstas pueden circular sin restricción y también se pueden intercambiar unas por otras sin ser convertidas en dinero fiduciario. Aunque es posible el intercambio de MV por dinero fiduciario, este vínculo no está regulado por la ley.

El respaldo del dinero electrónico es el dinero de curso legal, es por ello que se requiere que el valor monetario esté almacenado previamente en un soporte electrónico; el respaldo de las MV es la confianza en la tecnología y en los participantes en la red: el consenso es el aval de la transacción.

A efectos de evitar el doble gasto, en el caso del dinero electrónico el aceptante del medio de pago debe remitir la moneda a la entidad emisora y ésta debe verificar que la moneda no ha sido cobrada previamente antes de proceder a la conversión a dinero de curso legal. En el esquema de las MV el control del doble gasto lo proporciona la tecnología *blockchain*.

Respecto a su valor, las MV no solo funcionan como medios de pago, también se pueden intercambiar unas por otras. Su valor se basa en un tipo de cambio específico que puede fluctuar sobre la base de la demanda y oferta, es decir, pueden conservar, aumentar o disminuir su valor. El valor del dinero electrónico es fijo, se emite por un valor igual a los fondos recibidos y sólo es convertible en dinero efectivo a su valor nominal.

BIBLIOGRAFÍA

FERNÁNDEZ BURGUEÑO, PABLO: "Retos legales del bitcoin, Ethereum y los smart contracts", en *Hacia una Justica 2.0 volumen X,* Actas del XX Congreso Iberoamericano de Derecho e Informática, volumen II, 2016 pp. 345-356.

NAKAMOTO, Satoshi "*Bitcoin: a Peer to Peer Electronic Cash System*", disponible en https://bitcoin.org/bitcoin.pdf

MARTÍNEZ NADAL, A: *Dinero electrónico: aproximación jurídica*, Civitas, Madrid, 2003, p. 6

RICO CARRILLO, Mariliana: *El pago electrónico en Internet. Estructura operativa y régimen jurídico,* Thomson Reuters Aranzadi, Madrid, 2012.

TAPSCOTT D. y A. TAPSCOTT: *Blockchain Revolution*, Penguin Random House, LLC, New York, 2016 p.

ALCANCE DE LAS FIRMAS DIGITALES EN EL META

Por: ***Paula Naranjo***
Colombia

1. INTRODUCCION

Contexto de las firmas digitales.

Con la llegada de importantes y trascendentes tiempos como lo fue el término del siglo XX y el arrasador siglo XXI vemos incorporados en ellos la solución a muchos problemas, aun no solucionados del todo, en los que se veía un país como Colombia con los temas de las Comunicaciones y las Tecnologías, que de forma considerable han dado un giro de 180 grados en la forma en como no solo la administración ve la necesidad de funcionar, desarrollar e interactuar con las demás entidades y los administrados, sino como los privados y de forma general personas del común han hecho de estos avances actos de cotidianidad.

Otro acontecimiento que dio cabida al uso de la firma digital como herramienta tecnológica fue el innovador comercio electrónico, este surge de la combinación entre la informática y los medios de comunicación, esto claramente demostrando el alcance de la ciencia en la cotidianidad de la vida de todas las personas.
Sin embargo, hay temas que carecen de información y promulgación suficiente que lleguen de manera directa y eficaz a las personas para el debido conocimiento de estos y por qué no la implementación de los mismos; es así que desde la academia decidimos por medio de la investigación aprehender y transmitir lo adquirido por medio de este artículo.

Importancia del recorrido de mensaje de datos.

En el marco del desarrollo de las comunicaciones y las tecnologías se habla ahora de una información que plasmada en un medio tecnológico pasara a llamarse un mensaje de datos contenido ahora en un documento electrónico que debe gozar de seguridad, autenticidad y si el usuario lo desea también de disponibilidad, es de esta forma como se recurre a la internet**,** (Herrera Pérez 2005):

> En el mundo moderno la información se maneja en forma de datos, es decir, la información que se procesa y almacena en los sistemas de cómputo y que normalmente se relaciona con números, símbolos y texto. La generación y el procesamiento de los datos se realizan por medio de los sistemas de cómputo, y es lo que se conoce como informática. El transporte de esos datos para el intercambio de información se efectúa a través de las redes de transmisión de datos y en lo que se conoce como tele informática. Si bien la primera disciplina puede funcionar por sí sola, cuando se trata de compartir con otras entidades la información y el resultado el procesamiento de esta, es imprescindible el apoyo de la segunda disciplina.

Ahora bien, hablando de aquel mensaje de datos que requiere de seguridad, confidencialidad, autenticidad y no repudio es necesario la intervención de una herramienta que brinde todos estos componentes para la confiabilidad a la hora de necesitar intercambiar ese mensaje de datos con otra persona, esa herramienta es la firma digital.

Las firmas digitales, como se habló anteriormente es una herramienta útil y eficaz que se ha venido implementando debido a los avances del siglo xxi para realizar comunicaciones, efectuar transacciones, crear documentos electrónicos o cualquier otra actividad mediante el uso del intercambio electrónico de datos y su importancia para el desarrollo del comercio y la producción,

permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado.

Claramente debe existir un manejo y vigilancia para contrarrestar cualquier tipo de amenaza al mensaje de datos que se va enviar, para ello es necesario un proceso de identificación y autenticación, en donde el usuario deberá ingresar un Nombre o cualquier otra cosa que lo determine y sumando a esto una contraseña que asegure que es en realidad la persona que dice ser.

Uso de las firmas digitales Colombia.

Ahora bien, con la llegada de la Ley 527 de 1999 a Colombia, el estado se ve en la necesidad de transformar y agregar al ordenamiento jurídico para estar a la vanguardia de los nuevos avances tecnológicos en materia comercial y de las comunicaciones, algo que facilitase la nueva manera de hace más fácil el intercambio de información, de adquirir productos y servicios de forma rápida y segura y en general de las relaciones internacionales tanto del sector público como del privado.

Como cualquier acontecimiento, las firmas digitales trajeron consigo la posibilidad de que con la más alta seguridad se mantuviese a salvo información que requiere de esta estricta característica, para ello según la historia de Certicámara, S. A. (Certicámara - Líderes en certificación digital en Colombia 2017) dice:

> En el año 2001, la Cámara de Comercio de Bogotá, en asocio con las Cámaras de Comercio de Medellín, Cali, Bucaramanga, Cúcuta, Aburrá Sur y la Confederación de Cámaras de Comercio, Confecámaras crearon la Sociedad Cameral de Certificación Digital, CERTICÁMARA S.A., entidad de certificación digital abierta, constituida con el propósito de asegurar jurídica y técnicamente las transacciones, comunicaciones, aplicaciones y en general cualquier proceso de administración de información digital de conformidad con la Ley 527 de 1999 y los estándares técnicos internacionales. Los servicios de Certificación Digital de nuestra entidad están soportados gracias a la mundialmente y reconocida tecnología PKI, de origen europeo, para el envío, recepción, archivo y procesamiento de la información electrónica.” Fue así, con la ayuda de las principales Cámara de Comercio del País y Confecámaras se crea esta sociedad para que sea en el caso de las firmas digitales aquella entidad que participaría como un tercero de confianza para la expedición de los certificados digitales o también llamados claves públicas en el proceso de envío de mensaje de datos o documentos electrónicos de entidades públicas y también del sector privado.

Ahora bien, las entidades encargadas de esto expiden “Certificados Digitales” que son en pocas palabras aquel documento digital (quiere decir, no es un papel) que garantiza o respalda de forma técnica y legal los datos del titular de ‘este junto con su clave pública y que además es firmado para que tenga validez por una autoridad certificado, un ejemplo de ello es que sea firmado por Certicámara, S.A.

El cuestionamiento que surge es: ¿no se le hará necesario implementar un recurso tecnológico para el mejoramiento de la administración en cuanto a seguridad?, pues por supuesto no somos ajenos a distintos delitos de corrupción, falsificación de documentos y entre otros que podrían ser evitados con la implementación de esta herramienta y no solo en la administración sino en el comercio a cargo de los particulares, cuyos negocios se han podido ver afectados por artimañas de terceros para delitos de estafa, hurto entre otros, y es que en Meta, el uso de esta herramienta útil como lo es la firma digital tanto en las entidades públicas como privadas no es habitual, y el desconocimiento sobre todo aun en los administrados y personas en general.

2. MARCO TEORICO

En el artículo 2 de la Ley 527 de 1999 encontramos la definición de firma digital, como un procedimiento matemático conocido vinculado a la clave del iniciador y al texto del mensaje; que garantiza dos atributos propios de las comunicaciones electrónicas: la autenticidad y la integridad, que a su vez derivan en un tercero que tiene también gran trascendencia jurídica: el no repudio de acuerdo al Decreto 2364 de 2012, el mecanismo que garantiza autenticidad e integridad.

> La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel, es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. Algunos de los atributos más representativos de la firma digital son: es única, es verificable, está bajo control exclusivo del iniciador, está ligada a la información del mensaje y está de acuerdo con la reglamentación. (Firma digital: instrumento de transmisión de información a entidades financieras 2011).

Funcionamiento.

La firma digital de un mensaje electrónico está asociado a un proceso coordinado, organizado y secuencial para permitir que sea seguro, para ello se tiene que:

1. El emisor crea un mensaje determinado
2. El emisor aplica al mensaje una función hash y así obtiene un resumen del mensaje
3. El emisor cifra el mensaje utilizando su clave privada
4. El emisor le envía al receptor un correo electrónico con los siguientes elementos:
   4.1 El cuerpo del mensaje (sin cifrar o cifrado, por medio de la clave pública del receptor)
   4.2 La firma del mensaje, que se compone de:
      4.2.1 El hash o mensaje cifrado con la clave privada del emisor
      4.2.2 El certificado digital del emisor con todos sus datos y que está cifrado con la clave privada del Prestador de Servicios de certificación.

(LRDM, BSMD, DMNC. "Firma digital: instrumento de transmisión de información a entidades financieras". Escuela de Ingeniería de la Organización. Facultad de Minas, Universidad Nacional de Colombia. 2011.)
Las firmas digitales se basan en los certificados digitales que son comprobadoras de identidad, son emitidos por un tercero conocido como la entidad certificadora CA donde garantizara que la persona natural o jurídica está registrada, existe y cuenta con un certificado digital. En las utilidades de las firmas digitales encontramos la autenticidad que nos permite garantizar que la persona que firma es quien dice ser, la integridad que garantiza que el contenido no se ha modificado y la no renuncia que demuestra a todas las partes el origen del contenido firmado.

Requisitos para la firma digital:

1. La firma digital debe ser válida. Para ello una entidad de certificación en la que confíe el sistema operativo debe firmar el certificado digital en el que se basa la firma digital.
2. El certificado asociado a la firma digital no debe a ver caducado.
3. La persona o la organización que firma (conocida como el publicador) es de confianza para el destinatario.
4. El certificado asociado a la firma digital ha sido emitido para el publicador firmante por una entidad de certificación acreditada.

El proceso que se lleva a cabo para realizar la firma digital es el siguiente: Se emplean 2 algoritmos de cifrado de clave asimétrica (o pública), estos algoritmos funcionan mediante el uso de 2 claves, una pública y una privada que van a pertenecer a un mismo sujeto, esas claves se obtienen mediante un algoritmo y empleando un algoritmo concreto. Un mensaje cifrado con la clave pública de un sujeto solo podrá ser descifrado con la clave privada del mismo y nunca con la pública, la clave pública está al alcance de cualquiera, mientras que la clave privada debe ser custodiada únicamente por el propietario del par de claves.

Entonces al momento de recibir el correo electrónico el receptor descifra el certificado digital del emisor que está en el correo electrónico usando la clave pública del prestador de servicios de certificación que ha expedido el certificado , ahora esa clave pública se encuentra en la página web del prestador de servicios de certificación, posteriormente una vez descifrado el certificado el receptor accede a la clave pública del emisor y con esta clave descifrara el hash creado por el emisor para ello el receptor aplicara al cuerpo del mensaje la misma función has que utilizo el emisor con anterioridad para obtener un mensaje , en el caso en el que el cuerpo del mensaje también este cifrado para garantizar una mayor seguridad , el receptor deberá descifrarlo utilizando su propia clave privada .

Después el receptor comparara el hash que tienen que coincidir y de esta manera se asegurara de que el mensaje no haya sido alterado durante su envió, de esta manera se garantiza que el mensaje cifrado por el receptor con la clave pública no ha sido cifrada con la clave privada del emisor y por tanto proviene de este. (Firma digital: instrumento de transmisión de información a entidades financieras 2011).

Entidad de certificación abierta: Son las que se encargan de ofrecer servicios propios de las entidades de certificación. Su uso no se limita al intercambio de mensajes entre la entidad y el suscriptor como la cerrada y recibir remuneración por estos. (Duran Noble, 2012)

Entidad de certificación cerrada: Encargadas de ofrecer servicios propios de las entidades de certificación solo para el intercambio de mensajes entre la entidad y el suscriptor, pero sin exigir remuneración por ellos. (Duran Noble, 2012)

La firma digital se define como una secuencia de datos electrónicos que se obtienen como consecuencia de aplicar a un mensaje determinado un algoritmo de cifrado asimétrico. Estos sistemas de criptografía asimétrica están basados en el cifrado de la información a partir de un par de claves diferentes, denominadas pública y privada, que se atribuyen a una persona determinada. El proceso se fundamenta en que la clave privada sólo es conocida por la persona a la que se han atribuido el par de claves. En cambio, la clave pública puede ser conocida por cualquier persona que el emisor desee. (Seguridad en el comercio electrónico 2018)

Antecedentes y Desarrollo legal de la Firma Digital.

La evolución tecnológica de los últimos años en el campo electrónico y digital, ha transformado la industria, el comercio, el sector servicios, domestico, entre otros.

Hoy en día cada vez hay una demanda mayor de las transacciones ante una necesidad de interactuar por intermedio de redes de computadoras. El concepto de firma digital nace de una oferta tecnológica para acercar la firma manuscrita (hológrafa) a lo que se llama el trabajo en redes o ciberespacio que garantiza los trámites hechos en Internet.

Jijena Leiva, Palazzi Téllez Valdés 2003

> En lo que respecta al derecho, el encuentro con esta sociedad e Internet es inevitable, ya "que donde hay sociedad hay derecho" (ubi societas ibi ius) y esta sociedad de la información no puede constituir una excepción. Ahora que el grado de tele informatización de la sociedad ha

llegado a puntos insoslayablemente álgidos, la intervención del derecho se convierte en imperioso menester, a través del surgimiento de un cuerpo de normas jurídicas que rigen de manera efectiva estas nuevas situaciones, dentro de las cuales y sin pretender ser exhaustivos, tenemos a Internet, los nombres dominios, el comercio electrónico Y las firmas digitales, como sólo algunos ejemplos representativos.

En 1976 el concepto de firma digital fue introducido por Diffie y Hellman y decía que la firma digital era un conjunto de datos asociados a un mensaje que permite asegurar la identidad del firmante y la integridad del mensaje.

En 1978 R. Riveros, A Shamir y L. Adleman, del MIT proponen el hasta hoy más usado método firma digital, denominado RSA, ese método en principio obedece a los mismos principios que la firma autógrafa.
En 1985 se publica la tesis (A Public Key Cryptosystem and Signature Scheme Based Discrete Logarithms) con la que posteriormente se construyó la base de algoritmos de la firma digital, adoptando por el instituto Nacional de Estándares y Tecnológico como el estándar de firmas digitales.

1991 Ub algoritmo propuesto por el instituto nacional de normas y tecnología de los estados unidos para su uso en su estándar de firma digital (DSS) ese algoritmo como su nombre lo indica, sirve para firmas y para cifrar información.

1995 La primera ley en materia de firma digital en el mundo fue la denominada "Utah Digital Signature Act" publicada en mayo de 1995 en el Estado de UTAH, en Estados Unidos.

3. MARCO LEGAL

Aunque el tema de firmas digitales aparentemente se podría decir que ha tenido poca regulación, a continuación se presenta la normatividad de la cual la gente tiene poco conocimiento pero que es de necesario aprendizaje.

Ley 527 de 1999: esta desarrolla varios temas de datos pero en concreto respecto a la firma digital, nos da una pequeña definición de esta y en un capítulo dedicado a este tema, expresa los atributos de la firma digital y equipara esta con la firma escrita, siempre y cuando cumpla con ciertos requisitos allí previstos. Así pues la Corte Constitucional explica el porqué de la necesidad de esta ley:

Los antecedentes de la Ley 527 de 1999

- ✓ ***Ley 1564 de 2012*:** comúnmente conocido como código general del proceso y que reemplaza al antiguo código de procedimiento civil o DECRETO 1400 DE 1970 y sus posteriores modificaciones. A diferencia del antiguo código que en los temas de poderes especiales solo podían ser conferidos mediante escritura pública o memorial dirigido al juez, en el nuevo código general del proceso promueve el uso de la firma digital, haciendo uso de esta para conferir poderes especiales. (Código General del Proceso 2012)

- ✓ ***Ley 962 de 2005:*** conocida como ley anti tramites, en sus primeros artículos se refiere al tema de la firma digital, haciendo un énfasis de hacer uso de las nuevas tecnologías con el fin de cumplir principios tales como economía, celeridad, entre otros y ya en el tema específico, hace alusión de que en caso de la sustanciación de actuaciones y actos administrativos, la firma escrita puede ser reemplazada por la firma digital, siempre y cuando esta cumpla sus requisitos legales. Es importante aclarar que todo el tema del uso de tecnologías y entre estas esta la firma digital, podrán ser usados si la entidad de la administración pública dispone de las herramientas necesarias para el uso de estos avances tecnológicos. (Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades

del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. 2005)

- ✓ ***Ley 1150 de 2007:*** que regula temas de contratación estatal, añade el uso de los medios tecnológicos entre ellos la firma digital, para todo lo relacionado a actos administrativos, contratos o actos derivados en la etapa contractual o pre-contractual entre otros temas, el uso de estos medios está regulado por ley 527 de 1999. (Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. 2007)

- ✓ ***Decreto 1747 de 2000:*** es aquel decreto que reglamenta parcialmente la ley 527 de 1999 en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. Claramente dan definiciones de conceptos implementados en las entidades y en los certificados. Explican todo lo relacionado a las entidades de certificación abiertas y cerradas, sus acreditaciones y la información que en ello va. También sobre la Declaración de Prácticas de Certificación, su contenido; la infraestructura de todo lo relacionado en los certificados, patrimonio, garantías deberes entre otras como lo relacionado a las facultades de la Superintendencia de Industria y Comercio. (por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales. 2000)

- ✓ ***Decreto Ley 019 de 2012***: modificó unos artículos de la Ley 527 de 1999 en lo relacionado a las entidades de certificación. En el presente decreto ley el artículo 160 dispuso necesario y obligatorio que las entidades de certificación debían estar acreditadas ante la ONAC. Derogó este decreto ley en su artículo 176 también artículos de la ley 527 de 1999 como lo son el 41 y 42. (Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública 2012)

- ✓ ***Decreto 333 de 2014:*** este decreto es el encargado de reglamentar el artículo 160 del decreto ley 019 de 2012, de lo que resulta la reglamentación de las entidades de certificación y la renovación del artículo 29 de la Ley 527 de 1999. Por ende el haber este decreto reglamentado el artículo 160 del decreto ley 019 de 2012 con respecto a la acreditación de las entidades de certificación seguido a esto entraría a agregar o complementar los artículos 29, 30, literal (h) del 32 y el 34 de la ley 527 de 1999. (Por el cual se reglamenta el artículo 160 del Decreto-ley 19 de 2012 2014)

- ✓ ***Sentencia C-662-2000:*** es la respuesta de la Corte Constitucional a La ciudadana Olga Lucia Toro Pérez, en ejercicio de la acción pública de inconstitucionalidad consagrada en la Constitución Política de 1991, pide a la Corte declarar inexequibles los artículos 10, 11, 12, 13, 14, 15, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44 y 45 de la Ley 527 de 1999.A lo que la corte responde declarando exequible todos y cada uno de estos artículos, además aclarando a la accionante cual había sido modo groso el porqué de la expedición de la ley, y esto fue lo que aclaro:

  "Desde luego, este cambio tecnológico ha planteado retos de actualización a los regímenes jurídicos nacionales e internacionales, de modo que puedan eficazmente responder a las exigencias planteadas por la creciente globalización de los asuntos pues, es indudable que los avances tecnológicos en materia de intercambio electrónico de datos ha propiciado el desarrollo de esta tendencia en todos los órdenes, lo cual, desde luego, implica hacer las adecuaciones en los regímenes que sean necesarias para que estén acordes con las transformaciones que han tenido lugar en la organización social, económica y empresarial, a nivel mundial, regional, local, nacional, social y aún personal.

  La exposición de motivo del proyecto presentado al Congreso de la República por los Ministros de Justicia y del Derecho, de Desarrollo, de Comercio Exterior y de Transporte,

que culminó en la expedición de la Ley 527 de 1999, ilustró las exigencias que el cambio tecnológico planteaba en términos de la actualización de la legislación nacional para ponerla a tono con las nuevas realidades de comunicación e interacción imperantes y para darle fundamento jurídico a las transacciones comerciales efectuadas por medios electrónicos y fuerza probatoria a los mensajes de datos, en los siguientes términos :

"…

El desarrollo tecnológico que se viene logrando en los países industrializados, permite agilizar y hacer mucho más operante la prestación de los servicios y el intercambio de bienes tangibles o intangibles, lo cual hace importante que nuestro país incorpore dentro de su estructura legal, normas que faciliten las condiciones para acceder a canales eficientes de derecho mercantil internacional, en virtud a los obstáculos que para éste encarna una deficiente y obsoleta regulación al respecto"

Claro está, tomando también en cuenta directrices u observaciones hechas por la Comisión de las Naciones Unidas para el desarrollo del Derecho Mercantil Internacional y la expedición de la Ley Modelo sobre comercio electrónico.

- ✓ ***Sentencia C-831-2001:*** es la respuesta de la Corte Constitucional ante la acción pública de inconstitucionalidad presentada por el ciudadano Daniel Peña Valenzuela que demandó el artículo 6 de la Ley 527 de 1999 que se encuentra en el Capítulo 2 y habla sobre la Aplicación de los requisitos jurídicos de los mensajes de datos, pues cree que vulnera los articulo 28 y 152 de la constitución política, ya que el artículo se refiere a que cualquier norma que exija información por escrito quedara satisfecho aun cuando esta se haya hecho por un mensaje de datos y que luego pueda volverse a consultar, pero el ciudadano cree que vulnera el Artículo 28 de C.P que trata sobre la libertad personal, adherido a esto como un derecho fundamental, y que una tema como este de derecho fundamental ha debido ser tratado por una ley estatutaria y no por una ley ordinaria como lo es la ley 527 de 1999, a lo que la corte respondió que la ley hacia énfasis al comercio electrónico de bienes y servicios, y por tanto no debía ser entendido por el ciudadano desde ese punto de vista el artículo 6 de la ley 527 de 1999, así que la Corte declaro exequible el artículo de la presente.

- ✓ ***La Circular No.643 de 2004:*** de la Superintendencia de Notariado y Registro:

En esta circular fijan las condiciones para enviar documentos que nazcan de las Notarías a las Cámaras de Comercio utilizando firmas digitales certificadas. (Rincón Cárdenas 2006)

- ✓ ***La Circular 012 de 2004:*** La Supersalud exige que el envío de reportes de información financiera y general de las ESE (Empresas Sociales del Estado) se haga con el uso de las firmas digitales certificadas. (Rincón Cárdenas 2006)

- ✓ ***La Circular 013 de 2004***: La Supersalud exige que el envío de reportes de información sobre IVA cedido al Sector Salud por parte de las gobernaciones, secretarias de hacienda, secretarias de salud, productores de licores entre otros. (Rincón Cárdenas 2006)

- ✓ ***La Circular externa 50 de 2003***: Ministerio de Industria y Comercio, establece la posibilidad del registro de importación a través de Internet (VUCE Ventanilla única de Comercio Exterior). Este trámite puede hacerse de forma remota firmado digitalmente y de ese modo reducir el trámite que se piensa racionalizar por este medio.

Esta circular crea la posibilidad de que se pueda hacer el registro de importación a través de Internet, y este trámite se podrá hacer de forma rápida firmado digitalmente y así crear rapidez para este procedimiento. (Rincón Cárdenas 2006)

- ✓ ***Circular de Supersociedades:*** Dirigida a todas las sociedades mercantiles vigiladas y controladas por la superintendencia para el envío de información financiera y contable a través del sistema SIREM el Sistema de Información y Riesgo Empresarial un sistema vía Web que

permite entregar todos los reportes e informes por esta vía con el uso de certificados digitales. (Rincón Cárdenas 2006)

- ✓ ***La Circular 011 de 2004:*** La Supersalud exige que el envío de reportes de información financiera y general de las IPS se haga con el uso de las firmas digitales certificadas. (Rincón Cárdenas 2006)

- ✓ ***Directiva Presidencial N° 4 del 03 de Abril de 2012*** Consiste en el reemplazo del papeleo por soportes y medios electrónicos, que se fundamentan en la implementación de Tecnologías de la Información y las Telecomunicaciones. Claro que esto tiene aspectos más favorables que el descongestionamiento en la administración, también ayuda a la mejora y protección del medio ambiente. El propósito de seguir adelante con la Política de Eficiencia Administrativa y Cero Papel en la Administración Publica, los organismos y entidades a las que va destinada esta directiva tienen el deber de organizar, racionalizar, disminuir todo los tramites y procesos internos para una eficiente y rápida prestación del servicio por parte de estas entidades. (Eficiencia administrativa y lineamientos de la política cero papel en la administración pública 2012)

4. ACERCA DEL FUNCIONAMIENTO DE LAS FIRMAS DIGITALES

¿Cómo asegura esto la autenticidad, la integridad y el no repudio de este mensaje?

Cuando el destinatario recibe el mensaje, lo primero que debe hacer es verificar la firma digital del correo. Para ello, en base al funcionamiento del algoritmo de clave asimétrica, deberá emplear la clave pública del remitente para descifrar el hash del correo. Si el hash se descifra correctamente y corresponde con el resto del correo recibido se puede concluir que, en primer lugar, dicho correo ha sido enviado por quien dice ser (autenticidad), ya que en caso de que la firma no hubiera sido cifrada con la clave privada del remitente, no se podría haber descifrado con su clave pública. (LRDM, BSMD, DMNC. "Firma digital: instrumento de transmisión de información a entidades financieras". Escuela de Ingeniería de la Organización. Facultad de Minas, Universidad Nacional de Colombia. 2011.)

En segundo lugar su integridad, ya que en caso de que el mensaje hubiera sido manipulado el hash del correo no coincidiría tras descifrar el mismo; y por último el no repudio que no deja de ser la consecuencia de las dos anteriores, si la firma es correcta el emisor no podrá negar el contenido de dicho correo ni que haya sido redactado o enviado por nadie que no fuese él mismo según David Cutanda. (Cutanda, 2013)

David Cutanda también nos explica que existe el protocolo SSL que es un estándar de transmisión de datos seguros sobre Internet empleado en diversos protocolos de la capa de aplicación y protocolos de la capa de transporte (TCP) como medio para establecer conexiones seguras. El protocolo SSL funciona empleando certificados de clave asimétrica .El funcionamiento básico de SSL consiste en lo siguiente: la entidad establece una conexión con el servidor mediante su puerto HTTPS (de forma estándar 443), para lo cual tendrá que realizar una solicitud de inicio de sesión segura , como respuesta el servidor devuelve un certificado en formato X.509 , que constituye su clave pública .Después de certificar que los datos del certificado son correctos , el cliente procede a generar una clave simétrica aleatoria, la cual se empleara en la transmisión de datos , cifra esta clave con la clave pública del servidor y la envía al mismo ,tras la recepción , el cliente como el servidor abran establecido una conexión segura empleando una clave simétrica para su sesión , en caso de que se finalizare la sesión por cualquier motivo se desechara dicha clave y se renegociara una nueva en la siguiente conexión.

Un Certificado Digital consta de una pareja de claves criptográficas, una pública y una privada, creadas con un algoritmo matemático, de forma que aquello que se cifra con una de las claves sólo se puede descifrar con su clave "la clave pública", esta forma parte de lo que se denomina

Certificado Digital, que es un documento digital que contiene la clave pública junto con los datos del titular, todo ello firmado electrónicamente por una Autoridad de Certificación, que es una tercera entidad de confianza que asegura que la clave pública si corresponde con los datos del titular y la clave privada es la de un titular que debe ser privada y exclusiva .El formato de los Certificados Digitales está definido por el estándar internacional ITU-T X.509. De esta forma, los certificados pueden ser leídos o escritos por cualquier aplicación que cumpla con el mencionado estándar. Los certificados digitales posibilitan el envió de mensajes cifrados esto es según Certsuperior y la universidad politécnica de valencia. Los certificados digitales posibilitan el envío de mensajes cifrados. (Certsuperior. Como obtener un certificado digital . 2002)

(Valencia, 2012):

> Para emitir los certificados digitales las Entidades de Certificación Digital utilizan lo que se conoce como la Infraestructura de Clave Pública PKI, que es el conjunto de elementos tecnológicos que, mediante la utilización de un par de claves criptográficas, una privada que solo posee el suscriptor del servicio y una pública que se incluye en el certificado digital, logran.
> - Identificar a quien envía una comunicación
> - Impedir que terceras personas puedan observar los mensajes que se envían a través de medios electrónicos
> - Impedir que un tercero pueda alterar la información que es enviada a través de medios electrónicos
> - Evitar que el suscriptor del servicio de certificación digital que envió un mensaje electrónico pueda después negar dicho envío.

Según Microsoft existen 2 técnicas básicas para cifrar información o dos tipos fundamentales de criptosistemas, una es el cifrado simétrico que es denominado como cifrado de clave secreta y el otro es el asimétrico que es denominado cifrado de clave pública.
Cifrado electrónico o sistema criptográfico proveerá los 3 servicios de seguridad informático: Integridad, confidencialidad, disponibilidad. Uno de los puntos más importantes es la confiabilidad del mismo debido a que cualquiera puede generar una clave asimétrica e incluir los campos que desee en el certificado. De nuevo en base a este hecho surge la necesidad de la existencia de Autoridades de Certificación (CA), quienes se encargan de emitir certificados confiables y reconocidos. La criptografía te permite cifrar y descifrar información utilizando las técnicas conocidas (algoritmos).

Sistema simétrico o clave compartida, el Criptosistemas simétricos o de clave, en este sistema se usara solo una clave que es utilizada por el emisor y el receptor, esta clave es utilizada para encriptar y des encriptar.
Sistema asimétrico, Criptosistemas asimétricos o de clave pública ,en este sistema se usaran dos claves, una clave pública que es de libre acceso y puede ser concisa por cualquier persona y una clave privada que es de uso exclusivo y privado del usuario es decir la clave secreta.
Un certificado digital es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet. Se trata de un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de Internet. (Cutanda, 2014)

¿Cómo sé que el certificado descargado es real y no se ha generado de forma fraudulenta?

Allí aparecen las Autoridades de Certificación (CA), que son organismos directamente encargados de generar certificados digitales de cualquier tipo, desde firma digital hasta certificados de servidor SSL , estas serán entidades autorizadas que generan certificados como anteriormente las nombrábamos ,en cada uno de los certificados SSL (en base del protocolo x.509) se establece un emisor que es la entidad (persona, asociación, empresa etc.) que ha generado el certificado , verificando el emisor , así como los certificados involucrados se puede

asegurar si el certificado lo ha emitido dicha entidad y de este modo se puede clasificar en base a la confianza que se deposita en dicha entidad . Esta validación queda reflejada en el diagrama de funcionamiento de SSL.

Existe una jerarquía nacional de certificadores registrados, que son todas las autoridades certificadoras que han aprobado el proceso de evaluación del ECA y que se han registrado ante la Dirección. Esto incluye: La CA Raíz, Las CA de Políticas y las CA emisoras registradas.

La CA Raíz y las CAS de Políticas son parte de la jerarquía nacional administrada por el Ministerio de Ciencia y Tecnología (MICIT), que se reglamentan a través del Comité Asesor de Políticas (CAP) y de la Dirección de Certificadores de Firma Digital (DCFD). Las CAS emisoras registradas deben implementar esta política, para formar parte de la jerarquía nacional de certificadores registrados.

Las Autoridades de Certificación disponen de un certificado conocido como Certificado Raíz (Root CA), y como su nombre indica es el certificado que validará todos y cada uno de los certificados emitidos por la CA; sin embargo, este certificado no es el que firmará los certificados de suscriptor (o certificados finales), sino se empleará únicamente para firmar los denominados Certificados Subordinados (Sub-CA), y estos últimos firmarán los certificados de suscriptor (o finales) pero en Colombia aún no se ve esta jerarquía. (Cutanda, 2014)

¿Cómo sabemos que el certificado que tenemos ha sido emitido por una de estas entidades?

Por la cadena de confianza, este modelo establece una relación entre certificados que permiten asegurar que dicho certificado ha sido emitido por una autoridad de certificación. (Cutanda, 2014)

¿Cómo sé que el certificado que firma el anterior es válido?

El modelo de cadena de confianza este modelo establece una relación entre certificados, el Root CA que validara todos los certificados, pero solo firmara los certificados subordinados y los certificados subordinados firmaran los certificados finales, es decir los del suscriptor, el motivo de esta jerarquía es para proteger al certificado raíz ya que si un tercero consiguiera la clave privada de un certificado raíz emitiría certificados de CA debido a ello los certificados finales no están firmados con esta clave , un certificados de suscriptor firmado por el raíz no sería de suscriptor sino subordinado, lo que conllevaría dar esa clave a un usuario , por este motivo la clave privada del certificado de raíz se encuentra en offline , en un dispositivo de seguridad cifrado. De modo que, para validar un certificado de un suscriptor, se deberá comprobar la firma para toda la cadena de confianza de la CA emisora, quedando así clara la procedencia del mismo. (Cutanda, 2014)

El formato de verificado x.509 el cual es un estándar del ITU-T (International Electro technical Commission) que se publicó por primera vez 1988 ese era el formato de versión en 1993 es extendida para incluir dos (nuevos campos que permitirían soportar el control de acceso a directorios ese sería el X.509 v2 para desarrollar el estándar de correo electrónico, en 1996 es publicado el nuevo formato x.509 v3 y sus elementos van hacer:

1. Versión: Versión del certificado codificado. Los valores aceptables son 1, 2 y 3.
2. Número de serie del certificado: Cada certificado emitido por una CA debe tener un número de serie único
3. Identificador del algoritmo de firmado: Este campo identifica el algoritmo empleado para firmar el certificado (como por ejemplo el RSA o el DSA).
4. Nombre del emisor: Este campo identifica la CA que ha firmado y emitido el certificado

5. Periodo de validez: La CA está obligada a mantener información sobre el estado del mismo. El campo consiste en una fecha inicial, la fecha en la que el certificado empieza a ser válido y la fecha después de la cual el certificado deja de serlo.
6. Nombre del sujeto: El nombre debe ser único para cada entidad certificada por una CA dada, aunque puede emitir más de un certificado con el mismo
7. Información de clave pública del sujeto: Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.
8. Identificador único del emisor: Este es un campo opcional que permite reutilizar nombres de emisor.
9. Identificador único del sujeto: Este es un campo opcional que permite reutilizar nombres de sujeto.
10. Extensiones: Las extensiones del X.509 V3. Proporciona una manera de asociar información adicional a sujetos, claves públicas, un campo de extensión tiene tres partes:
    10.1 Tipo de extensión. Es un identificador de objeto que proporciona la semántica y el tipo de información (cadena de texto, fecha u otra estructura de datos) para un valor de extensión.
    10.2 Valor de la extensión. Este subcampo contiene el valor actual del campo.
    10.3 Indicador de importancia. Es un flag que indica a una aplicación si es seguro ignorar el campo de extensión si no reconoce el tipo. El indicador proporciona una manera de implementar aplicaciones que trabajan de modo seguro con certificados y evolucionan conforme se van añadiendo nuevas extensiones. (Talens-Oliag, 2003)

Ley 527 de 1999 en su artículo segundo define las entidades de certificación de la siguiente manera: "*Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales*".

5. LA FIRMA DIGITAL COMO METODO DE SEGURIDAD INFORMATICA

Mediante derecho de petición con radicado 20170020009602 el día 16 de enero de 2017 se pidió información acerca de los delitos informáticos que se presentan en la zona del departamento del Meta, a cuya petición contestó DIANA MILENA BACCA DUARTE, Profesional de Gestión III, Dirección Seccional Meta. Fiscalía General de la Nación, quien arrojó el siguiente resultado:

Año	Delito	Cant.
2012	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	11
	Acceso abusivo a un sistema informático art 269a ley 273 de 2009, agravado por realizarse sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros art. 269h n1	2
	Acceso abusivo a un sistema informático. Art. 195 c. p.	2
	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	110
	Interceptación de datos informáticos, art 269c ley 273 de 2009	1
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009	1
	Transferencia no consentida de activos valiéndose de alguna manipulación informática o artificio semejante art. 269j ley 273 de 2009	2
	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	2

2013	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	123
	Interceptación de datos informáticos art 269c ley 273 de 2009 agravado por obtener provecho para sí o para un tercero. Art. 269h n5	1
	Interceptación de datos informáticos, art 269c ley 273 de 2009	1
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009	1
	Transferencia no consentida de activos valiéndose de alguna manipulación informática o artificio semejante art. 269j ley 273 de 2009	3
2014	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	10
	Acceso abusivo a un sistema informático. Art. 195 c. p.	2
	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	114
	Interceptación de datos informáticos, art 269c ley 273 de 2009	1
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009	5
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009, agravado por obtener provecho para sí o para un tercero. Art. 269h n5	1
	Transferencia no consentida de activos valiéndose de alguna manipulación informática o artificio semejante art. 269j ley 273 de 2009	2
2015	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	17
	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	120
	Interceptación de datos informáticos, art 269c ley 273 de 2009	2
	Transferencia no consentida de activos valiéndose de alguna manipulación informática o artificio semejante art. 269j ley 273 de 2009	1
2016	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	13
	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	140
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009	2
	Suplantación de sitios web para capturar datos personales art 269g ley 273 de 2009, agravado por aprovecharse de la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este. art. 269h n3	1
	Transferencia no consentida de activos valiéndose de alguna manipulación informática o artificio semejante art. 269j ley 273 de 2009	4
2017	Acceso abusivo a un sistema informático art 269a ley 273 de 2009	6
	Hurto por medios informáticos y semejantes art. 269i ley 273 de 2009	12
TOTAL		**713**

De lo anterior se puede inferir que la sociedad se encuentra en la necesidad de incorporar una herramienta tecnológica en su cotidiano vivir para disminuir las delitos informáticos.

6. METODOLOGÍA

La investigación manifiesta en este artículo es de carácter cualitativo, pues para la realización de tal se necesitó la caracterización de un tema y se partió de algo ya conocido y no de simples teorías, determinar sus cualidades y alcances en un determinado territorio, el uso de entrevista

como medio de recolección de datos característico de esta metodología llevo a una correcta dirección de nuestro escrito, además de otros medios como algunos libros. Además, se implementó un método descriptivo y analítico de las firmas digitales, abarcando una amplia manifestación del legislador que aparentemente no había pero que se logró manifestar en el reciente escrito.

7. CONCLUSIONES

El uso de herramientas tecnológicas a lo largo de la historia ha provocado que las mismas se hagan trascendentales para el desarrollo de las sociedades, desarrollo necesario para no quedar en el olvido, o sin importancia para otros países.

Ahora bien, es entendible que del uso de las herramientas tecnológicas se desprendan problemáticas a las que constantemente se ven avocadas las sociedades a solucionar, tal y como es el caso de firma digital, donde a raíz de su creación los mismos pensadores de la mismas tuvieron que desarrollar medidas de seguridad para impedir, detener o descartar del todo la violación o alteración de la información al momento de transmitir un mensaje de datos.

En un principio de nuestra investigación creímos que la firma digital era un tema que a lo mejor solo se llegó a plantear en una ley, pero que en realidad no se materializo en la realidad. A lo largo de la investigación nos dimos cuenta que la Firma Digital tenía una amplia regulación y que gozaba de elementos muy importantes que a lo ojos del sector público y privado se hacía cada vez más atractivo su uso.

No se puede desconocer claramente según lo expresado anteriormente el esfuerzo que se ha venido haciendo para que la firma digital pueda ser un mecanismo alterno de firma de documentos, en este caso de documentos electrónicos, por ello el Estado se vio en la tarea de darle una mayor garantía a las firmas digitales, y aquella garantía se ve plasmada en la creación de la ONAC como un medio de seguridad y de confianza a la sociedad de que estos nuevos medios traídos por las TICS gozan de total aprecio por el Estado, de tal manera que hasta la administración para una mejor y una mayor eficacia de su labor la han implementado.
Para nadie es un secreto que con la revolución digital ha traído consigo determinantemente el ingreso de nuevas tecnologías, consecuente a esto unas problemáticas que a lo largo de su desarrollo (de las tecnologías) también se han ido incrementando los problemas. Con ello hago alusión a las inseguridades que se generan con el uso de medios electrónicos para la comunicación, realización, finalización o dirección de negocios internacionales de índole público o privado.

Ahora bien, en el marco de una seguridad en los documentos electrónicos, manera por la cual se hacen posible las comunicaciones de sujetos que se encuentran muchas veces al otro lado del mundo, se ha visto necesario que a estos (documentos electrónicos) se les adhiera una herramienta para imposibilitar a un tercero ajeno de dicha relación a intervenir de forma negativa en ello, en otras palabras, evitar delitos informáticos, tales como: acceso abusivo a un sistema informático, hurto por medios informáticos y semejantes, suplantación de sitios web para capturar datos personales, interceptación de datos informáticos, entre otros, que, sin una herramienta como la firma digital, para asegurar esa información, sea o no trascendental para los sujetos de dichas relaciones, puede ser fácilmente hurtada, modificada, plagiada o en pocas palabras hackeada.

Es por ello, que uno de los factores implementados con el apogeo de la globalización, especialmente la llegada directa de las TIC'S, es la necesidad en la que se encuentran los estados de regular aquellas acciones y sus consecuencias, donde trascendentalmente y sin querer dejarlo a un lado, es por orden internacional que aquellas figuras han debido regularse. En el caso concreto, como Colombia, ha hecho caso a aquellas directrices de la ONU, en principio, de legislar sobre ello; sin embargo aunque su marco legal es amplio y especifico, aun no se ha podido llegar a la creencia fundamental que se pretende con el implemento de estas nuevas herramientas,

que es la de prevenir los delitos, que como se dijo antes, se suscitan en dichos temas, pues para nadie es un secreto que actualmente existen personas que dedican a la tarea de sustraer información no pertinente de manera ilícita, irregular o ilegal, ello, gracias al avance exponencial y no controlado de materiales tecnológicos que está al alcance fácilmente para cualquier persona; pero ahora es aún más necesario que estas herramientas que el legislador ha dispuesto, sean usadas idóneamente por los demás entes descentralizados para que exista armonía, integridad y buena práctica de aquellas herramientas.

8. REFERENCIAS

1. ¿Qué es un Certificado SSL? | Cert Superior, 2016. Certsuperior.com [online]
2. AREITIO BERTOLÍN, JAVIER, 2008, *Seguridad de la información*. 1. Madrid: Paraninfo Cengage Learning.
3. BACA URBINA, GABRIEL, 2016, *Introducción a la seguridad informática*. Distrito Federal: Grupo Editorial Patria.
4. BENNASAR, ANDRÉS JAUME, 2010, *La validez del documento electrónico y su eficacia en sede procesal*. 1. Valladolid: Lex Nova.
5. Certicámara - Líderes en certificación digital en Colombia, [no date]. Web.certicamara.com [online]
6. COMERCIO ELECTRÓNICO B2C: *LA PROTECCIÓN DE LOS CONSUMIDORES EN COLOMBIA*, 2002. e-Mercatoria [online], P. 8-10.
7. CORTÉZ SÁNCHEZ, JULIÁN DAVID and CARDONA MADARIAGA, DIEGO FERNANDO, 2015, *Gobierno electrónico en América Latina.* 1. Bogotá: Editorial Universidad del Rosario.
8. CUTANDA, DAVID, 2013, *Fundamentos sobre certificados digitales* - Security Art Work. Security Art Work [online]. 2013. [Accessed 19 April 2017]. Available from: https://www.securityartwork.es/2013/05/13/fundamentos-sobre-certificados-digitales/
9. CUTANDA, DAVID, 2014, *Fundamentos sobre certificados digitales – Declaración de Prácticas de Certificación* - Security Art Work. Security Art Work [online]. 2014. [Accessed 1 June 2017]. Available from: https://www.securityartwork.es/2014/02/07/fundamentos-sobre-certificados-digitales-declaracion-de-practicas-de-certificacion/
10. DÍAZ ORUETA, GABRIEL, 2014, *Procesos y herramientas para la seguridad de redes.* 1. Madrid: CASTRO GIL Manuel Alonso, DÍAZ ORUETA Gabriel, ALZÓRRIZ ARMENDÁRIZ Ignacio, SANCRISTÓBAL RUIZ Elio.
11. FIRTMAN, SEBASTÍAN J, 2005, *Seguridad informática*. 1. Buenos Aires: MP Ediciones.
12. FLÓREZ, GERMÁN DARÍO, 2014, *La validez jurídica de los documentos electrónicos en Colombia a partir de sus evolución legislativa y jurisprudencial*. Verba Iuris [online]. 2014. P. 45-46. [Accessed 15 July 2017]. Available from: http://www.unilibre.edu.co/verbaiuris/31/la-validez-juridica-de-los-documentos-electronicos-en-colombia-a-partir-de-su-evolucion-legislativa-y-jurisprudencial.pdf
13. GARCÍA MÁS, FRANCISCO JAVIER and ARREDONDO GALVÁN, FRANCISCO XAVIER, 2015, *El documento electrónico. Un reto a la seguridad jurídica.* 1. Madrid: Dykinson.
14. GÓMEZ VIEITES, ÁLVARO, 2011, *Enciclopedia de la seguridad informática*. 2. Madrid: Ra-Ma.
15. GONZÁLEZ MANZANO, LORENA and FUENTES GARCÍA-ROMERO DE TEJADA, JOSÉ MARÍA DE, 2014, *Sistemas seguros de acceso y transmisión de datos. 1. Antequera,* Málaga: IC Editorial.
16. GUTIÉRREZ, JAIME and TENA, JUAN, 2003, *Protocolos criptográficos y seguridad en redes.* 1. Santander: Servicio de Publicaciones de la Universidad de Cantabria.
17. HERRERA PÉREZ, ENRIQUE, 2005, *Tecnologías y redes de transmisión de datos*. México: Limusa.

18. HUIDOBRO MOYA, JOSE M, BLANCO SOLSONA, ANTONIO and JORDAN CALERO, J, 2006, *Redes de área local [recurso electrónico]*. 2. México: International Cengage Editores Spain Paraninfo, S.A.
19. Introducción a los certificados digitales, [no date]. Certificados Digitales [online]
20. JIJENA LEIVA, RENATO JAVIER, PALAZZI, PABLO ANDRÉS and TÉLLEZ VALDÉS, JULIO, 2003, *El derecho y la sociedad de la información. México, D.F.: Miguel Ángel Porrúa.*
21. Legislación informática en Colombia, 2012. *legislación informática en Colombia - JUAN GUILLERMO DURAN NOBLE(grupo 02)* [online]
22. *LEY 527 DE 1999*, 1999. , DIARIO OFICIAL 43.673.
23. Ley Modelo de la CNUDMI sobre Firmas Electrónicas con la Guía para su incorporación al derecho interno 2001, 2002. , 1. Nueva York: Naciones Unidas.
24. MAZA GAZMURI, IÑIGO DE LA, 2002, *Derecho y tecnologías de la información. 1. Chile*: Fundación Fernando Fueyo Laneri.
25. ORTIZ, RIERA, PAEZ MORENO, ANY and EMIRO, ANGEL, 2017, 10. *Innovación, burocracia y gobierno electrónico en la administración pública. HOLOGRAMTICA* [online]. 2017. Vol. 2, p. 25-42. ISSN: 1668-5024.Available from: http://www.cienciared.com.ar/ra/usr/3/895/hologramatica_n12vol2pp25_42.pdf
26. QUINTERO PEÑA, JUAN GABRIEL, 2006, *Firma digital basada en redes*. *Revista Científica, 2006-08-00 nro: 8* [online]. 2006. [Accessed 17 April 2016]. Available from: https://revistas.udistrital.edu.co/ojs/index.php/revcie/article/view/336/499
27. RAMOS ÁLVAREZ, BENJAMÍN and RIBAGORDA GARNACHO, ARTURO, 2004, *Avances en criptología y seguridad de la información*. Madrid: Ediciones Díaz de Santos.
28. RAMOS ÁLVAREZ, BENJAMÍN, RIBAGORDA GARNACHO, ARTURO and HERNÁNDEZ CASTRO, JULIO C, 2004, *Avances en criptología y seguridad de la información*. Madrid: Díaz de Santos.
29. RINCÓN CÁRDENAS, ERICK and VERGARA, CAMILO, 2017, *Administración pública electrónica: hacia el procedimiento administrativo electrónico*. 1. Bogotá: Editorial Universidad del Rosario.
30. RINCÓN CÁRDENAS, ERICK, 2006, *Manual de derecho de comercio electrónico y de Internet*. Bogotá: Centro Ed. Rosarista.
31. Rojas López, Miguel David, Suarez Botero, Diana Marcela, Meneses Durango, Cleidy Nataly, *Firma digital: instrumento de transmisión de información a entidades financieras.* Revista Avances en Sistemas e Informática [en línea] 2011, 8 (Marzo): [Fecha de consulta: 3 de mayo de 2017] Disponible en:<http://www.redalyc.org/articulo.oa?id=133117278002> ISSN 1657-7663
32. SAN MARTÍN GONZÁLEZ, ENRIQUE, 2014, *Salvaguarda y seguridad de los datos*. Antequera, Málaga: IC Editorial.
33. SARUBI, PABLO, 2008, *Seguridad informática – Técnicas de defensa comunes bajo variantes del sistema operativo Unix* [online]. BUENOS AIRES. [Accessed, 1 May, 2017]. Available from: https://es.scribd.com/document/7103092/Seguridad-Informatica-Tecnicas-de-defensa-comunes-bajo-variantes-del-sistema-operativo-Unix
34. *SEGURIDAD DE LA INFORMACIÓN*, 2014. [online], 1. GUATEMALA: Segunda Cohorte del Doctorado en Seguridad.
35. SSL Certificate | *what is an SSL certificate?* - DigiCert.com, [no date]. DigiCert[online]
36. STALLINGS, WILLIAM, 2004, *Fundamentos De Seguridad En Redes*. 2. Madrid: Pearson Educación de México, SA de CV.
37. TORRE ALVAREZ, HERNAN, 2005, *El Sistema de Seguridad Jurídica en el comercio electrónico* [online]. 1. PERU. [Accessed 16 December 2016]. Available from: https://books.google.com.co/books?id=lXnlrIO09yUC&pg=PA115&dq=seguridad+de+las+firmas+digitales+revistas&hl=es-

419&sa=X&ved=0ahUKEwjFwpD4ueXaAhVQzFMKHSdOBaMQ6AEIPTAF#v=onepage&q=seguridad%2
38. TORRES ÁLVAREZ, HERNÁN, 2005, *El sistema de seguridad jurídica en el comercio electrónico*. 1. Lima: Pontificia Universidad Católica del Perú - Fondo Ed.
39. VEGA LOZADA, FREDERICK, 2012, Puerto Rico*: Comentarios a la Ley de Firmas digitales de... Portal de e-governo, inclusão digital e sociedade do conhecimento* [online]. 2012. [Accessed 21 May 2017]. Available from: http://www.egov.ufsc.br/portal/conteudo/comentarios-la-ley-de-firmas-digitales-de-puerto-rico
40. ZAMBRANO CETINO, FREDY ALEXANDER, *Elementos legales de validez jurídica de los actos administrativos emitidos a través de medios electrónicos de acuerdo a la ley 1437 de 2011* [online]. 1. CRAIUsta. [Accessed 2 March 2017]. Available from: http://repository.usta.edu.co/handle/11634/572

CIBERSEGURIDAD Y DATOS PERSONALES: UNA POLÍTICA PRIORITARIA DEL ESTADO RECOLECTOR.

Por: ***Silvia S. Toscano, Ma.Eugenia Lo Giudice y Luciano Galmarini.*** *Argentina*

Introducción

La pregunta inicial con la que abrimos la ponencia es: ¿Cuál es el nivel de preocupación que tenemos los ciberusuarios respecto de la protección de nuestros datos personales en Internet? Muy probablemente, para gran parte de la sociedad y muchos de los llamados "nativos digitales", su nivel sería prácticamente bajo o nulo.

Es claro que, desde el surgimiento de la convergencia tecnológica y la tecnología 4G, cualquier persona se conecta a la red desde su teléfono celular. Es más, un porcentaje alto de la población mundial ha nacido y se ha formado a través de un lenguaje digital y/o electrónico que abarca desde los videojuegos, la Xbox o la Play, el iPod y iPad, las plataformas de *streaming* como Netflix o Spotify, las redes sociales como Instagram, Twitter y Facebook, o apps como Snapchat y WhatsApp, para mencionar sólo algunos de los usos más habituales.

Pero, ¿cuántos miembros de esa gran masa se han detenido a pensar qué ocurre con toda la información que los teléfonos celulares almacenan respecto de nuestros datos personales en las distintas aplicaciones que descargamos y usamos?

Es indudable que el avance de las nuevas tecnologías contribuyó a un más fácil y accesible acceso a la información, pero también trajo aparejadas nuevas complejidades y peligros para la seguridad de los datos personales.

Los delitos informáticos alcanzaron los diversos ámbitos de la web, desde las redes sociales hasta los *malware* diseñados para atacar los sistemas operativos de los teléfonos celulares del tipo Android, llegando hasta los más recientes casos de ciberterrorismo y ciberespionaje.

Ante este panorama, y las cada vez más novedosas y sofisticadas modalidades de los ciberdelitos, uno de los ejes centrales para contrarrestar estas amenazas cibernéticas lo constituye la ciberseguridad.
Debemos plantearnos en el actual contexto donde se habla de inteligencias y amenazas, y no de vulnerabilidades, a qué se llama "ciberseguridad" y "ciberterrorismo".

"Ciberseguridad", hace referencia a las técnicas que se utilizan con el objetivo de resguardar la integridad, confidencialidad y disponibilidad de datos, redes, sistemas y aplicaciones. Los actores involucrados se dan tanto en el sector privado como en el público. En el ámbito público, es función del Estado poner a seguro las TIC sin menoscabar la participación de la sociedad civil y de las empresas del sector.

En cuanto a "Ciberterrorismo", se incorpora al clásico concepto de "terrorismo" la ejecución mediante las TICs teniendo como efecto sembrar el terror por bandas criminales y siendo sus objetivos múltiples: desde dañar reputaciones (de organizaciones, países, etc.) a destruir capacidades de tipo operacional.

Es decir, que van desde atacar la privacidad de una persona, que si está en el ámbito público dará mayor exposición y repercusión, hasta atacar bancos de datos de estructuras capaces de paralizar un sistema de producción comercial o boicotear eventos de índole política. Valga el ejemplo del *hackeo* a los Juegos Olímpicos de Pieonchang 2018, oficialmente conocidos como los XXIII

Juegos Olímpicos de Invierno, donde hubo infección del sistema a través de un malware que logró inutilizar el sitio oficial y el *WiFi* del estadio creando una gran caos.

Ciberseguridad como política pública

Los avances tecnológicos aplicados a la identificación, registro y clasificación de los datos personales pertenecientes a los habitantes de cualquier país han permitido a los Estados el acceso remoto, una mayor capacidad de análisis, reducción de costo, transparencia y agilidad en la gestión pero ha traído aparejados nuevos riesgos que los anteriores sistemas analógicos de registro no presentaban.

Por tal motivo y frente a un Estado cada vez más recolector, urge la necesidad de implementar sistemas de seguridad apropiados siguiendo criterios de uniformidad y en el marco de una política pública con el correspondiente control de los ciudadanos respecto del nivel de protección que sus datos merecen.

Asimismo, deben impulsarse políticas de ciberseguridad que sean acordes con los criterios de transparencia propios de la nueva gestión pública y que involucren a todos los actores tanto del sector público como del privado y de otros sectores de la sociedad civil.

Como menciona la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la Organización de los Estados Americanos(OEA),[1] ¨…la respuesta de los Estados en materia de seguridad en el ciberespacio debe ser limitada y proporcionada y procurar cumplir con fines legales precisos que no comprometan las virtudes democráticas que caracterizan a la red.¨

En reiteradas oportunidades tanto la Relatoría como la Corte Interamericana de Derechos Humanos en su jurisprudencia han manifestado que ¨…las políticas públicas en materia de ciberseguridad deben ser proporcionales al riesgo que enfrentan y, en cualquier caso, deben sopesar el objetivo de seguridad y la protección de los derechos fundamentales¨.

En concordancia con estos principios, un conjunto de organizaciones de la sociedad civil de América Latina suscribieron una declaración tendiente a articular las políticas de seguridad digital con una perspectiva más afín con los derechos humanos y otras libertades[2].

Entre las recomendaciones, se detallan aquellas relativas a la necesidad de alinear cualquier estrategia de ciberseguridad con las normativas de derechos humanos tanto a nivel regional como a los estándares internacionales. Asimismo y a los efectos de eficacia, debe asegurarse el uso de herramientas que cumplan con estándares reconocidos de seguridad digital.

Para la formulación de políticas públicas eficientes, los Estados deben tener presente que cualquier medida de seguridad cibernética puede impactar en el ejercicio de libertades individuales. Por otra parte, deben procurar garantizar la mayor protección de la información y de servicios críticos salvaguardando los mismos de ataques cibernéticos. Un interesante análisis a considerar es el Informe de ¨Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? elaborado en 2016 por el Observatorio de la Ciberseguridad en América Latina y el Caribe mediante una colaboración entre el Banco Interamericano de Desarrollo (BID), la Organización de los Estados Americanos (OEA) y el Centro Global de Capacitación de Seguridad Cibernética (GCSCC) de la Universidad de Oxford[3].

[1] OEA, CIDH Libertad de Expresión e Internet.31 de diciembre de 2013.
www.oas.org/es/cidh/expresion/docs/informes/2014.04.08.internet.web.pdf
[2] ADC Digital ¨OEA Declaración de sociedad civil latinoamericana sobre seguridad digital ¨ Abril 2016
https/adcdigital.org.ar/2016/04/06/OEA-declaración-sociedad-civil-latinoamericana-seguridad-digital
[3] Informe ¨ Ciberseguridad 2016; Estamos preparados en América Latina y el Caribe¨ BID-OEA
https://publications.iadb.org/handle/11319/7449

El informe presenta una imagen completa y actualizada sobre el estado de la ciberseguridad en dichos países. En el mismo, se incluyen análisis de expertos en el tema como así también, se examina la "madurez cibernética" de cada uno de los países mediante la aplicación del Modelo de Madurez de Capacidad de Seguridad Cibernética (CMM) Este índice evalúa mediante cinco variables la capacidad de seguridad cibernética para permitir el crecimiento sostenible a la vez que busca el equilibrio con las libertades individuales y sus derechos conexos.

Algunos de los resultados indican que pocos son los países de la región que han establecido políticas de ciberseguridad aunque todos son contestes en la necesidad de su implementación para asegurar un entorno digital y cibernético que resulta necesario para el desarrollo económico. Dado que el ciberespacio es el escenario vigente para la vida de los negocios y de la sociedad, resulta imprescindible informar y fomentar la confianza de los individuos.

Finalmente, se insta a que los países adopten respuestas eficientes y proactivas frente a las amenazas cibernéticas. La ciberseguridad debe ser considerada un tema prioritario ¨…para fortalecer las capacidades de nuestros países para proteger las personas, las economías, y la infraestructura crítica de nuestra región¨[4].

Tal es la importancia de la ciberseguridad que entre los organismos internacionales y diferentes ONG's, se plantean seriamente los procedimientos para reforzarla. En el encuentro organizado por la OEA, durante la II Conferencia Internacional sobre Seguridad Digital en Perú, junio 2018, se dijo que "La ciberseguridad debe proteger infraestructuras críticas pero también garantizar otros aspectos transversales como los datos personales, que tendrán un papel destacado en la Región"[5].

A continuación, haremos una breve referencia a los antecedentes internacionales, regionales y nacionales en materia de normas uniformes respecto de la ciberseguridad.

Antecedentes internacionales y nacionales

Directiva (UE) 2016/1148

En Julio de 2016, el Parlamento Europeo y el Consejo de Europa adoptaron la Directiva (UE) 2016/1148, relativa a las Medidas Destinadas a Garantizar un Elevado Nivel Común de Seguridad de las Redes y Sistemas de Información en la Unión.

En sus distintos considerandos, se pone de manifiesto la importancia del papel fundamental que tienen en la actualidad las redes y sistemas de información en la actividad social y económica de los países. Por ello, se destaca que su fiabilidad y seguridad son elementos esenciales para garantizar dichas actividades en el mundo virtual.

También se resalta el incremento de nuevos incidentes de seguridad que pueden poner en peligro la actividad en la red, ocasionando no solo pérdidas económicas, sino dañando gravemente la confianza de los ciberusuarios, dada la característica de transnacionalidad que es propia de la red de Internet, pudiendo afectar a diferentes países al mismo tiempo.

La Directiva (UE) 2016/1148 es consecuencia de un largo proceso tendiente a la armonización de los distintos ordenamientos jurídicos internos de los Estados miembros, mediante la adopción de una solución uniforme.

[4] Idem informe BID-OEA citado
[5] https://twitter.com/OEA_Cyber/status/1004086444699287554

El objetivo de la Directiva es elaborar una estrategia nacional de seguridad de las redes y sistemas de información en el que se establezcan los objetivos estratégicos y las medidas políticas y normativas adecuadas para mantener un elevado nivel de seguridad. Entre estas medidas, se encuentra la red CSIRT, red de equipos de respuesta a incidentes de seguridad informática a escala nacional, difundir alertar tempranas, avisos e información sobre riesgos e incidentes entre los interesados.

Para ello es necesario que no sólo los Estados se involucren, sino que los proveedores de servicios esenciales de Internet cumplan con determinados requisitos de seguridad informática, como el alerta de incidentes.

También se pone de resalto que las capacidades existentes en la mayoría de los países, no son suficiente para garantizar un elevado nivel de seguridad en la red, lo que ocasiona niveles de protección desigual.

A fin de alcanzar y mantener un nivel elevado de seguridad en la red y sistemas de información, la Directiva postula que los Estados deben disponer de una estrategia nacional de seguridad que fije los objetivos estratégicos y las medidas concretas a aplicar por la autoridad nacional competente responsable de ejercer las funciones vinculadas a la seguridad de las redes y sistemas de información de los operadores de servicios esenciales y los proveedores de servicios digitales.

Para ello, es importante que cada país designe un "punto de contacto único nacional" que se encargue de facilitar la coordinación de las cuestiones de seguridad de las redes y sistemas de información y la comunicación transfronteriza, que cuenten con recursos técnicos, financieros y humanos adecuados para garantizar de manera efectiva y eficiente las funciones que se le atribuyan.

Asimismo, cada país debe contar con una "CSIRT" (Computer Security Incident Response Team), un Equipo de Respuesta a Incidentes de Seguridad Informática, el cual será el encargado de recibir las distintas notificaciones de los diversos incidentes que efectúen los prestadores de servicios de internet, y transmitírselas a los "puntos de contacto únicos" para que éstos a su vez se lo comuniquen a los "puntos de contacto único" de los demás países de la Unión.

A su vez, estos "puntos de contacto único" deben presentar un informe resumido de los distintos incidentes, bajo técnicas de disociación de datos que protejan la confidencialidad de los notificadores (proveedores de internet y de servicios digitales), que contenga: el número de notificaciones recibidas, las características de los incidentes reportados, los tipos de vulnerabilidad de la seguridad, su gravedad y duración.

La cooperación entre los ámbitos público y privado, resulta esencial, ya que la mayor parte de las redes y sistemas de información son de gestión privada. De esta manera, los países podrán adoptar medidas de prevención, detección, respuesta y contingencia de los incidentes y riesgos de la red.

Para esto se requiere que los prestadores de servicios esenciales de Internet se comprometan en una gestión de riesgos responsable que implique una evaluación del riesgo y la aplicación de medidas de seguridad que respeten requisitos normativos adecuados.

También se destaca que la información sobre incidentes de seguridad, tiene cada vez mayor utilidad para la población como para las empresas. En tal sentido se encomienda a las CSIRT a informar en su sitio web cuales son los principales incidentes en materia de seguridad, que afecten a las redes y sistemas de información acaecidos en la Unión Europea.

Por último, se pone de manifiesto que el alcance mundial de los problemas que afectan a la seguridad de las redes y sistemas de información hace necesaria una mayor cooperación

internacional para mejorar las normas de seguridad y el intercambio de información, y promover un planteamiento global común con respecto a las cuestiones de seguridad.

A nivel latinoamericano, la Organización de los Estados Americanos (OEA) aconseja a sus países miembros que adopten programas de seguridad cibernética. Para ello instrumentan los consejos pertinentes desde el Programa de Ciberseguridad de su Comité Interamericano contra el Terrorismo (CICTE).

Día a día, se suman los países que en el entendimiento de la necesidad de cooperación han implementado o están implementado las estrategias pertinentes.

En esta línea de ideas, en Argentina y más allá de la creación en el ámbito del Ministerio de la Modernización del Comité de Ciberseguridad (Decreto 577/2017) con el apoyo del Comité Interamericano contra el Terrorismo de la OEA, se trabaja en una estrategia nacional.

BA-CSIRT y Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad.

Como antecedentes de la presente propuesta, puede mencionarse en primer lugar el BA-CSIRT, el cual constituye el primer Centro de Ciberseguridad de la ciudad de Buenos Aires, cuya finalidad es asistir y concientizar a los ciudadanos y al Gobierno de la Ciudad de Buenos Aires en todo lo relacionado a la seguridad de la información, mediante servicios de prevención y educación en aspectos que involucren las TIC[6].

Para ello, cuenta con una plataforma electrónica que permite informar y/o capacitar a la ciudadanía, como también solicitar su colaboración ante eventuales incidentes de seguridad relacionados con el uso de la tecnología.

En nuestro país, El BA-CSIRT, constituye el primer Centro de Ciberseguridad de la ciudad de Buenos Aires, cuya finalidad es asistir y concientizar a los ciudadanos y al Gobierno de la Ciudad de Buenos Aires en todo lo relacionado a la seguridad de la información, mediante servicios de prevención y educación en aspectos que involucren las TIC, ofreciendo una plataforma electrónica que permite informarse, capacitarse y solicitar ayuda ante eventuales incidentes de seguridad relacionados con el uso de la tecnología, como vulnerabilidades de software y hardware, códigos y contenidos maliciosos.
Si bien su misión es proteger los servicios de información del Gobierno de la Ciudad, también tiene la encomiable tarea de concientizar a los ciberusuarios respecto del uso seguro de las TIC, mediante la prevención, detección y tratamiento de los incidentes de seguridad, promocionando el conocimiento de la seguridad de la información en la comunidad, desde un centro de respuesta confiable y referente para la comunidad.

Este Centro de Seguridad es el órgano encargado de recibir los eventos e incidentes que ocurran en la red relacionados al uso de las TIC, que impliquen la pérdida, robo, difusión no consentida o daño de cualquier información o dato personal.
Entre las problemáticas más frecuentes en la red, el BA-CSIRT ha identificado:

- *GROOMING:* acoso sexual a niños por parte de adultos a través de medios digitales.
- *PHISHING:* robo de información personal altamente sensible a través del engaño.
- *RANSOMWARE*: secuestro de información ocasionada por la infección de un virus.
- *SEXTORSIÓN:* extorsión al dueño de una imagen y/o video con contenido erótico o sexual.
- *CIBERBULLYING:* hostigamiento entre pares a través de medios electrónicos.
- *ROBO DE IDENTIDAD:* creación de perfiles falsos con información de otra persona.

[6] https://www.ba-csirt.gob.ar/

En esta línea, en el año 2015, el BA-CSIRT firmó un convenio de cooperación con la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), para establecer acciones y programas de cooperación y asistencia técnica para investigar delitos informáticos, que incluyen el establecimiento de canales ágiles para transmitir al Ministerio Público Fiscal la información que el BA-CSIRT estime conducente para llevar adelante las investigaciones judiciales.

Por otra parte, también se acordó la generación de mecanismos para el intercambio de información y la realización de actividades conjuntas con el fin de contar con un canal de información de calidad para desarrollar investigaciones y combatir el delito, a través de la articulación de ambas instituciones con temáticas afines, redundando en un acceso a la justicia por parte de la ciudadanía.

Como segundo antecedente, se destaca el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad en el ámbito de la Dirección Nacional de Infraestructuras Críticas de Información y Ciberseguridad[7], dependiente de la Secretaría de Gabinete de la Jefatura de Gabinete de Ministros.

La misma fue creada con fundamento en que la seguridad de la infraestructura digital se encontraba expuesta a constantes amenazas, con graves incidentes en los sistemas de información y comunicaciones.

Así, la finalidad del Programa es impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y el sector privado que así lo requieran; y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías, entre otras acciones.

Entre sus objetivos se destacan: elaborar y proponer normas destinadas a incrementar los niveles de seguridad en los recursos y sistemas relacionados con las tecnologías informáticas en el ámbito del Sector Público Nacional; colaborar con el sector privado para elaborar en conjunto políticas de resguardo de la seguridad digital; administrar la información sobre reportes de incidentes de seguridad en el Sector Público Nacional que hubieren adherido al Programa y encausar sus posibles soluciones de forma organizada y unificada; establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad; promover la concientización en relación a los riesgos que acarrea el uso de medios digitales en el Sector Público Nacional, las Organizaciones de Gobierno y la ciudadanía.

Ciberseguridad y Seguridad de los Datos Personales

En un contexto de multiconexión y *oversharing* de información navegando en un océano de contenidos en el ciberespacio, se torna necesario adoptar una política de seguridad y protección de los datos personales.

En primer lugar, la casi totalidad de las usuarios de Internet no tienen noción de que al abrir una cuenta o perfil en una red social, tal los casos de Facebook, Instagram, WhatsApp, Twitter, Tinder o Snapchat, celebra un contrato electrónico por el que acepta los términos y condiciones establecidos por el sitio o aplicación, que incluso pueden variar en cualquier tiempo sin aviso previo a sus usuarios. Esta situación puede tornar pública, información que había sido configurada como privada, hasta tanto no ajuste la nueva configuración.

[7] "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" (ICIC), Resolución JGM Nº 580/2011

Por otra parte, los usuarios tampoco conocen al abrir dicha cuenta o perfil, que le están dando una serie de permisos a las mencionadas redes sociales para que dispongan de sus datos, como por ejemplo cederlos a terceros o "partners".

A ello debe sumarse el empleo de las "*cookies*", que permiten la recolección de una gran cantidad de datos que luego son usados para crear un perfil *online* con los gustos, intereses, preferencias y hábitos de consumo de los usuarios, para luego cederlos a terceros para el envío de publicidad no deseada ni solicitada.

También suelen emplearse los "*píxels*" o líneas de código, que identifican a las "*cookies*" con quienes intercambian recíprocamente información. Se suelen usar en los botones del tipo "me gusta" y "compartir" de las redes sociales.

Debe recordarse que la Ley Nº 25.326 de Protección de Datos Personales de Argentina, prevé las condiciones de licitud para el tratamiento de los datos recolectados y tratados por las bases de datos públicas y privadas destinadas a proveer informes. Entre dichas disposiciones, la ley dispone entre una de las obligaciones de los bancos de datos, la de adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad y confidencialidad de los datos.

Respecto a esto, hay dos factores que no se pueden soslayar: el aumento exponencial de dispositivos móviles con tecnología "*I-mode*" de conexión a la red, que permite descargar una gran cantidad de aplicaciones del tipo "*social networking*"; y la posibilidad de conexión a través de redes inalámbricas (*WiFi*) que hacen muy vulnerable la privacidad de los usuarios.

A esto debe agregarse que, en seguridad informática, lo que se conoce como ingeniería social, es la primera causa de robo de datos, de identidad, fraudes, etc.

Si bien es dable reconocer que las redes sociales mencionadas utilizan el sistema de *"Safe Harbor"* (Puerto Seguro), en verdad, sólo se encargan de "hacer lo posible" para mantener a salvo nuestra información. Información de público conocimiento da cuenta de lo que puede hacerse con la información y los perfiles.

Es que justamente se debe distinguir el cambio de paradigma actual, que requiere una transformación digital en la cultura de la sociedad. No podemos dejar de recordar que más allá de lo tecnológico el ataque actualmente está dirigido a la identidad social (generalmente implementad a través de esas redes sociales).

Justamente entre otras, la tarea que tienen las áreas de seguridad es implementar la concientización de los social risks, el monitoreo permanente de servicios de threat intelligence; implementar CSIRT para responder eficientemente ante un ciberincidente.

Es por ello que la labor de un CSIRT a nivel nacional, debería enfocarse en prevenir y proteger los datos personales frente a toda amenaza o ataque tanto interno como externo.

Propuesta

En base a lo expuesto, se propone que Argentina adopte una Estrategia Nacional de Seguridad de las Redes y Sistemas de Información, que proporcione las prioridades y objetivos estratégicos de seguridad, que permita la adopción de las medidas políticas y normativas adecuadas con el objeto de lograr un elevado nivel común de seguridad en la red.

Entre dichas medidas, debería crearse un marco de gobernanza a nivel nacional, que contenga una autoridad de aplicación, que ejerza una función de enlace, para garantizar la cooperación transfronteriza entre las autoridades de los distintos Estados; y una red CSIRT, Equipo de

respuesta a incidentes de seguridad informática, que contribuya al desarrollo de la confianza y seguridad en la red en nuestro país.

También deberían identificarse las medidas de prevención, respuesta y gestión de riesgos, para lo cual es necesario idear un mecanismo de notificación de alertas por parte de los proveedores de servicios esenciales de Internet y prestadores de servicios digitales a la CSIRT, de todo incidente que tenga efectos significativos en la continuidad de los servicios que prestan, que permita identificar el número de usuarios afectados, la duración del incidente y la extensión geográfica del incidente.

La Estrategia también debe establecer requisitos en materia de seguridad y notificación para los proveedores de servicios esenciales de Internet y prestadores de servicios digitales, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilizan en sus operaciones, como para prevenir y reducir al mínimo los efectos de los incidentes que afecten los mismos con el objeto de garantizar su continuidad.

En numerosas ocasiones los datos de carácter personal se ven comprometidos a raíz de incidentes. En este contexto, las autoridades competentes deben cooperar e intercambiar la información sobre todos los asuntos pertinentes ante las violaciones de los datos personales.
Como parte de la Estrategia se debe contemplar la elaboración de Programas de educación, concienciación y capacitación relacionados con la seguridad de las redes y sistemas de información.

Por último, se propone a nivel del Mercosur, la creación de un Grupo de Cooperación para apoyar y facilitar la cooperación estratégica y el intercambio de información entre los Estados miembro, a fin de proporcionar orientación estratégica para las actividades de la red CSIRT, como el intercambio de buenas prácticas referentes a las capacidades y preparación de los distintos países.

Conclusiones

La ciberseguridad ha tomado un rol fundamental en el ámbito privado y público especialmente por el alto costo que genera su ausencia y donde las brechas de seguridad se van haciendo cada vez más cotidianas causando impactos profundos en la sociedad.

La renovación tecnológica en una constante superación lleva a que sea imperativo un programa de respuesta a ciberincidentes como así mismo educar a la ciudadanía cubriendo los ataques desde la ingeniería social con la debida concientización para así gestionar en niveles aceptables los riesgos tecnológicos y ser resilientes en la recuperación y minimización de impactos.

Tal como cita en los considerando el Decreto citado que dio lugar a la creación de la Comisión de Ciberseguridad en el ámbito del Ministerio de la Modernización en la Argentina, el Estado debe implementar los recursos y medidas para "encarar una adecuada protección en materia de Ciberseguridad … tarea compleja que resulta necesaria en la actualidad, debido al incremento exponencial y a la diversidad de las amenazas y ataques informáticos, así como el impacto que los mismos puedan ocasionar en las infraestructuras críticas de un país y su población." Todo lo dicho en un marco de cooperación interregional pues las TIC no conocen de fronteras delimitantes.

América Latina y el Caribe tienen un gran desafío por delante para avanzar en un nuevo escenario que contemple un concepto de ciberseguridad más moderno, más transparente y que se enmarque en la adopción de políticas públicas en la materia que permitan el reconocimiento y el respeto por las libertades individuales especialmente la libertad de expresión y la privacidad tan priorizadas por la Convención Americana de derecho Humanos y sostenida por la Corte Interamericana en su jurisprudencia.

Bibliografía Consultada

Basterra, Marcela, "El Derecho Fundamental de Acceso a Información Pública", Lexis Nexis, Buenos Aires, 2006

Fundación Telefónica, "Ciberseguridad, la protección de la información en un mundo digital", editado por Editorial Ariel S.A. Barcelona, 2016, y Fundación Telefónica, Madrid 2016, España.

Maggiore, Marcia, "Normas internacionales y nacionales vinculadas a la seguridad de la información", André Materson Ediciones, 2009

Palazzi, Pablo A., "Los Delitos Informáticos en el Código Penal", Análisis de la Ley 26.388, Tercera edición actualizada y ampliada, Ciudad Autónoma de Buenos Aires, Abeledo Perrot, 2016

Plaza Penadés, Javier, "Aspectos Básicos de los Derechos Fundamentales y la Protección de Datos de Carácter Personal en Internet", en Derecho y Nuevas Tecnologías de la Información y la Comunicación, coord., por Javier Plaza Penadés, Eduardo Vázquez de Castro, Raquel Guillén Catalán, Fernando Carbajo Cascón, 2013, Thomson Reuters Editorial Aranzadi, Primera Edición 2013

Sitios Web Consultados

https://eur-lex.europa.eu/homepage.html?locale=es Unión Europea
www.un.org/es Organización de las Nacionales Unidas
http://www.oas.org/es/default.asp Organización de los Estados Americanos
https://adcdigital.org.ar/ Asociación por los Derechos Civiles (ADC)
https://publications.iadb.org/facet-view?field=type_view Banco Interamericano de Desarrollo
https://www.ba-csirt.gob.ar/ Centro de Ciberseguridad (BA-CSIRT)

COMERCIO ELECTRÓNICO EN COLOMBIA: DINÁMICAS Y DESAFÍOS

Por: ***Rodrigo Cortés Borrero***
Colombia

Antecedentes del comercio electrónico en Colombia

A. La aparición del comercio electrónico en Colombia

El comercio electrónico no es nuevo. Existe desde hace varios años y ha sido tradicionalmente realizado a través de redes privadas reguladas por códigos o acuerdos de dicha naturaleza en el contexto de EDI. Con anterioridad a la expedición de normas como la ley 527 de 1999, los comerciantes acudían al contrato como la estrategia jurídica para dar validez al uso de la tecnología en los negocios (REMOLINA , 2006, pág. 333)

La aparición del comercio electrónico siguiendo a (O. BURITICÁ Y R. BURITICÁ, 2001) citado por (BECERRA, 2012, págs. 54-55) en Latinoamérica fue totalmente ajena al desarrollo de estas nuevas tecnologías y se posicionó corno importador, realizando las primeras conexiones a comienzos de 1990, con acceso exclusivo para centros académicos y científicos. Colombia tan solo se conectó en 1994, teniendo grandes dificultades, sobre todo, por la baja capacidad de las redes de telecomunicaciones y de los computadores para esa época. Esto sumado al monopolio de las empresas telefónicas en las llamadas a larga distancia.

Empero, el ingreso de grandes multinacionales como AT&T y Global One, en cierta forma impulsó la introducción de nuevas tecnologías en las telecomunicaciones de Colombia, como la fibra óptica, las redes inalámbricas, las redes privadas para transmisión de datos, entre otras; que mejoraron de manera significante el acceso al Internet, el cubrimiento telefónico y la evolución del comercio electrónico. En el año 2000, el cubrimiento telefónico era del 80 por ciento en las zonas urbanas y del 20 por ciento en las zonas rurales del país.

Las transacciones virtuales se inician en Colombia desde finales de los años noventa, y los pioneros en esa materia aparecieron entre 1998 y 1999, como lo fueron algunos portales horizontales latinoamericanos, masificando, pero a la vez saturando el mercado del comercio electrónico colombiano.

En 1999, en el campo mundial, debido a la incertidumbre y desconfianza de diversos inversionistas, se disminuyó dramáticamente la cotización de las acciones de compañías de comercio electrónico. En Colombia, la idea de colocar las acciones de estas compañías en la Bolsa apenas se contemplaba cuando se desató la crisis, como lo afirman BURITICÁ et al. (2001): "en nuestro país la «fiebre de la red» fue tardía" Posteriormente, los inversionistas en la industria del e-commerce decidieron planificar mejor sus compañías para así evitar correr mayores riesgos. Ingresaron a Colombia la tecnología del WAP (Wireless Access Protocol), agendas digitales (PDA) y los computadores portátiles, facilitando no solo la venta de productos, sino también la prestación de servicios como la banca en línea.

Frente a esa realidad el legislador no podía quedarse atrás y erige hace algunos años con una norma de comercio electrónico, la ley 527 de 1999, en la cual se regulan aspectos como el principio equivalente funcional, el valor probatorio de los mensajes de datos, la firma electrónica y la firma digital, entre otros. Sin embargo, se trata más de una norma de carácter procesal que de carácter sustancial (VILLALBA, 2012)

Esta ley se basó en la normativa modelo de comercio electrónico, aprobada en 1996 por la Comisión de las Naciones para el Desarrollo del Derecho Mercantil Internacional (CNUDMI) sobre comercio electrónico, obedeció a la necesidad de contar con un régimen jurídico acorde con

la evolución de las comunicaciones, de sus elementos técnicos y del comercio. Además, como novedad, la ley agregó dos capítulos: Uno sobre relación que existe entre los documentos de transporte y los medios electrónicos, y otro capítulo sobre entidades certificadoras y su control por la Superintendencia de Industria y Comercio. (MEDINA, 2013)

Con la ley 527 de 1999, Colombia se adapta a las modernas tendencias del derecho internacional privado, una de cuyas principales expresiones ha sido la adopción de legislaciones que llenen vacíos normativos para facilitar y regular el uso de los medios de comunicación modernos. (MEDINA, 2013)

Esto como respuesta a un fenómeno económico y social como lo describe PEÑA (2013) el comercio electrónico ha venido creciendo en importancia en los mercados desarrollados y de manera paulatina también en los mercados emergentes, incluyendo Latinoamérica. Las razones por las cuales han venido despertando· nuestra economía a una realidad incontrovertible proviene de varios factores: la mayor eficiencia, las menores barreras de entrada al entorno internacional y el impulso que el uso de medios electrónicos trae consigo para el desarrollo económico que conlleva la consolidación de los mercados digitales. (pág. 469)

B. Desarrollo normativo colombiano del comercio electrónico

Solo hasta principios de la década del noventa, Colombia comenzó la regulación de las actividades del comercio electrónico. El pionero en imponer esta clase de regulaciones fue el sistema financiero. De esta manera, el Estatuto Orgánico Financiero proferido por el gobierno en 1993 a través del Decreto 663, incluyó la posibilidad del uso de sistemas e intercambios electrónicos. Dos años más tarde, en 1995, se expidió la Ley 222 por la cual se modificaron ciertas disposiciones del Código de Comercio colombiano.

Posteriormente, se llegó específicamente al sector público mediante el decreto 2150 de 1995, en su artículo 25, se permitió el envío de información a las entidades públicas por correo electrónico y en su artículo 26 se impuso la obligación a las entidades públicas de habilitar sistemas de transmisión electrónica para que los usuarios puedan recibir o solicitar información.

Ese mismo año, con la aparición de la factura electrónica en las transacciones, surgió la necesidad de regularla, por tanto, se promulgó la Ley 223 de 1995 (Ley de la Factura Electrónica) impulsada por la DIAN. Seguidamente en 1996, se expidió el decreto 1094 que regulaba el artículo 616-1 del Estatuto Tributario, cuyo texto muestra como aspecto relevante el otorgamiento de la equivalencia a la factura electrónica con la factura de venta, convirtiéndose así en un antecedente del llamado principio de equivalencia funcional. Lo anterior, estuvo acorde con el concepto de la DIAN 40333 de 2000.

Más tarde, el gobierno de Colombia se encamino en la conformación de una comisión interinstitucional para estudiar la Ley Modelo de Comercio Electrónico y diseñar su adecuación al ordenamiento jurídico, luego de haber participado como observador de la CNUDMI entre 1996 y 1998. Esto dio origen al proyecto de ley 227 de 1999, que finalmente se concretó en la ley 527 de 1999, conocida como la "Ley de Comercio Electrónico". Esta ley se fundamentó en la Ley Modelo de Comercio Electrónico de la CNUDMI, lo cual puede observarse en sus dos primeras partes, ya que incluyen en su totalidad el texto de la Ley Modelo.

En palabras de CÁRDENAS, (2009)**:**

> "*con la expedición de la Ley 527 de 1999, conocida como la Ley de comercio electrónico, se acogieron los principios de las leyes modelo de UNCITRAL* (CNUDMI). *Esta ley*

> *constituye el marco jurídico que legitima el uso de mensajes de datos en todas las actividades del sector público y privado."* (pág. 86).

La ley 527 de 1999 se convirtió en la más completa en materia de comercio electrónico en el país, puesto que se transformó en el eje fundamental de las negociaciones electrónicas. Además de incluir el principio de equivalencia funcional, el de neutralidad tecnológica, autonomía de las partes, entre muchos otros, también consagraba la aparición de nuevas instituciones hasta ese tiempo desconocidas para el derecho, como las entidades de certificación, los certificados y firmas digitales.

Otro aspecto importante que estudio la Ley 527 de 1999 fue la manera de cómo se estudiaba la formación de contratos contenidos en el Código de Comercio, puesto que ya las disposiciones del estatuto mercantil no serán aplicables a todas las transacciones de derecho privado, especialmente las de tipo electrónico. De esta forma, los interrogantes que habían surgido respecto al perfeccionamiento y formación de la contratación electrónica en sí, se resolvieron equiparando la oferta a través de medios electrónicos con la establecida en el artículo 850 del Código de Comercio, que es la oferta verbal o por vía telefónica; así la oferta en la contratación electrónica quedaba como la propuesta verbal entre presentes.

Posterior a la expedición de la ley 527 de 1999, la producción legislativa en torno al tema del comercio electrónico se expandió considerablemente. Tal es el caso de la resolución 26930 de la Superintendencia de Industria y Comercio del 26 de octubre de 2000, por medio de la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores en Colombia. Además, el decreto 1747 de 2000, por el cual se reglamenta parcialmente la ley 527 de 1999 en materia de entidades de certificación, certificados y firmas digitales. Este decreto otorga los derechos y deberes de los servicios de certificación (VALENZUELA, & CASTRO, 2002) citado por (BECERRA, 2012, págs. 59,60)

En este orden de ideas, la ley 527 de 1999 fue el verdadero primer paso de un masivo proceso por regular la actividad electrónica en Colombia. No obstante, a la sombra también se iba desarrollando un importante respaldo jurisprudencial con la declaratoria de constitucionalidad de la mencionada ley 527, mediante la sentencia C- 662 (2000). La Corte se pronunció al respecto y tomo una posición categórica al establecer que la ley 527 de 1999 cumplía con todos los requisitos para obtener su constitucionalidad y que los principios de la validez de la prueba y las entidades de certificación no constituían ninguna distorsión de la función notarial y el orden público. (2000)

También en el ámbito del derecho procesal se observaron algunos avances legislativos, siendo el principal la ley 98 de 1999, también denominada la ley del libro, que ampliaba la interpretación del artículo 251 del Código de Procedimiento Civil, cuyo texto consagraba el concepto de documento como: "todo objeto mueble que tenga carácter representativo o declarativo y las inscripciones en lápidas, monumentos, edificios o similares". A partir de esta concepción, se empezó a considerar como libros, revistas o folletos, los impresos hechos dentro o fuera de la República de Colombia, en papel o por medios electrónicos. Esta interpretación del artículo 251 y la ley 98 de 1999 permitieron otorgarle validez probatoria al ahora llamado documento electrónico, situación que era muy difícil anteriormente debido a la excesiva formalidad del derecho colombiano. Esto, además, se complementó con el artículo 95 de la Ley Estatutaria de Administración de Justicia.

En el transcurso del año 2000, se expidió la directiva presidencial 2, donde se estableció la estrategia de *Gobierno en línea*, por medio de la cual el gobierno nacional pretendía enlazar e intercambiar información con el mayor número de entidades públicas posibles en el territorio nacional y, a la vez, facilitar mayor acceso a los ciudadanos, empresas, funcionarios y otras entidades públicas acerca de las actividades de la administración pública. (2000)

Tabla N° 1. Normativa colombiana en materia de contratación electrónica

NORMATIVA	ASUNTO
Ley 962 de 2005 "Antitrámites"	Utilización de medios electrónicos en las actuaciones administrativas.
Ley 1150 de 2007 y decreto 2474 de 2008	Transacciones electrónicas en contratación pública.
Decreto 1151 de 2008	Implementación de la estrategia *Gobierno en línea*.
Ley 1266 de 2008 "Habeas Data"	Manejo de información confidencial en bancos de datos electrónicos.
Ley 1273 de 2009	Se eleva a categoría de delito las conductas que atenten contra la protección de datos en la tecnología de la información y las comunicaciones.
Ley 1286 de 2099	Fortalecimiento del desarrollo tecnológico y de la innovación.
Documento Conpes 3620 de 2009	Lineamientos para el desarrollo e impulso del comercio electrónico en Colombia.
Ley 1341 de 2009	Principios y conceptos sobre la sociedad de la información y organización de las TIC.

NOTA: Descripción de la normatividad en Contratación electrónica, adaptado de (BECERRA RODRIGUEZ, 2012 pág. 62),

El desarrollo normativo del comercio electrónico ha hecho posible la transformación de teorías ya establecidas en el derecho privado colombiano. Un reflejo de ello es el surgimiento de un nuevo término: *el establecimiento comercial virtual.* Dicho término se basa en que, también, a través de las páginas web se llevan los fines y objetivos de la empresa, contenidas estas mismas por sinnúmero de conjuntos de bienes. Este concepto parece tener su iniciación en la Ley 633 de 2000 por la cual "*se expiden normas en materia tributaria, se dictan disposiciones sobre el tratamiento a los fondos obligatorios para la vivienda de interés social y se introducen normas para fortalecer las finanzas de la Rama Judicial*", cuyo artículo 91 señala que: "(...)todas las páginas web y sitios de Internet de origen colombiano que operan en la Internet y cuya actividad económica sea de carácter comercial, financiera o de prestación de servicios, deberán inscribirse en el registro mercantil y suministrar a la DIAN la información de transacciones económicas en los términos que la entidad lo requiera" (Ley 633 , 2000, pág. 36).

C. Estado actual y desafíos del comercio electrónico en Colombia

Las innovaciones tecnológicas han permitido el surgimiento de nuevas modalidades de transacciones electrónicas. Una muestra de ello ha sido el avance en grandes sectores comerciales como el bancario y el de la telefonía móvil, en su fusión manifestada en el servicio llamado banca móvil, por medio del cual se realizan notificaciones y se envían alertas de otras transacciones en diversos canales, garantizando mayor seguridad a los usuarios del sistema financiero.

El constante crecimiento del comercio electrónico ha permitido el avance en distintos ámbitos, pero en otros no ha existido mayor impacto. El segundo es el caso de las Mipymes, en las cuales no se evidencia un uso de Internet y nuevas tecnologías en su actividad comercial debido, principalmente, a la poca información y capacitación sobre el manejo de las nuevas tecnologías.

Por otro lado, en la parte oscura del comercio electrónico, encontramos los delitos informáticos los cuales se presentan como una gran barrera para el desarrollo del comercio electrónico en

Colombia, tal como sucede en el comercio mundial. Esto se debe a la gran vulneración de la información confidencial que existe en Colombia sobre la entidad financiera o el cliente, lo cual deja a merced que *hackers* cometan delitos de lavado de activos, hurtos y extorsiones.

Definición de Comercio electrónico

El artículo 2, inciso b) de la Ley 527 de 1999, consagra que el comercio electrónico:

> "*abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera*" (1999)

Esta ley define al comercio electrónico como aquel que abarca toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Así mismo, la sentencia C-1147 de 2001 reitera en su pronunciamiento la definición antes dada por la ley 527 de 1999 (2001). Por otra parte, Ernesto RENGIFO GARCÍA define comercio electrónico, como:

> *...el intercambio de información entre personas que da lugar a una relación comercial, consistente en la entrega en línea de bienes intangibles o en un pedido electrónico de bienes tangibles. Este intercambio de datos puede ser "multimedial" o consistir en imágenes, textos y sonidos*. (GÓMEZ, 2004, pág. 18).

El concepto de comercio electrónico es conocido también como e-commerce, donde: "La "e" que precede toda terminología en la Red, hace alusión al término electrónico en inglés. De ahí que la anteposición a la palabra comercio venga a designar la modalidad de éste que se efectúa mediante Internet". Al término comercio electrónico, conocido como e-commerce en inglés, se le puede diferenciar de otro concepto conocido como e-business, donde éste último presenta un significado más amplio porque abarca las operaciones de e-commerce y toda la organización del negocio en general, donde estaría todo lo relacionado con la aplicación de las nuevas tecnologías informáticas. (MERAZ, 2006, pág. 28)

En otras palabras, el comercio electrónico (*e-commerce*) se refiere a todas las transacciones comerciales realizadas o basadas en sistemas electrónicos de procesamiento y transmisión de información, especialmente EDI (*Electronic Data Interchange*) e Internet *(Interconnected networks)* (REMOLINA, 2006, pág. 331)**.** El Autor David KOSIUR aproximándose a una definición más rica en cuanto a variantes nos expone el siguiente concepto:

> "Comercio Electrónico es un sistema que incluye no sólo aquellas transacciones que se centran en la compra y venta de bienes y servicios para generar ingresos, sino también aquellas transacciones que respaldan la generación de los ingresos, tales como la creación de la demanda para esos bienes y servicios, ofreciendo respaldo a las ventas y el servicio al cliente, o facilitando la comunicación entre socios de negocios". (GÓMEZ, 2004, pág. 18)

Puede también analizarse el concepto desde distintas perceptivas. Para MERAZ (2006) existen cuatro tipos de perspectivas para definir el comercio electrónico:

> - *Desde una perspectiva de las comunicaciones: "es la entrega de información, producto/servicios o pagos por medio de líneas telefónicas, redes de ordenadores o cualquier otro medio electrónico"*
> - *Cómo proceso de negocios: "es la aplicación de la tecnología a la automatización de procesos de negocios y flujo de trabajo"*
> -*Desde el punto de vista del servicio: "es una metodología de negocios que permite satisfacer a los proveedores y clientes, ahorrando costes, aumentando la calidad de los productos y la rapidez de su entrega"*
> - *Desde su perspectiva online, "es la capacidad para comprar y vender productos/servicios e información a través de Internet u otras redes que se encuentran interconectadas*. (págs. 27,28)

La Comisión de la Unión Europea en la comunicación COM. 97.157 denominada *"Una iniciativa europea en materia de comercio electrónico",* lo ha definido corno:

> "El desarrollo de actividad comercial y de transacción por vía electrónica y comprende actividades diversas: la comercialización de bienes y servicios por la vía electrónica; la distribución *online* de contenido digital, la realización por vía electrónica de operaciones financieras y de bolsa; la obra pública por vía electrónica y todo procedimiento de ese tipo celebrado por la administración pública" (PLAZAS, 2012, pág. 6).

Por su parte la OMC Define, en términos generales, al comercio electrónico como "*la producción, publicidad, venta y distribución de productos a través de las redes de telecomunicaciones*". (Organizacion Mundial del Comercio (OMC), s.f.). En un sentido más amplio, es un sistema global que utilizando redes informáticas y en particular Internet permite crear un mercado electrónico (operado por computadora y a distancia) de todo tipo de productos, servicios, tecnologías, y bienes, e incluye todas las operaciones necesarias para concretar operaciones de compra y venta, matching negociación, información de referencia comercial, intercambio de documentos, acceso a la información de servicios de apoyo (aranceles, seguros, transportes, etc.) y banking de apoyo; todo ello, en condiciones de seguridad y confidencialidad razonables. (PIAGGI, 2001 pág. 69)

El comercio electrónico puede definirse como el conjunto de actividades económico-comerciales ejecutadas por personas comerciantes o no, que se desarrollan mediante la utilización de uno o más mensajes de datos o de cualquier otro medio semejante (MEDINA, 2013, págs. 323,324). Así mismo el Departamento Nacional de Planeación a través del *Conpes resalta la importancia del comercio electrónico en la competitividad, y destaca la necesidad de generar confianza en los usuarios por medio de desarrollos en seguridad, propiedad intelectual y régimen de impuestos.* (PLAZAS, 2012, pág. 12)

Ya que la definición de comercio electrónico abarca toda forma de comercio que se estructure a partir de la utilización de mensajes de datos, dentro de los cuales se incluye de manera no taxativa los datos por Internet, el correo electrónico, el telegrama, el télex o el telefax; no es necesario que por la vía de la reglamentación de la Ley 1480 de 2011 se complemente la definición de ventas a distancia de la Ley de Consumidor, para mencionar así de forma expresa las ventas a distancia que se realizan por Internet y por correo electrónico (MONTOYA, 2013, pág. 442).

Aunque el término de comercio electrónico es de reciente creación, en pocas palabras puede considerarse como un tipo de comercio que se da con la interacción entre el consumidor y el vendedor/productor, pero a través de un escenario diferente, el de las nuevas tecnologías. Con el objeto de tener un panorama esclarecido para el tratamiento de la temática que se ocupa, es necesario precisar que el comercio electrónico conecta con nociones que deben ser diferenciadas, tales como: contrato electrónico, contrato informático, internet, ciber espacio y email.

Características del Comercio Electrónico.

Para PLAZAS (2012), lo que caracteriza al comercio electrónico moderno como algo diferente y novedoso, es "*la existencia de una infraestructura global de tecnologías de la telecomunicación y redes en la que se lleva a cabo un proceso de digitalización y transmisión de la información"* (pág. 6). Así mismo, el comercio electrónico goza de ser un medio más barato de promoción de bienes y servicios, ya que aliviana los costos relacionados con el pago de arrendamiento o compra de un local y la contratación de personal de ventas. De igual manera, se caracteriza por permitir, sin necesidad de desplazamiento de las partes, acceder a una gran cantidad de ofertas de bienes y servicios.

Además de ello, el comercio electrónico se caracteriza por utilizar contratos predispuestos, a través de los cuales los empresarios pretenden vender masivamente sus bienes o servicios, con la característica de que una de las partes (el aceptante) no puede discutir el contenido del contrato. Esta circunstancia ha situado este tipo de contratación bajo la órbita del derecho del consumo. (VILLALBA, 2008, pág. 87). En otras palabras, se pueden enunciar algunas de las características del comercio electrónico:

- Disminuir costos de bodega, empleados y cadenas.
- Disminuir costos de entrega y comunicación
- Optimiza la logística
- Viabilidad de la penetración en mercados internacionales
- Fomenta la comunicación interactiva con los clientes y permite conocer las necesidades futuras de productos o servicios.
- Brindar métodos efectivos y rápidos de pago.
- Acceso global abierto todo el tiempo, para contactar a cualquier persona, en cualquier horario y lugar.

Este tipo de comercio abarca todas las transacciones comerciales realizadas mediante sistemas electrónicos de procesamiento y transmisión de información en Internet. Su importancia radica en que es un área donde las tecnologías de la información permiten el manejo y la recolección, procesamiento, almacenamiento, recuperación y comunicación de grandes cantidades de información confidencial (PLAZAS, 2012, pág. 6).

Clasificación (Tipología) del comercio Electrónico

La práctica internacional del comercio electrónico ha conducido a una categorización de los mismos. VILLALBA (2008), los explica de esta forma:

— ***"Comercio entre empresas y consumidores B2C:***
(Business to consumer, o empresa a consumidor). Se trata de web sites o páginas de Internet en las cuales las empresas ofrecen sus productos o servicios a los consumidores con la posibilidad de compra a través de la red a través de diferentes medios de aceptación y pago. El pionero de esta forma de comercio electrónico fue el sitio Amazon.com. Hoy en día gran cantidad de empresas ofrecen esta modalidad, algunas como forma exclusiva de venta.

— ***Comercio entre empresas B2B*** *(business to business o empresa a empresa) Consiste en la colaboración entre empresas con la creación de plataformas electrónicas en las cuales se realizan transacciones de manera eficiente y con la utilización de medios electrónicos.*

— ***Comercio entre consumidores C2C:*** *(consumer to consumer o consumidor a consumidor) Se trata de páginas de Internet a través de las cuales los particulares ofrecen diferentes clases de bienes o servicios. La página sirve solamente como un intermediario para que los particulares intercambien y ofrezcan bienes y servicios a cambio de una comisión.*" Negrita fuera del texto (págs. 87,88)

Por otro lado, DEL RÍO CORTINA & MARTINEZ (2015) dividen el comercio electrónico en directo e indirecto, y señalan que:

- "***Comercio electrónico directo:*** *Es aquel en el cual tanto el pedido como el pago y el envío de los bienes intangibles o tangibles y/o servicios inclusive, se producen 'on-line', como es el caso de transacciones u operaciones vinculadas con viajes, venta de boletos (teatros, conciertos, etc.), software, toda la rama de entretenimientos (música, juegos, apuestas), servicio de banca, venta de inmuebles, asesoría legal, consejos de salud, temas de educación y servicios por parte del Gobierno.*
- ***Comercio electrónico indirecto:*** *Consiste en adquirir bienes tangibles que necesitan luego ser enviados físicamente, utilizando para ello los canales o vías tradicionales de distribución*". Negrita fuera del texto. (págs. 7,8)

El comercio electrónico concebido en el marco de redes abiertas, puede generar varias modalidades, las cuales están plenamente diferenciadas por la doctrina y tienen que ver con las mercancías o servicios que se transan y la manera de hacerlo (GÓMEZ, 2004, pág. 21)**.** Existe una multiplicidad de categorización o clasificación del comercio electrónico que puede sintetizarse en la tabla que se muestra a continuación:

Tabla N° 2. Clasificación del comercio electrónico

Clasificación del Comercio electrónico		
Según los agentes económicos que participan	**Según la operatividad y funcionalidad**	**Según el sistema que soporta**
-Comercio entre empresas y consumidores B2C: (*Business to consumer* o empresa a consumidor). -Comercio entre empresas B2B (*business to business* o empresa a empresa) -Comercio entre consumidores C2C: (*consumer to consumer* o consumidor a consumidor)	-Comercio electrónico directo: el pedido, el pago y el envío de los bienes intangibles y/o servicios se producen online -Comercio electrónico indirecto: utilizado para la adquisición de bienes tangibles que necesitan ser enviados físicamente usando canales tradicionales de distribución	-Sistema cerrado: el sistema de intercambio de datos electrónico (EDI) - Sistema abierto: Internet.

NOTA: Descripción de los modelos de comercio electrónico, adaptado de (BECERRA RODRIGUEZ, 2012 pág. 35) *y* (BRIZZIO, 2001 pág. 68), *realizado por Rodrigo Cortes Borrero*

En el caso de bienes tangibles, internet es una herramienta de promoción eficaz para el acceso instantáneo a todos los mercados, que permite detectar y desarrollar nichos, donde los pequeños productos pueden encontrar ventajas competitivas; y, como las distancias entre oferente y demandante desaparecen, quedan eliminadas las resultantes de la ubicación geográfica (PIAGGI, 2001 págs. 72,73)**.**

Las operaciones que el comercio electrónico despliega son tan diversas como la tecnología que se desarrolla diariamente. Las principales actividades generadoras de ingresos en internet son: 1) publicidad y Marketing, 2) venta directa de bienes, 3) adquisición de servicios. Estas operaciones tienen un objetivo: hacer circular una infinidad de productos y servicios que son demandados por la sociedad a nivel mundial.

Productos con vocación para el comercio electrónico

Un proceso comercial que está especialmente adaptado al comercio electrónico es la venta de artículos básicos. Se trata de bienes o servicios que son difíciles de distinguir de aquellos proporcionados por otros vendedores, sus características se han estandarizado y son muy

conocidas como la gasolina, artículos de oficina, jabón, computadores, transporte aéreo y libros (CÁRDENAS, 2009 pág. 79)

Tabla N° 3. Calificación de productos

Propios del comercio electrónico	**Compatibles con el e-comercio y el comercio tradicional**	**Propios del comercio tradicional**
- Venta y compra de libros - Entrega de software por internet - Venta de servicios de viaje - Seguimiento de envíos en línea - Venta de historietas coleccionables	- Venta y compra de automóviles - Banca en línea - Servicios de búsqueda de compañeros de habitación compatibles - Venta/compra de productos relacionados con inversiones y seguros	- Venta y compra de ropa de marca - Venta/compra de productos alimenticios perecederos - Compras y ventas de pequeña denominación - Venta de joyas actividades valiosas

NOTA: Descripción de productos compatibles en el Comercio electrónico, adaptado de Gary P SCHNEIDER citado por (CÁRDENAS, 2009, pág.80)

Una combinación de estrategias de comercio electrónico y tradicional funciona mejor cuando el proceso de negocio incluye elementos tanto de artículos básicos como de inspección personal como ocurre con la gente que encuentra en la web información sobre carros nuevos y usados.

Tabla N° 4. Bienes y servicios aptos para el comercio electrónico

Productos	Servicios
● Música ● Videos en línea ● Teléfono sobre IP ● Subastas electrónicas ● Comunidades virtuales ● Productos configurables por el cliente ● Tiquete electrónico	● Soporte técnico en línea ● Banca electrónica ● Capacitación virtual ● Teletrabajo ● Automatización de la fuerza de ventas ● Conectividad inalámbrica (WiFi y Wimax) ● e-salud ● Recorridos virtuales (Turismo)

NOTA: Productos y servicios frecuentes en el comercio electrónico, adaptado de Gary P SCHNEIDER citado por (Cárdenas, 2009, pág.81)

El comercio electrónico no estaría completo en su tratamiento sino se pronuncia respecto de los medios de pago, que este nuevo escenario contractual, de transacción, de interconexión nos presenta, y son los medios de pago, pues a su vez que las operaciones se han transformado de manera exponencial se han creado paralelamente formas para satisfacer las obligaciones que este entorno requiere.

Ventajas y desventajas del Comercio Electrónico.

Ventajas

Se conoce, generalmente, que el comercio electrónico tiene efectos agudos en el sistema de comercio multilateral; el cambio de los métodos tradicionales a la tecnología de información digital electrónica, de comunicación y almacenamiento de información sustitutivos del papel, puede cambiar la estructura de los mercados relevantes, y en ese contexto los países de la OMC

tienen un importante rol que jugar. El comercio electrónico reduce o simplifica la necesidad de movilizar personas físicas; el tráfico adquiere mayor fluidez a menor costo y permite a las empresas desplazar sus oficinas a lugares menos cotizados, porque empleados y empleadores pueden acceder a Internet desde cualquier parte (PIAGGI, 2001 pág. 74)**.**

De hecho, el comercio electrónico amplía la posibilidad de promocionar y vender en el exterior servicios tradicionalmente poco transables, como turismo y servicios profesionales (asesoramiento contable y auditoría, arquitectura y diseño, ingeniería, legal, bienes raíces, y capacitación a distancia). También viabiliza la potenciación de oportunidades a través del armado de redes de productores de bienes o servicios similares, con producción insuficiente para satisfacer demandas externas. Las redes están siendo utilizadas por empresas que quieren aprovechar nuevos tipos de actividad, o formas de trabajo (teletrabajo y entornos de virtuales compartidos) y, los entes públicos las operan en su interacción con empresas y ciudadanos (BRIZZIO, 2001 pág. 73)**.**

Se puede entonces a través de 2 posturas doctrinales establecer las ventajas del comercio electrónico. Según (CÁRDENAS, 2009 pág. 82) se pueden clasificar en 3 grandes perspectivas de ventajas:

Tabla N° 5. Ventajas del comercio electrónico desde distintas perspectivas

Desde el punto de vista de los productores:	- Menores costos de entrada: La entrada en los mercados virtuales no es costosa y se caracteriza por su sencillez. - Diversificación: Un conjunto de productos digitalizados puede presentarse de diversas formas para crear líneas secundarias de producto. - Acceso directo al cliente: La red garantiza un contacto directo entre productores y consumidores, sin que sean necesarios los distribuidores o las redes de ventas. - Menores costos de distribución: La separación entre el contenido y los medios de almacenamiento permite la eliminación o simplificación de varias etapas en la cadena de distribución tradicional. - Circuitos indirectos de ventas: Los minoristas pueden utilizar la red para indicar los puntos de venta tradicionales al por mayor o al detalle. - Mercados pre-segmentados: La red fomenta la auto segmentación y el autoposicionamiento. - Ahorro en los costos de publicidad: La simple presencia en la red es un acto publicitario. - Menores costos de salida: La salida del mercado también es poco onerosa como en los costos de entrada. - Mercados secundarios: Es posible obtener ingresos suplementarios por la venta de espacios publicitarios o por el diseño de páginas de bienvenida.
Desde el punto de vista del consumidor:	- Incitación a abandonar la pasividad: La red ofrece la posibilidad al consumidor de hacer oír su voz y de informarse más a fondo sobre los productos. - Ampliación de las opciones: El consumidor tiene mayores posibilidades de elección debido a la ampliación y a la diversificación de productos que se ofrecen. - Transparencia: Se favorece la transparencia, ya que se facilita el intercambio de información entre los consumidores. - Control de precios: La transparencia del mercado hace más difícil engañar al consumidor. - Comodidad: Las compras electrónicas resultan más cómodas para los consumidores. - Sensibilidad a las reacciones del consumidor: Los vendedores estarán atentos a las reacciones de los consumidores. - Carácter impersonal de las operaciones: Algunos consumidores aprecian el anonimato que proporciona el comercio electrónico.

Otras ventajas que se establecen según PEÑA VALENZUELA:

Tabla N° 5. Continuación

Desde el punto de vista de la sociedad	- La emisión y llegada, con seguridad y rapidez, de pagos electrónicos, de devoluciones de impuestos, pago de jubilaciones y asistencia social, cuestan menos cuando se hacen por internet. - Los pagos electrónicos pueden ser más fáciles de auditar que los pagos hechos con cheque, lo cual proporciona protección contra el fraude y pérdidas por robo. En la medida de que el comercio electrónico permite que las personas trabajen desde la casa, todos se benefician con la reducción de tráfico y contaminación. - Permite que productos y servicios sean más accesibles en áreas distantes, por ejemplo, la educación y la salud "a distancia".

NOTA: Análisis de diferentes puntos de vista sobre comercio electrónico, adaptado de (Cárdenas, 2009), *realizado por Rodrigo Cortes Borrero.*

Tabla N° 6. Ventajas del comercio electrónico

El consumidor online tiene opciones de comparación de ofertas:	- La variedad de productos en un solo lugar le permite al consumidor comparar productos y ofertas de manera más fácil y le asegura reducción de costos en el proceso de búsqueda. - El comercio electrónico facilita que el consumidor compare de manera mucho más fácil uno de los aspectos más relevantes en su decisión de compra: el precio. Esto se hace posible por medio de buscadores, "ShopBots" intermediarios "online" y otros recursos de información "online" que ayudan a reducir tiempo, esfuerzo y los costos en los que se tiene que incurrir cuando se va de almacén en almacén buscando un producto. - Los consumidores que usan el Internet como medio de adquisición, saben regularmente que pueden hacer una búsqueda mucho más amplia que si la hacen "offline". - Saben que pueden considerar en una sola visita una variedad de alternativas que no lograrán con una salida a la calle. Asimismo, saben que gastarán menos tiempo y dinero en su labor de búsqueda.
El vendedor "online" reduce costos y puede ofrecer mejores precios	- Los costos del vendedor "online" (y de todas las ventas a distancia) se reducen y por ende el oferente puede ofrecer mejores precios y otros beneficios lo cual se traduce en beneficios al consumidor. - La tienda "online" no tiene que preocuparse por invertir en un local comercial que, además de estar situado en un lugar estratégico, debe lucir agradable para el consumidor y cautivarlo. - No tiene que pensar en contratar personal con buena presentación; al contrario, puede ubicar una gran bodega con toda la mercancía en lugares donde los servicios básicos y los impuestos son más bajos, lo cual significa variedad de bienes y servicios más accesibles al público. - La accesibilidad a cualquier tienda o almacén "online" permite la democratización del consumo, pues en principio el acceso a ellas y su éxito depende de la versatilidad del sitio web, de su facilidad de uso y de las herramientas técnicas que le dan vida y que brindan beneficios a cualquier consumidor, independientemente de su apariencia y estrato.
No existen límites territoriales	- En las ventas a distancia por transmisión de datos no existen límites geográficos. - La velocidad de la transmisión de los mensajes de datos en la red es casi completamente independiente de la ubicación física. - Los mensajes de datos para consolidar una venta a distancia se transmiten casi de manera perfecta sin sufrir alteraciones o retrasos considerables. - La inexistencia de linderos y la inmensidad del espacio, multiplican las posibilidades de ofertas en calidad y precios

	- Aminora la posibilidad que tienen los gobiernos de asumir el control total, por lo que se impone la flexibilidad de las reglamentaciones, a fin de que, a partir de principios básicos regulatorios, se puedan sortear diferentes irregularidades que la velocidad de la tecnología no permite prever.

NOTA: Análisis de las ventajas del Comercio electrónico, adaptado de (PEÑA, 2013, pág. 444), *realizado por Rodrigo Cortes Borrero*

En conclusión, el comercio electrónico a través del alcance de Internet, cuenta con la posibilidad de contactar a cualquier persona y a cualquier hora y en cualquier lugar. Lo cual significa acceso global y servicio las 24 horas del día (RUEDA, 2007, pág. 42).

Desventajas

La mayor desventaja proviene de la falta de confianza en los mecanismos tecnológicos es uno de los principales obstáculos para el desarrollo del comercio electrónico. Esto obedece a varios factores: (1) El anonimato de las transacciones electrónicas; (2) La dificultad práctica de garantizar la confidencialidad e integridad de la información; (3) El bajo acceso de las personas a las TIC´s así como el desconocimiento de la forma como éstas funcionan, y (4) la barrera cultural. (REMOLINA, 2006, pág. 326) Por eso, se insiste, el problema del desarrollo del comercio electrónico no es sólo tecnológico o legal, porque estamos en una etapa de transición donde aún existe mucho desconocimiento y desconfianza sobre los negocios electrónicos o virtuales. En este sentido, Reichheld y Schefter estiman que el precio no es el elemento esencial que impulsará los negocios a través de medios electrónicos sino la confianza que se genere en los mismos.

Por ende, como lo determina VILLALBA (2012) la seguridad y confianza son factores estrechamente ligados. De no contar con medios electrónicos seguros las actividades no crecerán en las escalas deseables. Por eso, el desarrollo del comercio electrónico dependerá, en parte, del nivel de seguridad de las aplicaciones utilizadas en el mismo. (pág. 326) Confianza, en el contexto del comercio electrónico, puede entenderse como el hecho de tener seguridad de que la empresa y el consumidor van a realizar una transacción o cualquier actividad con las mismas o mayores garantías de las que tiene en el negocio tradicional. Ciertos aspectos que involucran el desarrollo de la confianza y la seguridad en el uso de medios electrónicos se destacan en la siguiente gráfica:

***Tabla N° 7. Algunos factores que inciden en el grado de confianza de los negocios electrónicos*.**

Identidad	Estar seguros que: (1) realizamos negocios con determinada persona y no con otra; (2) dicha persona existe y tiene capacidad jurídica.
Confidencialidad	Impedir que personas no autorizadas accedan a la información que queremos proteger.
Integridad	Garantizar que los documentos electrónicos no sean alterados, modificados, falsificados o manipulados.
No repudio	Tener la certeza jurídica de que los mensajes de datos son una forma válida de manifestar la voluntad y un medio de prueba.

NOTA: Descripción de los factores que inciden en el grado de confianza de los negocios electrónicos, adaptado de (Analisis de la Ley 1480 de 2011, que reforma el Estatuto de Proteccion al Consumidor en Colombia, 2012 pág. 326)

Riesgos del Comercio Electrónico:

Según DEL RÍO CORTINA & MARTINEZ (2015) los riesgos acerca del comercio electrónico son los siguientes:

- *"Elección del producto o servicio: Uno de los riesgos a los que se enfrenta el consumidor electrónico es en lo que tiene que ver con la idónea selección del producto o servicio a adquirir, como quiera que la negociación no es de carácter presencial, el consumidor se*

ve expuesto a materializar un negocio jurídico viciado por error, entre lo que se quiere y lo que realmente se obtiene.

- *Riesgo de Seguridad: Este riesgo está asociado al negocio, a las partes que en el intervienen, al medio de pago, entre otras, como quiera que puede haber dificultad en identificar a las partes, que la transacción no queda registrada, así como dificultades probatorias de los negocios*
- *Violación a Derechos de Propiedad Intelectual: Especialmente los relacionados con Derechos de autor por la compra de contenidos digitales protegidos por estos derechos, tal es el caso de la adquisición de libros, discografías etc.*
- *Conflictos de jurisdicción tributaria - Situaciones de doble imposición o de ausencia de imposición.*
- *Principios clásicos del derecho tributario internacional no son aplicables al comercio electrónico: identificación precisa de las partes, existencia de territorios con límites claros, existencia de intermediarios que controlan y retienen los tributos, necesidad de registros comerciales precisos, aplicación de tributos sobre bienes físicos.*
- *Evasión fiscal por Internet "* (págs. 8,9)

Así mismo CÁRDENAS (2009) señala que existen algunas problemáticas respecto a este tipo de comercio:

- *Problemas para integrar software de bases de datos y procesamiento de transacciones existentes diseñados para el comercio tradicional al software del comercio electrónico.*
- *Obstáculos culturales y legales en la conducción de comercio electrónico (reticencia de los "Algunos procesos de negociación tal vez nunca se ajusten al comercio electrónico como alimentos perecederos o artículos de alto costo (joyas de diseño específico y antigüedades)*
- *Dificultad para calcular el rendimiento sobre la inversión al hacer uso de una nueva tecnología.*
- *Inconveniencias para contratar y retener empleados con habilidades en procesos tecnológicos y en el diseño de procesos comerciales requeridos para crear un comercio electrónico eficiente.*
- *consumidores al cambio e inseguridad, ausencia de leyes o existencias de las mismas poco claras y conflictivas)."* (págs. 83,84)

Conclusiones

El escenario del comercio electrónico, aunque novedoso y dinámico presenta riesgo y desafíos, que, sin embargo, se ven superados por las bondades de un nuevo espacio de negociación, de riqueza de información, de ofertas y beneficios; claro está que debe ser gobernado, usado e interpretado a través de prácticas no contrarias a la buena fe o en búsqueda de comisión de ilícitos.

Colombia presenta un marco normativo que aúna esfuerzos para dar solución a las diversas problemáticas que la realidad económica dinámica y cambiante presenta, puesto este nuevo escenario es de orden global, sin estándares determinados y que requiere de cada vez mayores esfuerzos estatales para sus buenas prácticas.

BIBLIOGRAFÍA

Analisis de la Ley 1480 de 2011, que reforma el Estatuto de Proteccion al Consumidor en Colombia. **Villalba Cuellar, Juan Carlos. 2012.** s.l. : Universidad Santo Tomás, 2012, Principia IURIS, págs. p.32-63.

Analisis Historico y Comparado del Comercio Electrónico. **Trujillo Cabrera, Juan y Becerra Rodríguez, Ronald. 2010.** s.l. : Corporación Universitaria Republicana, 3 de Agosto de 2010, Revista Republicana, págs. p.37-53.

Aspectos legales del comercio electrónico, la contratación y la empresa electrónica. **Remolina Angarita, Nelson. 2006.** Bogotá D.C : Universidad de los Andes, Agosto de 2006, Revista de Derecho: Comunicaciones y Nuevas Tecnologías, págs. p.323-370.

Becerra Rodriguez, Ronald Ralf. 2012. Retrospectivas de la Regulación del comercio electrónicosu evolución y retos. [aut. libro] María Elena Grueso Rodríguez. *La Regulacion del Comercio Electronico Mundial.* Bogotá : Temis, 2012, págs. 33-78.

Brizzio, Claudia R. 2001. Contratos informáticos y contratos por medios informáticos. [aut. libro] Atilio Aníbal Alterini, José Luis de los Mozos y Carlos Alberto Soto. *Contratación Contemporánea - Contratación Electrónica y tutela del consumidor.* Lima, Perú : Temis, 2001, págs. 79-112.

Cárdenas, Manuel José. 2009. *¿Cuál en la situación del comercio electrónico en Colombia?* Bogotá : Universidad Sergio Arboleda, 2009.

1996. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Ley Modelo de la CNUDMI sobre Comercio Electronico (Resolución 51/162).* [En línea] 16 de diciembre de 1996. https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf.

1991. *Constitución Política de Colombia [Const]*. 7 de Julio de 1991.

Contratos por medios electrónicos. Aspectos sustanciales y procesales. **Villalba Cuellar, Juan Carlos. 2008.** 22, s.l. : Universidad Militar Nueva Granada, Julio-Diciembre de 2008, Prolegómenos: Derechos y Valores, Vol. XI, págs. p.85-108.

—. **Villalba Cuellar, Juan Carlos. 2008.** Bogotá : Universidad Militar Nueva Granada Colombia, 2008, Prolegómenos: Derechos y Valores, págs. 85-108.

Cubillos Velandia, Ramiro y Rincón Cardenas, Erick. 2002. *Introducción Jurídica al Comercio Electrónico.* Bogotá : Gustavo Ibañez. , 2002.

Del Río Cortina, Jorge y Martínez Pacheco, Belkys . 2015. Los derechos del consumidor electronico y su impacto frente a las transacciones internacionales. s.l. : Universidad Tecnológica de Bolívar, 19 de Noviembre de 2015.

2000. Directiva presidencial N° 02. *Gobierno en linea.* s.l., Colombia : Presidencia de la Republica, Ministerio de Tecnologías de la Información y las Comunicaciones, 28 de agosto de 2000.

2000. *Corte Constitucional de Colombia.* Sentencia C-662, s.l. : MP. Fabio Morón Díaz, 8 de junio de 2000.

Gómez Pérez, Victor Ivan. 2004. Realidad jurídica del comercio electrónico en Colombia. *Tesis de grado de Abogado, Facultad de Ciencias Jurídicas.* Bogotá, Colombia : Pontificia Universidad Javeriana, 2004.

La protección de los ciberconsumidores desde la mirada del derecho internacional privado argentino. **Cárdenas, Sara L. Feldstein de, y otros. 2010.** Buenos Aires : Universidad de Buenos Aires, 2010. III Congreso Euroamericano de Proteccion Juridica de los Consumidores. págs. 1-9.

La protección del consumidor en el contexto del comercio electrónico. **Remolina Angarita, Nelson y Flórez Rojas, María Lorena. 2012.** Bogotá D.C : Universidad de los Andes, Junio de 2012, Revista de Derecho: Comunicaciones y Nuevas Tecnologías, págs. 1-19.

2011. Ley 1480. *Por medio de la cual se expide el Estatuto del Consumidor.* s.l., Colombia : Diario Oficial No. No.48220, 12 de Octubre de 2011.

1999. Ley 527. *por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.* s.l., Colombia : Diario Oficial No.43.673, 18 de agosto de 1999.

2000. Ley 633 . *Por la cual se expiden normas en materia tributaria, se dictan disposiciones sobre el tratamiento a los fondos obligatorios para la vivienda de interés social y se introducen normas para fortalecer las finanzas de la Rama Judicial.* s.l., Colombia : Diario Oficial No.44275, 29 de Diciembre de 2000.

Medina Vergara, Jairo. 2013. *Derecho Comercial, parte general.* Bogotá : Temis, 2013.

Meraz Espinoza, Ana Isabel . 2006. Aspectos jurídicos del comercio electrónico como comercio transnacional. *Memoria para optar al grado de doctor en Derecho, Facultad de Derecho.* s.l., España : Universidad Complutense de Madrid, 2006.

Montoya Naranjo, Claudia M. 2013. Reflexiones sobre las ventas a distancia y el comercio electrónico. [aut. libro] Carmen Ligia Valderrama Rojas. *Perspectivas del Derecho del Consumo*. Bogotá : Universidad Externado de Colombia, 2013, págs. 435-462.
Organizacion Mundial del Comercio (OMC). s.f.. Comercio electrónico. *wto.org*. [En línea] s.f. https://www.wto.org/spanish/thewto_s/whatis_s/tif_s/bey4_s.htm.
Organización para la Cooperación y el Desarrollo Económico- OCDE-. 1999. Recomendación del Consejo de la OCDE relativa a los lineamientos para la protección al consumidor en el contexto del comercio electrónico. [En línea] 9 de Diciembre de 1999.
Peña Valenzuela, Daniel. 2013. La protección del consumidor en el comercio electrónico. [aut. libro] Carmen Ligia Valderrama Rojas. *Perspectivas del Derecho del Consumo*. Bogotá : Universidad Externado de Colombia, 2013, págs. 463-498.
Piaggi, Ana Isabel. 2001. El Comercio Electronico y el Nuevo escenario de los Negocios. [aut. libro] Atilio Aníbal Alterini, José Luis de los Mozos y Carlos Alberto Soto. *Contratacion Contemporánea - Contratación Electrónica y Tutela del Consumidor*. Lima, : Temis, 2001, págs. 65-78.
Plazas Estepa, Rodrigo Alberto. 2012. [aut. libro] María Elena Grueso Rodríguez. *La regulación del comercio electrónico mundial.* Bogotá : Temis, 2012, págs. 1-17.
Rincón Cárdenas, Erick. 2015. *Derecho del Comercio Electrónico y de Internet.* Segunda. Bogotá : Legis, 2015. pág. 488. ISBN: 978-958-767-249-7.
Río Cortina, Jorge Del y Martínez Pacheco, Belkys. 2015. Los derechos del consumidor electrónico y su impacto frentea las transacciones internacionales. *researchgate.net.* [En línea] 19 de Noviembre de 2015. https://www.researchgate.net/publication/284179440_LOS_DERECHOS_DEL_CONSUMIDOR_ELECTRONICO_Y_SU_IMPACTO_FRENTE_A_LAS_TRANSACCIONES_INTERNACIONALES.
Villalba Cuellar, Juan Carlos. 2012. *Introducción al Derecho del Consumo.* Bogotá : Universidad Militar Nueva granada., 2012.

DELITOS INFORMÁTICOS Y OTRAS CONDUCTAS PUNIBLES COMETIDAS A TRAVÉS DE REDES SOCIALES Y SUS IMPLICACIONES JURÍDICAS EN COLOMBIA

Por: ***Jully Pauliny González López y***
Rafaél Esteban Llerena Riascos
Colombia

INTRODUCCIÓN

No se puede negar que el desarrollo de las tecnologías de la información y comunicación ha generado una revolución en la sociedad permitiendo un desarrollo en todos los contextos y ámbitos que ella contiene. Así, para las personas las TIC hoy en día son un elemento necesario que contribuyen a su desarrollo en la llamada sociedad de la información y el conocimiento.

Uno de esos beneficios y revoluciones generadas por las TIC son las nuevas formas de interacción y relación entre las personas a nivel global, evidenciado especialmente por el uso de las redes sociales. Sin embargo, a pesar del sin número de beneficios que traen las nuevas tecnologías a la sociedad, existen situaciones en las que a través de ellas se pueden generar afectaciones a sus usuarios, es decir, conductas ilícitas que deben regularse por parte del Derecho con el propósito de garantizar la protección de los derechos de todos los usuarios de estas nuevas formas de comunicación.

De acuerdo con el artículo El impacto de Internet y las redes sociales en el derecho a la libertad de expresión, el concepto de Red Social de Internet se refiere a:

> "la interacción de los sujetos en este ámbito, que se lleva a cabo a través de los mecanismos que ofrece la Web 2.0. En las redes sociales, el factor central es la actividad del individuo y su interacción con los demás integrantes de la red. Estos dos elementos conforman el concepto de las redes sociales que se desarrollan en un entorno electrónico, en el entendido que sin el factor humano no puede hablarse de red social y sin la plataforma electrónica no puede llegar a configurarse la red. El factor humano es fundamental, a tal punto que es considerado el elemento neurálgico de este concepto. La actividad de los individuos que forman parte de la red es una de las fuentes que más problemas genera en el ámbito de la protección de los derechos fundamentales." [1]

Así como también se ponen en riesgo la seguridad de la información, como consecuencia de delitos informáticos que se cometen a través de estos medios, atentando contra la dignidad de las personas, la libertad, entre otros.

Tomando como base el concepto dado en el libro Derecho informático, "los delitos informáticos se entienden desde dos formas: típica y atípica, refiriendo a la primera las conductas típicas antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin, y a la segunda actitudes ilícitas en que se tienen a las computadoras como instrumento o fin." [2]

---

[1] RICO CARRILLO, M., 2012. El impacto de Internet y las redes sociales en el derecho a la libertad de expresión. *Revista de filosofia juridica, social y politica FRONESIS* [en línea], vol. 19, no. 3, pp. 331–349. Disponible en: http://dspace.uah.es/dspace/handle/10017/6439.

[2] TÉLLEZ VALDÉS, J., 2009. *Derecho informático*. Cuarta edi. México, D. F.: McGraw-Hill. ISBN 978-970-10-6964-6.

De acuerdo con ello, es importante diferenciar cuando el computador es un instrumento o fin, así se podrán identificar claramente las conductas punibles cometidos por estos medios. Así, Mario Arboleda Vallejo, en su libro Manual de Derecho Penal Especial, cita que:

> "cuando la conducta criminal es cometida como método es aquella en la cual los sujetos "utilizan métodos electrónicos" para cometer el ilícito. Como medio son consideradas aquellas conductas criminales en donde, para realizar un delito, se usa una computadora como medio o símbolo. Como fin son las conductas criminales dirigidas en contra de la "entidad física del objeto o máquina electrónica o su material con objeto de dañarla." [3]

Esta investigación centra su atención en aquellas conductas que se cometen a través de las redes sociales, toda vez que, con el uso masivo de las mismas, éstas se han convertido en un medio para la comisión de un sin número de delitos informáticos y de otras conductas punibles que a pesar de no encontrase en esta categoría de delitos, tienen implicaciones jurídicas, en razón a que afectan derechos fundamentales y tipo de derechos. De esta manera se recopilan e identifican, los delitos informáticos que hasta la fecha ocurren con mayor frecuencia entre las personas que utilizan las redes sociales, así como también aquellas conductas que no adquieren la categoría de delito informático, pero se enmarcan en otras conductas punibles; esto con el propósito de estudiar e identificar las implicaciones jurídicas que tienen este tipo de conductas a la luz de la legislación colombiana.

Lo anterior obedece a que los usuarios desconocen los peligros a los que están expuestos, ello se evidencia en la gran cantidad de información que se generan y se comparten diariamente a través de estos medios electrónicos, dejando a un lado medidas mínimas de seguridad en el manejo de la información. De otra parte, se evidencia la confianza de los usuarios en la utilización de las redes sociales y de la red internet, descuidando como se mencionó anteriormente la seguridad básica que debe existir en el uso de plataformas tecnológicas y que los convierten en sujetos vulnerables y expuestos a posibles ataques de ciberdelincuentes u otros usuarios, donde no solo está en riesgo la información, sino también la integridad física, moral, emocional y financiera.

Ahora bien, teniendo en cuenta que uno de los elementos del tipo penal es el sujeto activo, es decir, quien desencadena o comete la conducta punible (delito), en las conductas cometidas a través de las redes sociales es claro que los usuarios de éstas pueden o no ser expertos en el manejo o utilización de la informática y de la tecnología misma, sin embargo, por omisión o desconocimiento pueden incurrir en conductas inadecuadas que conllevan a la realización de un delito informático (comisión) u otra conducta punible, convirtiéndolo en autor o partícipe, desencadenado así las consecuencias jurídicas, dependiendo de la conducta y el bien jurídico vulnerado.

En Colombia, en el año 2009 se expide la Ley 1273 [4], cuyo objeto de protección es la información y los datos, y en la cual se han tipificado una serie de conductas como delitos informáticos, sin embargo, con el uso de las redes sociales se presenta y generan nuevas conductas ilícitas que deben identificarse y así prevenirse, de otra parte, es importante que los usuarios de la red adquieran una cultura digital apropiada para evitar ser víctimas de estos delitos y/o ser autores o partícipes de alguna conducta delictiva.

Asimismo, es importante retomar la información del trabajo Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación, en la cual se busca

---

[3] ARBOLEDA VALLEJO, M. y RUIZ SALAZAR, J.A., 2016. *Manual de derecho penal especial*. 13. Bogota D.C.: UniAcademia Leyer. ISBN 978-958-769-479-6.

[4] CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2009a. Ley 1273 de 2009. *Diario Oficial 47.223 de enero 5 de 2009* [en línea]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492.

describir "Los comportamientos que se pueden reconocer como delitos informáticos en dichas redes y como se está adecuando la normatividad en Colombia a este crecimiento constante de las tecnologías de información y comunicación para prevenir, proteger y establecer un adecuado manejo." [5]

Otro estudio previo de gran relevancia para el tema que se aborda en este trabajo es el artículo denominado Delitos informáticos y entorno jurídico vigente en Colombia, en el cual se establecen algunos antecedentes de carácter jurídico (sobre la base de los derechos de autor) y alguna normatividad complementaria (Código Penal y circulares de la Superintendencia Financiera). "En 2009 se logró expedir la Ley 1273, con la cual pudo acceder al grupo de países que se han preparado con herramientas más eficaces para contrarrestar las acciones delictivas del cibercrimen, en sectores claves de la sociedad como el financiero, cuyas condiciones de vulnerabilidad son las más estudiadas e investigadas por los delincuentes informáticos." [6]

Es importante señalar que los resultados presentados en el presente artículo son los resultados parciales de una investigación macro de la cual se pretenden establecer estrategias de prevención en la comisión de delitos informáticos y demás conductas a través de las redes sociales.

El presente artículo se enmarca dentro del eje temático denominado *Riesgos de las nuevas tecnologías y grupos vulnerables*, toda vez que su propósito es la de generar conciencia en el uso adecuado de las redes sociales, por cuanto como usuarios de las mismas, podemos incurrir por omisión o conocimiento en la comisión de un delito informático u otras conductas punibles, así como también podemos ser potenciales víctimas de los ciberdelincuentes que aprovechan la falta de mecanismos de prevención por parte de las personas cuando navegan por internet, en especial cuando se expone demasiada información en las diferentes redes sociales.

RESULTADOS

Realizada la revisión bibliográfica de varios autores y de acuerdo con las estadísticas presentadas por la Policía Nacional de Colombia del año 2017, se han identificado los siguientes delitos informáticos y conductas punibles cometidos a través de las redes sociales, los cuales se detallan en las tablas (1 y

[5] RODRÍGUEZ ARBELÁEZ, J.D., 2011. Análisis de los delitos informáticos presentes en l as redes sociales en Colombia para el año 2011 y su regulación. [en línea]. [Consulta: 22 enero 2018]. Disponible en: http://bdigital.ces.edu.co:8080/repositorio/handle/10946/1334.

[6] OJEDA PÉREZ, J.E., RINCÓN RODRÍGUEZ, F., ARIAS FLÓREZ, M.E. y DAZA MARTÍNEZ, L.A., 2010. Delitos informáticos y entorno jurídico vigente en Colombia. *Computer crime and current legislation in Colombia.* [en línea], vol. 11, no. 28, pp. 41–66. ISSN 01231472. Disponible en: http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=59522387&lang=es&site=ehost-live.

2). [7] [8] [9] [10] [11] [12]

DELITOS INFORMATICOS COMETIDOS A TRAVÉS DE LAS REDES SOCIALES Y TIPIFICADOS EN LA LEGISLACION COLOMBIANA

DELITO INFORMÁTICO	DEFINICIÓN	LEY	PENA
Acceso abusivo a un sistema informático	El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.	LEY 1273 de 2009 - Artículo 269A	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
Obstaculización ilegítima de sistema informático o red de telecomunicación	El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones.	LEY 1273 de 2009 - Articulo 269B	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes

DELITO INFORMÁTICO	DEFINICIÓN	LEY	PENA
Interceptación de datos informáticos incurrirá en	El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte	Ley 1273 de 2009 - Artículo 269C	Prisión de treinta y seis (36) a setenta y dos (72) meses.
Daños informáticos	El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos	LEY 1273 de 2009 - Articulo 269D	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
Uso de software malicioso	El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional	LEY 1273 de 2009 - Articulo 269E	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes

[7] REVELO, L.C., 2011. *Guía de seguridad para prevenir y controlar delitos informáticos*. Pasto - Colombia: Institucion Universitaria CESMAG.

[8] RODRÍGUEZ ARBELÁEZ, J.D., 2011. Análisis de los delitos informáticos presentes en l as redes sociales en Colombia para el año 2011 y su regulación. [en línea]. [Consulta: 22 enero 2018]. Disponible en: http://bdigital.ces.edu.co:8080/repositorio/handle/10946/1334.

[9] OJEDA PÉREZ, J.E., RINCÓN RODRÍGUEZ, F., ARIAS FLÓREZ, M.E. y DAZA MARTÍNEZ, L.A., 2010. Delitos informáticos y entorno jurídico vigente en Colombia. *Computer crime and current legislation in Colombia.* [en línea], vol. 11, no. 28, pp. 41–66. ISSN 01231472. Disponible en: http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=59522387&lang=es&site=ehost-live.

[10] AREVALO MUTIZ, PAULA LUCÍA; GARCÍA LEGUIZAMÓN, FERNANDO MAURICIO; NAVARRO HOYOS, JULIÁN ANTONIO; PARDO ARIAS, A., 2012. Aproximación a problemáticas jurídicas de las redes sociales virtuales. *Revista Virtual Universidad Católica del Norte* [en línea], pp. 62–92. [Consulta: 25 enero 2018]. Disponible en: http://www.redalyc.org/html/1942/194224568005/.

[11] TÉLLEZ VALDÉS, J., 2009. *Derecho informático*. Cuarta edi. México, D. F.: McGraw-Hill. ISBN 978-970-10-6964-6.

[12] CENTRO CIBERNÉTICO POLICIAL, 2017. Amenazas del Cibercrimen en Colombia 2016-2017. [en línea]. Bogota D.C.: [Consulta: 26 enero 2018]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf.

	software malicioso u otros programas de computación de efectos dañinos		
Violación de datos personales	El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes.	LEY 1273 de 2009 - Articulo 269F	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
Suplantación de sitios web para capturar datos personales	El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes.	LEY 1273 de 2009 - Articulo 269G	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
Hurto por medios informáticos y semejantes	El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos.	LEY 1273 de 2009 - Articulo 269I	Prisión de 3 a 8 años
Transferencia no consentida de activos	El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave.	LEY 1273 de 2009 - Articulo 269J	Prisión de 48 a 120 meses y multa de 200 a 1.500 salarios mínimos vigentes

CONDUCTAS PUNIBLES COMETIDAS A TRAVÉS LAS REDES SOCIALES

CONDUCTA ILÍCITA	DEFINICIÓN	DELITO / CONDUCTA PUNIBLE	LEY	PENA
Ciberbullying	Es un tipo de agresión psicológica que se da usando las nuevas tecnologías: teléfonos celulares e Internet. Por medio de correos, mensajes o imágenes que se envían se busca herir o intimidar a otra persona. Este tipo de acoso no se hace de frente, por ello la víctima desconoce la identidad de su agresor.	Amenaza Instigación a delinquir (inciso 1)	Código penal - Articulo 347 – 348 respectivamente	Prisión de 1 a 4 años y multa de 10 a 100 salarios mínimos.
		Injuria – Injuria por vía de hecho	Código penal - Articulo 220 - 226	Prisión de 1 a 3 años
		Calumnia	Código penal - Articulo 221	Prisión de 1 a 4 años
		Injuria y calumnia indirectas	Código penal – Artículo 222	
		Circunstancias especiales de graduación de la pena.	Código Penal – Artículo 223. Inciso 1	Las penas respectivas se aumentarán de una sexta parte a la mitad.
		Circunstancias de mayor punibilidad: son circunstancias de mayor	Código penal - Artículo 58.	

		punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 3. Que la ejecución de la conducta punible esté inspirada en móviles de intolerancia y discriminación referida a la raza, la etnia, la ideología, la religión, o las creencias, sexto u orientación sexual, o alguna enfermedad o minusvalía de la víctima. Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.	Numerales 3 y 17	
Grooming	Es una nueva forma de acoso y abuso hacia niños, jóvenes que se ha venido popularizando con el auge de las TIC, principalmente los chats y redes sociales. Inicia con una simple conversación virtual, en la que el adulto se hace pasar por otra persona, normalmente, por una de la misma edad de niño con el objetivo de obtener una satisfacción sexual mediante imágenes eróticas o pornográficas del menor o incluso como preparación para un encuentro sexual.	Acceso carnal abusivo con menor de 14 años. En la modalidad de tentativa.	Ley 1236 de 2008	Prisión de 4 a 8 años
		Actos sexuales con menor de 14 años. En la modalidad de tentativa.	Ley 1236 de 2008	Prisión de 3 a 5 años
		Acceso carnal o acto carnal abusivo con incapaz de resistir. En la modalidad de tentativa.	Ley 1236 de 2008	Prisión de 4 a 8 años
		Acoso sexual	Ley 1257 de 2008	Prisión de 1 a 3 años
		Proxenetismo con menor de edad	Ley 1329 de 2009	Prisión de 14 a 25 años
		Pornografía con personas menores de 18 años	Ley 1329 de 2009	Prisión de 10 a 20 años
		Utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores 18 años	Ley 1329 de 2009	Prisión de 10 a 14 años
		Circunstancias de mayor punibilidad: son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios	Código penal - Artículo 58. Numerales 17	

		informáticos, electrónicos o telemáticos.		
Sexting	Es cuando alguien toma una foto poco apropiada de sí mismo (sexualmente explícita), y la envía a alguien vía teléfono celular o Internet.	Injuria – Injuria por vía de hecho	Código penal - Articulo 220 - 226	Prisión de 1 a 3 años
		Injuria y calumnia indirectas	Código penal – Artículo 222	
		Pornografía con personas menores de 18 años	Ley 1336 de 2009.	Prisión de 10 a 20 años
		Acoso sexual	Ley 1257 de 2008	Prisión de 1 a 3 años
		Circunstancias especiales de graduación de la pena.	Código Penal – Artículo 223. Inciso 1	
		Circunstancias de mayor punibilidad: son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 3. Que la ejecución de la conducta punible esté inspirada en móviles de intolerancia y discriminación referida a la raza, la etnia, la ideología, la religión, o las creencias, sexto u orientación sexual, o alguna enfermedad o minusvalía de la víctima. Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.	Código penal - Artículo 58. Numerales 3 y 17	
Sextorsión	Es la amenaza con el fin de obtener provecho o beneficio de enviar o publicar imágenes o videos con contenido sexual de una persona. Esto puede hacerse a través de teléfonos celulares o Internet.	Extorsión	Código penal - Articulo 244	Prisión de 8 a 15 años
		Circunstancias de mayor punibilidad: son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos,	Código penal - Artículo 58. Numerales 3 y 17	

		electrónicos o telemáticos.		
		Utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores 18 años	Ley 1329 de 2009	Prisión de 10 a 14 años
		Constreñimiento ilegal	Código penal - Articulo 182	Prisión de 1 a 2 años
Carding / **Turinet /** **Estafa Electrónica**	El carding consiste en usar un número de tarjeta de crédito ya sea real o creado de la nada mediante procedimientos digitales para realizar compras a distancia por Internet y efectuar pagos. El Turinet es una estafa en la cual los delincuentes a través de redes sociales o internet en general ofrecen alquilar una propiedad (finca, casa, apartamento, etc.), y al momento de recibir el adelanto del pago total del alquiler, desaparecen sin dejar rastro, dejando a la víctima sin el alquiler de la propiedad ni el dinero. La estafa electrónica se da cuando en el e-commerce los usuarios desean comprar un producto por internet y suelen suceder estafas con productos falsos.	Hurto por medios informáticos y semejantes	LEY 1273 de 2009 -Articulo 269I	Prisión de 3 a 8 años
		Hurto por medios informáticos y semejantes	LEY 1273 de 2009 - Articulo 269I	Prisión de 3 a 8 años
		Estafa	Código penal - Articulo 246	Prisión de 2 a 8 años
		Circunstancias de mayor punibilidad: son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.	Código penal - Artículo 58. Numerales 3 y 17	
Phishing	Método más utilizado por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.	Violación de datos personales	LEY 1273 de 2009 -Articulo 269F	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
		Estafa	Código penal - Articulo 246	Prisión de 2 a 8 años
		Suplantación de sitios web para capturar datos personales	LEY 1273 de 2009 -Articulo 269G	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
		Hurto por medios informáticos y semejantes	LEY 1273 de 2009 -Articulo 269I	Prisión de 3 a 8 años

		Transferencia no consentida de activos	LEY 1273 de 2009 -Articulo 269J	Prisión de 48 a 120 meses y multa de 200 a 1.500 salarios mínimos vigentes
		Circunstancias de mayor punibilidad: son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.	Código penal - Artículo 58. Numerales 3 y 17	
Creación de perfiles falsos / Catfish	Es cuando una persona decide crear un nuevo perfil en una red social, con información que es falsa (falso nombre, falsa profesión, falso domicilio, etc.), o lo crea tomando información real pero que pertenece a otra persona.	Violación de datos personales	LEY 1273 de 2009 -Articulo 269F	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
		Injuria – Injuria por vía de hecho	Código penal - Articulo 220 - 226	Prisión de 1 a 3 años
		Calumnia	Código penal - Articulo 221	Prisión de 1 a 4 años
		Injuria y calumnia indirectas	Código penal – Artículo 222	
		Circunstancias especiales de graduación de la pena.	Código Penal – Artículo 223. Inciso 1	Las penas respectivas se aumentarán de una sexta parte a la mitad.
		Circunstancias de mayor punibilidad: son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.	Código penal - Artículo 58. Numerales 3 y 17	
Fraping	Es el acto de acceder al perfil de alguien cuando se lo deja conectado, e implica cambiar	Acceso abusivo a un sistema informático	LEY 1273 de 2009 -Artículo 269A	Prisión de 48 a 96 meses y multa de 100

	detalles de la cuenta como privacidad o actualizar su perfil con un estado falso mensaje o imagen mientras están temporalmente lejos de la computadora o dispositivo móvil.			a 1.000 salarios mínimos vigentes
		Daños informáticos	LEY 1273 de 2009 -Artículo 269D	Prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
		Violación de datos personales	LEY 1273 de 2009 -Articulo 269F	Prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
		Injuria – Injuria por vía de hecho	Código penal - Articulo 220 - 226	Prisión de 1 a 3 años
		Calumnia	Código penal - Articulo 221	Prisión de 1 a 4 años
		Injuria y calumnia indirectas	Código penal – Artículo 222	
		Circunstancias especiales de graduación de la pena.	Código Penal – Artículo 223. Inciso 1	Las penas respectivas se aumentarán de una sexta parte a la mitad.
		Circunstancias de mayor punibilidad: son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.	Código penal - Artículo 58. Numerales 3 y 17	

Outing	Acto deliberado para avergonzar o humillar publicando online información confidencial, privada o embarazosa sin el consentimiento de la persona.	Injuria – Injuria por vía de hecho	Código penal - Articulo 220 - 226	Prisión de 1 a 3 años
		Calumnia	Código penal - Articulo 221	Prisión de 1 a 4 años
		Injuria y calumnia indirectas	Código penal – Artículo 222	
		Circunstancias especiales de graduación de la pena.	Código Penal – Artículo 223. Inciso 1	Las penas respectivas se aumentarán de una sexta parte a la mitad.
		Circunstancias de mayor punibilidad: son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.	Código penal - Artículo 58. Numerales 3 y 17	
Trolling	Trolling se puede comparar a una forma de acoso cibernético e implica el envío o la presentación de correos electrónicos o publicaciones provocativas con la intención de incitar a una respuesta enojada.	Amenaza[13] Instigación a delinquir (inciso 1)	Código penal - Articulo 347 – 348 respectivamente	Prisión de 1 a 4 años y multa de 10 a 100 salarios mínimos.
		Injuria – Injuria por vía de hecho	Código penal - Articulo 220 - 226	Prisión de 1 a 3 años
		Calumnia	Código penal - Articulo 221	Prisión de 1 a 4 años
		Injuria y calumnia indirectas	Código penal – Artículo 222	
		Circunstancias especiales de graduación de la pena.	Código Penal – Artículo 223. Inciso 1	Las penas respectivas se aumentarán de una sexta parte a la mitad.
		Circunstancias de mayor punibilidad: son circunstancias de mayor	Código penal - Artículo 58.	

[13] Amenaza: Es un cualquier acto por el cual un individuo, sin motivo legítimo y sin pasar por los medios o por el fin a otro delito, afirma deliberadamente que quiere causarle a otra persona algún mal futuro. Se dice *cualquier acto*, porque la fuerza física subjetiva de este delito no exige especiales condiciones materiales, y es indiferente la naturaleza del acto, con tal que sea idóneo para infundir temor o expresar la idea de peligro. ARBOLEDA VALLEJO, MARIO. Código penal y de procedimiento penal básico. Vigésima octava edición. Leyer. Bogotá. Página 212

		punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.	Numerales 3 y 17	
Trickery	El Trickery, supone tratar de ganarse la confianza de una persona para que revele secretos o información embarazosa o cualquier clase de información que el acosador luego publicará online.	Injuria – Injuria por vía de hecho	Código penal - Articulo 220 - 226	Prisión de 1 a 3 años
		Calumnia	Código penal - Articulo 221	Prisión de 1 a 4 años
		Injuria y calumnia indirectas	Código penal – Artículo 222	
		Circunstancias especiales de graduación de la pena.	Código Penal – Artículo 223. Inciso 1	Las penas respectivas se aumentarán de una sexta parte a la mitad.
		Espionaje	Código penal – Artículo 463	Prisión de 4 a 12 años
		Utilización indebida de información obtenida en el ejercicio de función pública	Código penal – Artículo 431	Multa
		Pánico económico	Código penal – Artículo 302	Prisión de 2 a 8 años y multa de 50 a 500 smmlv
		Circunstancias de mayor punibilidad: son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.	Código penal - Artículo 58. Numerales 3 y 17	
Packs	El concepto de 'pack' hoy en día en redes sociales se refiere a un paquete de archivos digitales (fotos y/o vídeos) de una persona, la cual se puede mostrar desnuda(o) o con contenido sugestivo (sexual).	Pornografía con personas menores de 18 años	Código penal - Articulo 218 modificado por la ley 1336 del 2009	10 a 20 años y multa de 150 a 1.500 salarios mínimos
		Utilización o facilitación de medios de comunicación para ofrecer servicios	Ley 1329 de 2009	Prisión de 10 a 14 años

		sexuales de menores 18 años		
		Violación de datos personales	LEY 1273 de 2009 -Articulo 269F	Prisión de 48 a 96 meses y multa de 100 a 1.000 salarios mínimos vigentes
		Injuria – Injuria por vía de hecho	Código penal - Articulo 220 - 226	Prisión de 1 a 3 años
		Circunstancias especiales de graduación de la pena.	Código Penal – Artículo 223. Inciso 1	Las penas respectivas se aumentarán de una sexta parte a la mitad.
		Circunstancias de mayor punibilidad: son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.	Código penal - Artículo 58. Numerales 3 y 17	
Proxenetismo por redes sociales (Proxenetwork)	La inducción a la prostitución, requiere que el sujeto activo tenga la intención de lucro o de satisfacer los deseos de otro, y que con tal interés induzca al comercio carnal o a la prostitución a otra persona a través de redes sociales.	Inducción a la prostitución	Código Penal – Artículo 213- Modificado por el art. 8, ley 1236 de 2008.	Prisión de nueve (9) a trece (13) años y multa de sesenta y seis (66) a setecientos cincuenta (750) salarios mínimos legales mensuales vigentes
		Proxenetismo con menor de edad – Circunstancias de agravación punitiva	Código Penal – Artículo 216- Modificado por el art. 10, ley 1236 de 2008.	Las penas para los delitos descritos en los artículos anteriores, se aumentarán de una tercera parte a la mitad
		Pornografía con personas menores de 18 años	Ley 1329 de 2009	Prisión de 10 a 20 años

		Circunstancias de mayor punibilidad: son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera: Numeral 17. Adicionado por la Ley 1273 de 2009, art 2. Cuando la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.	Código penal - Artículo 58. Numerales 3 y 17	

Ahora bien, en la actualidad todos los ataques o conductas que se llevan a cabo por medios electrónicos, particularmente a través de las redes sociales se catalogan dentro del concepto de delitos informáticos, sin embargo, hay que tener en cuenta que para que sea catalogado como tal debe estar consignado en el código penal o en la ley, así las cosas, teniendo en cuenta el concepto dado en el libro Derecho del comercio electrónico y de internet, "Los delitos informáticos son aquellas actividades que si bien encuadran dentro los delitos tipificados tradicionalmente y reconocidos por nuestro ordenamiento jurídico por medio de nuestro Código Penal, cabe resaltar que a este tipo de delitos se les ha definido de esta manera por la única razón que son realizados a través de redes, medios electrónicos o similares." [14]

De lo cual se puede establecer que, existen algunos ataques que, aunque aún no están tipificados como delitos dentro de la ley de delitos informáticos, se consideran como tal toda vez que usan a los computadores como medio o fin. En razón a ello, la presente investigación hace una clara distinción entre estas dos situación, pues así se detalló en las tablas anteriores, en donde se identifican aquellas conductas que si están tipificadas como delitos informáticos por la Ley 1273 de 2009, ley que modifica el Código Penal creando como nuevo bien jurídico tutelado el denominado "*de la protección de la información y de los datos*" [15], como respuesta a la necesidad de proteger a la sociedad de los ataques cibernéticos a partir del uso intensivo de las tecnologías. Esta Ley tipifica las siguientes conductas como delitos informáticos incluyendo las circunstancias de agravación punitiva así:

> "Artículo 269A: Acceso abusivo a un sistema informático; Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación; Artículo 269C: Interceptación de datos informáticos; Artículo 269D: Daño Informático; Artículo 269E: Uso de software malicioso; Artículo 269F: Violación de datos personales; Artículo 269G: Suplantación de sitios web para capturar datos personales; Artículo 269H: *Circunstancias de agravación punitiva*.; Artículo 269I: *Hurto por medios informáticos y semejantes*.; Artículo 269J: *Transferencia no consentida de activos*."[16]

[14] RINCÓN CÁRDENAS, E., 2015. *Derecho del comercio electrónico y de internet* [en línea]. Segunda ed. Bogotá: Legis. [Consulta: 23 enero 2018]. ISBN 9789587672497. Disponible en: http://biblioteca.iucesmag.edu.co/pmb/opac_css/index.php?lvl=notice_display&id=19080.
[15] CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2009a. Ley 1273 de 2009. *Diario Oficial 47.223 de enero 5 de 2009* [en línea]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
[16] Ibíd.

Esta Ley tiene como antecedentes ciertos instrumentos internacionales importantes que brindan soporte y representan un marco general para su promulgación, como lo es la Cumbre de Túnez, el Convenio de Budapest, la clasificación de los delitos informáticos realizados por la Organización de las Naciones Unidas, Decisión 587 de la Comunidad Andina, Resolución 64/25 de la Asamblea General de las Naciones Unidas, entre otros.

Por parte, en la segunda tabla se describen aquellas conductas que se presentan con ocasión de la utilización de las redes sociales pero que si bien no están en la ley como delitos informáticos, si desencadenan otras conductas punibles consagradas en el Código Penal General (Ley 599 de 2000) [17] y las circunstancias de agravación punitiva, por ejemplo: Amenaza, Instigación a delinquir (inciso 1), Injuria – Injuria por vía de hecho, Calumnia, Injuria y calumnia indirectas, Circunstancias especiales de graduación de la pena, Pornografía con personas menores de 18 años, Utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores 18 años, entre otros (ver tabla 2).

Todos estos nuevos fenómenos sociales que se han presentado con el uso de las TIC, ha exigido que el Derecho deba ir evolucionando en la medida en que dichos fenómenos así lo requieran y más aún cuando la disciplina del Derecho debe velar por la protección y tutela de los derechos de una sociedad, sin embargo, en el caso de los ataques cibernéticos no alcanzan a ser regulados por completo por la ley, por cuanto cada vez los delincuentes encuentran la manera de evadirla y así cometer dichos ataques, generando algunos vacíos en la norma que no permiten adecuar las acciones cometidas u omitidas a una conducta punible clara.

En Colombia, se han expedido otras disposiciones legales cuyo propósito es proteger a los ciudadanos y prevenir este tipo de delitos, no obstante, continúan los vacíos en las normas, entre leyes promulgadas se destacan:

> Ley 679 de 2001, "busca prevenir y contrarrestar la explotación, la pornografía, el turismo sexual y más formas de abuso sexual con menores de edad mediante normas de carácter preventivo y sancionatorio. Se prohíbe alojar en los servidores imágenes, videos o cualquier contenido de tipo sexual." [18]

> Ley 1146 de 2007, referente a la "prevención de la violencia sexual y atención integral a niños, niñas y adolescentes contra cualquier forma de coerción física, psicológica o moral aprovechando condiciones de indefensión, poder entre víctima y agresor." [19]

[17] CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2000. Ley 599 de 2000 - Código Penal. *DIARIO OFICIAL N°:44097* [en línea]. [Consulta: 25 enero 2018]. Disponible en: http://legal.legis.com.co/document/legcol/legcol_75992041a9f8f034e0430a010151f034/ley-599-de-2000-ley-599-de-2000?text=articuloprincipal_$norma$%7Cley 599 de 2000 articulo 1%7C%7Carticulo_$norma$%7Cley 599 de 2000 articulo 1&type=qe&hit=1.

[18] CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2001. LEY 679 DE 2001. *Diario Oficial 44.509 de agosto 3 de 2001* [en línea]. Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_0679_2001.htm.

[19] CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2007. LEY 1146 DE 2007. *DIARIO OFICIAL N°:46685 DE JULIO 10 DE 2007* [en línea]. [Consulta: 25 enero 2018]. Disponible en: http://legal.legis.com.co/document/legcol/legcol_759920423519f034e0430a010151f034/ley-1146-de-julio-10-de-2007-ley-1146-de-2007?text=articuloprincipal_$norma$%7Cley 1146 de 2007 articulo 1%7C%7Carticulo_$norma$%7Cley 1146 de 2007 articulo 1&ty.

Ley 1236 de 2008, modifica el Título IV del Código Penal "relativos a delitos de abuso sexual." [20]

Ley 1329 de 2009, modifica el Título IV del Código Penal con el fin de "contrarrestar la explotación sexual, comercial de niños, niñas y adolescentes." [21]

Ley 1336 DE 2009, por medio de la cual "se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes." [22]

Ley Estatutaria 1581 de 2012, dictan las disposiciones para la "protección de datos personales." [23]

Ley 1620 de 2013, crea el "Sistema Nacional de Convivencia Escolar y formación para el ejercicio de los Derechos Humanos, la Educación para la Sexualidad y la Prevención y Mitigación de la Violencia Escolar." [24]

Decreto 1377 de 2013 [25], por el cual se reglamenta parcialmente la Ley 1581 de 2012, en relación con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información entre otros.

De acuerdo con la identificación de delitos informáticos y conductas ilícitas que se cometen a través de las redes sociales, las cuales se relacionan en el presente artículo, será posible determinar cuáles son las estrategias de prevención y corrección sobre las posibles consecuencias que se presentan cuando los ciberdelincuentes lanzan sus ataques, dichas estrategias serán de forma técnica, así como también de concientización en el buen uso de las redes sociales por parte de los usuarios.

CONCLUSIONES

Dado el uso masivo de las tecnologías las personas están siempre en un constante riesgo de ser potenciales víctimas de los delitos informáticos expuestos y los que a futuro se puedan presentar con motivo del avance vertiginoso de la tecnología.

Teniendo en cuenta que los ataques cibernéticos son cada vez más frecuentes y se realizan de diversas maneras con el fin de evadir la ley, el Estado debe procurar que sus leyes abarquen una gran cantidad de delitos con el fin de proteger la seguridad de los ciudadanos en el ciberespacio.

---

[20] CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2008. Ley 1236 de 2008. *DIARIO OFICIAL N°:47059* [en línea]. [Consulta: 25 enero 2018]. Disponible en: http://legal.legis.com.co/document/legcol/legcol_759920424b3cf034e0430a010151f034/ley-1236-de-julio-23-de-2008-ley-1236-de-2008?text=articuloprincipal_$norma$%7Cley 1236 de 2008 articulo 1%7C%7Carticulo_$norma$%7Cley 1236 de 2008 articulo 1&ty.

[21] CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2009a. Ley 1329 de 2009. *DIARIO OFICIAL N°:47413* [en línea]. [Consulta: 25 enero 2018]. Disponible en: http://legal.legis.com.co/document/legcol/legcol_759920426059f034e0430a010151f034/ley-1329-de-julio-17-de-2009-ley-1329-de-2009?text=articuloprincipal_$norma$%7Cley 1329 de 2009 articulo 1%7C%7Carticulo_$norma$%7Cley 1329 de 2009 articulo 1&ty.

[22] CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2009b. LEY 1336 DE 2009. *DIARIO OFICIAL N°:47417* [en línea]. [Consulta: 25 enero 2018]. Disponible en: http://legal.legis.com.co/document/legcol/legcol_759920426073f034e0430a010151f034/ley-1336-de-julio-21-de-2009-ley-1336-de-2009?text=articuloprincipal_$norma$%7Cley 1336 de 2009 articulo 1%7C%7Carticulo_$norma$%7Cley 1336 de 2009 articulo 1&ty.

[23] CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2012. *Ley Estatutaria 1581 De 2012*. 2012. S.l.: s.n.

[24] CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2013. Ley No 1620 Ley de Convivencia Escolar. 2013. S.l.: s.n.

25 PRESIDENCIA DE LA REPUBLICA, 2015. DECRETO 1377 DE 2013 [en línea]. 2015. S.l.: s.n. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646.

A través de las redes sociales no solo se pueden presentar conductas tipificadas como delitos informáticos sino también desencadenar otro tipo de conductas ilícitas reguladas por el código penal.

BIBLIOGRAFÍA

ARBOLEDA VALLEJO, M. y RUIZ SALAZAR, J.A., 2016. *Manual de derecho penal especial*. 13. Bogota D.C.: UniAcademia Leyer. ISBN 978-958-769-479-6.

AREVALO MUTIZ, PAULA LUCÍA; GARCÍA LEGUIZAMÓN, FERNANDO MAURICIO; NAVARRO HOYOS, JULIÁN ANTONIO; PARDO ARIAS, A., 2012. Aproximación a problemáticas jurídicas de las redes sociales virtuales. *Revista Virtual Universidad Católica del Norte* [en línea], pp. 62–92. [Consulta: 25 enero 2018]. Disponible en: http://www.redalyc.org/html/1942/194224568005/.

CENTRO CIBERNÉTICO POLICIAL, 2017. Amenazas del Cibercrimen en Colombia 2016-2017. [en línea]. Bogota D.C.: [Consulta: 26 enero 2018]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf.

CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2000. Ley 599 de 2000 - Código Penal. *DIARIO OFICIAL N°:44097* [en línea]. [Consulta: 25 enero 2018]. Disponible en: http://legal.legis.com.co/document/legcol/legcol_75992041a9f8f034e0430a010151f034/ley-599-de-2000-ley-599-de-2000?text=articuloprincipal_$norma$%7Cley 599 de 2000 articulo 1%7C%7Carticulo_$norma$%7Cley 599 de 2000 articulo 1&type=qe&hit=1.

CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2001. LEY 679 DE 2001. *Diario Oficial 44.509 de agosto 3 de 2001* [en línea]. Disponible en: https://www.icbf.gov.co/cargues/avance/docs/ley_0679_2001.htm.

CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2007. LEY 1146 DE 2007. *DIARIO OFICIAL N°:46685 DE JULIO 10 DE 2007* [en línea]. [Consulta: 25 enero 2018]. Disponible en: http://legal.legis.com.co/document/legcol/legcol_759920423519f034e0430a010151f034/ley-1146-de-julio-10-de-2007-ley-1146-de-2007?text=articuloprincipal_$norma$%7Cley 1146 de 2007 articulo 1%7C%7Carticulo_$norma$%7Cley 1146 de 2007 articulo 1&ty.

CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2008. Ley 1236 de 2008. *DIARIO OFICIAL N°:47059* [en línea]. [Consulta: 25 enero 2018]. Disponible en: http://legal.legis.com.co/document/legcol/legcol_759920424b3cf034e0430a010151f034/ley-1236-de-julio-23-de-2008-ley-1236-de-2008?text=articuloprincipal_$norma$%7Cley 1236 de 2008 articulo 1%7C%7Carticulo_$norma$%7Cley 1236 de 2008 articulo 1&ty.

CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2009a. Ley 1329 de 2009. *DIARIO OFICIAL N°:47413* [en línea]. [Consulta: 25 enero 2018]. Disponible en: http://legal.legis.com.co/document/legcol/legcol_759920426059f034e0430a010151f034/ley-1329-de-julio-17-de-2009-ley-1329-de-2009?text=articuloprincipal_$norma$%7Cley 1329 de 2009 articulo 1%7C%7Carticulo_$norma$%7Cley 1329 de 2009 articulo 1&ty.

CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2009b. LEY 1336 DE 2009. *DIARIO OFICIAL N°:47417* [en línea]. [Consulta: 25 enero 2018]. Disponible en: http://legal.legis.com.co/document/legcol/legcol_759920426073f034e0430a010151f034/ley-1336-de-julio-21-de-2009-ley-1336-de-2009?text=articuloprincipal_$norma$%7Cley 1336 de 2009 articulo 1%7C%7Carticulo_$norma$%7Cley 1336 de 2009 articulo 1&ty.

CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2012. *Ley Estatutaria 1581 De 2012*. 2012. S.l.: s.n.

CONGRESO DE LA REPÚBLICA DE COLOMBIA, 2013. *Ley No 1620 Ley de Convivencia Escolar*. 2013. S.l.: s.n.

OJEDA PÉREZ, J.E., RINCÓN RODRÍGUEZ, F., ARIAS FLÓREZ, M.E. y DAZA MARTÍNEZ, L.A., 2010. Delitos informáticos y entorno jurídico vigente en Colombia. *Computer crime and*

current legislation in Colombia. [en línea], vol. 11, no. 28, pp. 41–66. ISSN 01231472. Disponible en: http://search.ebscohost.com/login.aspx?direct=true&db=fua&AN=59522387&lang=es&site=ehost-live.

PRESIDENCIA DE LA REPUBLICA, 2015. *DECRETO 1377 DE 2013* [en línea]. 2015. S.l.: s.n. Disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646.

REVELO, L.C., 2011. *Guía de seguridad para prevenir y controlar delitos informáticos*. Pasto - Colombia: Institucion Universitaria CESMAG.

RICO CARRILLO, M., 2012. El impacto de Internet y las redes sociales en el derecho a la libertad de expresión. *Revista de filosofia juridica, social y politica FRONESIS* [en línea], vol. 19, no. 3, pp. 331–349. Disponible en: http://dspace.uah.es/dspace/handle/10017/6439.

RINCÓN CÁRDENAS, E., 2015. *Derecho del comercio electrónico y de internet* [en línea]. Segunda ed. Bogotá: Legis. [Consulta: 23 enero 2018]. ISBN 9789587672497. Disponible en: http://biblioteca.iucesmag.edu.co/pmb/opac_css/index.php?lvl=notice_display&id=19080.

RODRÍGUEZ ARBELÁEZ, J.D., 2011. Análisis de los delitos informáticos presentes en l as redes sociales en Colombia para el año 2011 y su regulación. [en línea]. [Consulta: 22 enero 2018]. Disponible en: http://bdigital.ces.edu.co:8080/repositorio/handle/10946/1334.

TÉLLEZ VALDÉS, J., 2009. *Derecho informático*. Cuarta edi. México, D. F.: McGraw-Hill. ISBN 978-970-10-6964-6.

EL CONVENIO ARBITRAL ELECTRÓNICO

Por: ***Ericka Edith Estrada Saavedra***
Panamá

1. Introducción.

El arbitraje es uno de los métodos alternos de solución de conflictos, que consiste en someter las partes sus diferencias a raíz de un contrato, a un tribunal arbitral, compuesto por uno o más árbitros que decidirán conforme a derecho o equidad, según lo hayan pactado las partes.

El mundo de los negocios ha encontrado una forma alternativa, facultativa, electiva de solucionar los conflictos. El arbitraje, que emergió desde tiempos antiguos,[1] ha venido popularizándose con el pasar del tiempo y con el devenir de los negocios tanto en la esfera doméstica[2] como a nivel internacional.[3]

En arbitraje prima la voluntad de las partes. ¿De qué manera se exterioriza dicha voluntad? ¿Cómo pactan las partes un arbitraje? El convenio arbitral es el instrumento por el cual las partes manifiestan su voluntad de resolver sus conflictos mediante arbitraje[4], la forma es el "medio con el cual la voluntad contractual debe exteriorizarse para alcanzar plena validez y eficacia."[5]

En lo que respecta a la forma, la Ley 131 de 31 de diciembre de 2013, Ley de Arbitraje de Panamá – en adelante LAP-, adoptó las reformas contenidas en el artículo 7 de la Ley Modelo de Arbitraje de la CNUDMI[6] - en adelante LMA-, opción 1. Según el artículo 16[7] de la LAP, la forma que puede adoptar el acuerdo de arbitraje es prácticamente libre para las partes, entendiéndose que éste deberá constar por escrito, pero no limitado al sentido tradicional de lo escrito, sino también en un sentido más amplio y moderno, adaptándose a la actualidad del mundo de los negocios.[8]

---

[1] Según nuestras investigaciones, el texto más antiguo que refiere a Arbitraje y al Convenio Arbitral, está en La Biblia, Libro de Éxodo, Capítulo 18, versículos 15 y16, versión Reina Valera, 1960, que dice "Y Moisés respondió a su suegro: Porque el pueblo viene a mí para consultar a Dios. Cuando tienen asuntos, vienen a mí; y yo juzgo entre el uno y el otro, y declaro las ordenanzas de Dios y sus leyes." En un lenguaje más actual, el mismo pasaje bíblico dice lo siguiente: "Moisés contestó: -Porque el pueblo acude a mí en busca de resoluciones de parte de Dios. Cuando les surge un desacuerdo, ellos acuden a mí, y yo soy quien resuelve los casos entre los que están en conflicto. Mantengo al pueblo informado de los decretos de Dios y le transmito sus instrucciones."
los años 1400 o 1500 a.C., en la época de Moisés.

[2] El artículo 3 de la LAP establece que el arbitraje será nacional si el tribunal tiene su sede dentro del territorio de la República de Panamá y el arbitraje no se enmarca dentro de ninguno de los supuestos mencionados en el artículo 2.

[3] El artículo 2 de la LAP establece que el arbitraje será internacional cuando las partes en un acuerdo de arbitraje tienen, al momento de la celebración de ese acuerdo, sus establecimientos en Estados diferentes, o cuando uno de los lugares siguientes está situado fuera del Estado en el que las partes tienen sus establecimientos: 1. La sede del arbitraje, si este se ha determinado en el acuerdo de arbitraje o con arreglo al acuerdo de arbitraje; 2. El lugar del cumplimiento de una parte sustancial de las obligaciones de la relación comercial o el lugar con el cual el objeto del litigio tenga una relación más estrecha. También el arbitraje será internacional cuando las partes han convenido expresamente en que la cuestión objeto del acuerdo de arbitraje está relacionada con más de un Estado; o cuando la materia objeto del arbitraje implica prestaciones de servicios, enajenación o disposición de bienes o transferencia de capitales que produzcan efectos transfronterizos o extraterritoriales. Si alguna de las partes tienen más de un establecimiento este será el que guarde una relación más estrecha con el acuerdo de arbitraje. Si una parte no tiene ningún establecimiento, se tomará en cuenta su residencia habitual.

[4] éste será determinante para el éxito del procedimiento, de principio a fin.

[5] PERALES VISCASILLAS, Pilar, Derecho Comercial Internacional, Tomo II, Editorial Temis, 2014, pág. 369.

[6] La Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI) es un órgano subsidiario de la Asamblea General. Prepara textos legislativos internacionales para ayudar a los Estados a modernizar el derecho mercantil y textos no legislativos para facilitar las negociaciones entre las partes en operaciones comerciales.

[7] El cual transcribimos más adelante."

[8] Reconoce la CNUDMI en Resolución aprobada por la Asamblea General 61/33 de 4 de diciembre de 2006[8] la necesidad que las nuevas disposiciones de la Ley Modelo en lo relativo a la forma del acuerdo arbitral se ajusten a las prácticas actuales

En un mundo donde la tecnología avanza a un ritmo acelerado, el uso del comercio electrónico es cada vez más frecuente. Un reciente estudio de la Comisión Económica para América Latina y el Caribe –CEPAL-, reveló el fuerte aumento en el uso y el acceso a Internet en el último quinquenio.[9] Otro estudio[10] señaló que un 38% de los internautas panameños han comprado alguna vez en línea, un importante indicador frente al 42% promedio de América Latina. Hoy, es muy común encontrarnos con contratos celebrados electrónicamente. Contratos mercantiles como el de transporte marítimo, compraventa de productos o servicios, entre muchos otros ejemplos, podrían incluir un convenio arbitral en su clausulado.

No pretendemos entrar a analizar cada uno de los contratos mercantiles mencionados como ejemplo[11], sino, que nos centraremos en el análisis del convenio arbitral electrónico y su surgimiento a la vida jurídica sujeto al cumplimiento de los requisitos de forma contenidos en la LAP y en los Convenios Internacionales suscritos por Panamá.

2. Marco Jurídico de referencia.

2.1. La Constitución Política de la República de Panamá.

Para comprender el origen del arbitraje es necesario tener presente que la jurisdicción arbitral nace en la Constitución Política, que en su Título VII, artículo 202, establece que la administración de justicia podrá ser ejercida, además del Órgano Judicial, por la jurisdicción arbitral de conformidad con la ley. Esto quiere decir, que la posibilidad de utilizar el arbitraje para dirimir controversias viene de la Carta Magna, que otorga y garantiza a los ciudadanos plena libertad para decidir sobre una u otra jurisdicción, lo que en esencia constituye la voluntad de las partes, pilar fundamental del arbitraje. Por defecto, todas las controversias deberán resolverse por medio de la jurisdicción ordinaria, esto es, mediante el Órgano Judicial, conformado por la Corte Suprema de Justicia, los tribunales y los juzgados que la ley establezca. La propia Constitución establece en su artículo 201 que la administración de Justicia es gratuita, expedita e ininterrumpida. Ahora bien, la realidad es que la Justicia ordinaria no marcha, ni en Panamá, ni en la mayoría de los países de la región, al ritmo y en la forma deseada o requerida en el día a día de los negocios, los cuales son muy dinámicos. Es por esto que existen los métodos alternos de solución de conflictos, como el arbitraje.

La pregunta ahora sería, ¿cómo activar nuestro derecho a acudir a la denominada justicia privada? La respuesta corta es, con un acuerdo de voluntades. La jurisdicción arbitral quedará siendo una herramienta latente para dirimir controversias mientras no exista la voluntad de dos o más personas que se encuentran ligados por una relación comercial y que, han determinado que, frente a una controversia pasada, presente o futura, someterán el asunto a arbitraje.

---

del comercio internacional y a los medios modernos de concertación de contratos; señala estar convencida de que tal modernización es oportuna para la promoción de una interpretación y aplicación uniformes de la Convención sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras, hecha en Nueva York el 10 de junio de 1958; considerando que las reformas fueron ampliamente discutidas con los gobiernos e interesados y que contribuirá al establecimiento de un marco jurídico armonizado que permita resolver de forma equitativa y eficiente las controversias comerciales internacionales.

[9] El 43,4% del total de los hogares estaban conectados a Internet en 2015, casi duplicando el valor de 2010, indica el informe Estado de la banda ancha 2016 presentado en el marco de la segunda reunión de la Conferencia de Ciencia, Innovación y TIC en Costa Rica. Ver https://www.cepal.org/es/publicaciones/estado-la-banda-ancha-america-latina-caribe-2016

[10] Firma consultora Tendencias Digitales http://tendenciasdigitales.com/evolucion-usos-de-internet-latam/ https://impresa.prensa.com/economia/consolida-comercio-electronico-Panama_0_4858764163.html

[11] por el principio de autonomía del convenio arbitral, también llamado principio de separabilidad, éste puede ser analizado separadamente del contrato principal.

2.2. Ley 131 de 31 de diciembre de 2013, de Arbitraje Comercial Nacional e Internacional de Panamá -LAP-.

La ley 131 de 31 de diciembre de 2013, que regula el Arbitraje Comercial Nacional e Internacional en Panamá, derogó el Título I del Decreto Ley 5 de 8 de julio de 1999, que establecía el régimen del Arbitraje Comercial Nacional e Internacional. El Decreto ley 5 de 1999, seguía el diseño de la Ley Modelo de Arbitraje de la CNUDMI. El convenio arbitral estaba revestido de la solemnidad escrita y requería la firma de las partes en aceptación.[12]

Según el derogado Decreto ley 5, la constancia por escrito era un requisito indispensable para la existencia y validez del convenio arbitral. La voluntad de las partes debía evidenciarse de forma inequívoca en el convenio arbitral, lo que se conoce como el principio de interpretación estricta, el cual tiene su base en la concepción del acuerdo arbitral como excepción a la regla general, cual es la justicia ordinaria.[13] En la medida en que dicho pacto es una excepción a una regla general, le aplica el principio *exceptio est strictissimae interpretationis.* Como resultado, el texto del acuerdo arbitral y su alcance, serían interpretados como regla a la excepción.

Bajo el principio de interpretación estricta de la cláusula arbitral, el sistema[14] presentó algunos inconvenientes en tanto que se cuestionaba la validez del acuerdo arbitral, principalmente por aquella parte afectada por el resultado del laudo, la cual trataba de invalidarlo, so pretexto de que no se cumplió a cabalidad la voluntad de las partes. No bastaba con que el acuerdo estuviera por escrito, sino que el mismo debía expresar lo pactado por las partes de forma indubitable. Cualquier inconsistencia de interpretación abría una ventana para alegar una causal de anulación del laudo.[15] Aparentemente tal rigidez ya no estaba acorde con los usos del comercio en la actualidad, razón por la cual la CNUDMI comenzó a mirar el asunto de cerca e introdujo las reformas a la Ley Modelo de Arbitraje en el año 2006.

Como mencionamos en el punto 1, de los aspectos generales, la nueva LAP adoptó las recientes reformas de la Ley Modelo -LMA[16], resultando una ley moderna, cuyo contenido es apto para promover el arbitraje tanto en el ámbito doméstico como en el internacional. El concepto de acuerdo

[12] En relación a la forma del convenio arbitral, el artículo 9 del Decreto Ley 5 de 1999, establecía que: "el convenio arbitral deberá constar por escrito. Se entenderá que adopta la forma escrita cuando conste en un documento firmado por ambas partes, o en documento intercambiado entre las partes por medio de télex, fax, correo electrónico o cualquier otra forma de comunicación que acredite la voluntad inequívoca de las partes."

[13] Por el derecho de todo ciudadano de acudir a la Administración de Justicia ejercida por el Órgano Judicial a través de la Corte Suprema de Justicia, los Juzgados y los Tribunales que la Ley establezca, consagrado en el Título VII, Capítulo 1, de la Constitución Nacional de Panamá.

[14] Para referirme al arbitraje como un todo, como sistema de solución de conflictos.

[15] El artículo 34 (derogado) del Decreto Ley 5 de 1999 establecía en cuanto a la impugnación del laudo arbitral: Artículo 34. Contra el laudo arbitral interno sólo podrá interponerse el recurso de anulación, por los siguientes motivos tasados: 1. Cuando la parte que interpone el recurso pruebe: a) Que el convenio arbitral estaba viciado por alguna de las causas de nulidad consagradas en el Código Civil y las causales contenidas en los convenios internacionales que la República de Panamá haya ratificado sobre la materia. b) Que la constitución del tribunal arbitral, el desarrollo del procedimiento arbitral o la emisión del laudo, no se ha ajustado al acuerdo celebrado entre las partes o de conformidad con lo establecido en el presente Decreto-Ley, o no ha sido una de las partes notificada en debida forma de la iniciación del arbitraje o de cualquier trámite del procedimiento. c) Que el laudo se refiere a una controversia no contenida en el convenio arbitral, o que contiene decisiones que exceden de su ámbito o alcance. d) Si el laudo se hubiere obtenido en virtud de violencia, cohecho o prevaricato. Parágrafo: la anulación afectará únicamente a las cuestiones a que se refiere los párrafos anteriores que se puedan separar de las demás contenidas en el laudo. 2 Que el tribunal compruebe que el objeto de la controversia no es arbitrable conforme a la ley panameña, o que el laudo es contrario al orden público panameño.

[16] No solamente en lo que a cláusula arbitral se refiere, sino también adoptó las reformas relativas a medidas cautelares,

de arbitraje quedó plasmado en el artículo 15 tomando como referencia el párrafo 1 de la Opción 1, de las dos que ofrecía la CNUDMI.[17]

> "Artículo 15. DEFINICIÓN Y FORMA DEL ACUERDO DE ARBITRAJE. El acuerdo de arbitraje es aquel por medio del cual las partes deciden someter a arbitraje todas las controversias o ciertas controversias que hayan surgido o puedan surgir entre ellas respecto de una determinada relación jurídica, contractual o no contractual. El acuerdo de arbitraje podrá adoptar la forma de una cláusula compromisoria incluida en un contrato o la forma de un acuerdo independiente."

El artículo 16 de la LAP describe los requisitos de forma del Acuerdo de Arbitraje, como sigue:

> "Artículo 16. **Requisitos de forma del acuerdo de arbitraje. El Acuerdo de arbitraje deberá constar por escrito. Se entenderá que el acuerdo de arbitraje es escrito cuando quede constancia de su contenido en cualquier forma, ya sea que el acuerdo de arbitraje o contrato se haya concertado verbalmente, mediante la ejecución de ciertos actos o por cualquier otro medio. El requisito de que un acuerdo de arbitraje conste por escrito se cumplirá con una comunicación electrónica o mensajes de datos, según lo previsto en el artículo 5, si la información en ella consignada es accesible para su ulterior consulta.** También se considerará que hay constancia escrita, cuando haya un intercambio de escritos de demanda y contestación, en los que la existencia de un acuerdo sea afirmada por una parte sin ser negada por la otra. La referencia hecha en un contrato a un documento que contenga una cláusula compromisoria constituye un acuerdo de arbitraje por escrito, siempre que dicha referencia implique que esa cláusula forma parte del contrato." (Lo resaltado es nuestro)

Centraremos nuestra atención en la modalidad de acuerdo arbitral concertado por medios electrónicos, y expondremos las razones por las cuales consideramos que es totalmente válido a la luz de los requisitos de forma contenidos en el artículo 16, aunados a los requerimientos de los convenios internacionales suscritos por nuestro país.

2.3. Los tratados internacionales en materia de arbitraje.

2.3.1. Convención de Nueva York de 1958 -CNY.

Panamá es País suscriptor[18] de la Convención sobre el reconocimiento y ejecución de las sentencias arbitrales extranjeras, también conocida como Convención de Nueva York, celebrada en esa Ciudad el 10 de junio de 1958.

La finalidad principal de la Convención es evitar que las sentencias arbitrales, tanto extranjeras como no nacionales, sean objeto de discriminación, por lo que obliga a los Estados parte a velar por que dichas sentencias sean reconocidas en su jurisdicción y puedan ejecutarse en ella, en general, de la misma manera que las sentencias o laudos arbitrales nacionales. Un objetivo secundario de la Convención es exigir que los tribunales de los Estados parte den pleno efecto a los acuerdos de

[17] La Opción II que ofrece la CNUDMI lee como sigue: Artículo 7. Definición del acuerdo de arbitraje (Aprobado por la Comisión en su 39º período de sesiones, celebrado en 2006) El "acuerdo de arbitraje" es un acuerdo por el que las partes deciden someter a arbitraje todas las controversias o ciertas controversias que hayan surgido o puedan surgir entre ellas respecto de una determinada relación jurídica, contractual o no.

[18] Aprobada mediante Ley 5 de 25 de octubre de 1983, publicada en Gaceta Oficial N°20,079 de 15de junio de 1984. Depósito del Instrumento de Adhesión el 10 de octubre de 1984. Entró en vigencia para Panamá el 8 de enero de 1985.

arbitraje negándose a admitir demandas en las que el demandante esté actuando en violación de un acuerdo de remitir la cuestión a un tribunal arbitral.[19]

El artículo II de la Convención de Nueva York a la letra dice:

> "Artículo II. 1. Cada uno de los Estados Contratantes reconocerá el acuerdo **por escrito** conforme al cual las Partes se obliguen a someter a arbitraje todas las diferencias o ciertas diferencias que hayan surgido o puedan surgir entre ellas respecto a una determinada relación jurídica, contractual o no contractual, concerniente a un asunto que pueda ser resuelto por arbitraje. 2. **La expresión "acuerdo por escrito" denotará una cláusula compromisoria incluida en un contrato o un compromiso, firmada por las Partes o contenidos en un canje de cartas o telegramas.** 3. El tribunal de uno de los Estados Contratantes al que se someta un litigio respecto del cual las Partes hayan concluido un acuerdo en el sentido del presente artículo, remitirá a las Partes al arbitraje, a instancia de una de ellas, a menos que comprueba que dicho acuerdo es nulo, ineficaz o inaplicable. (El énfasis es nuestro).

Las condiciones de "por escrito" y "firmado por las partes" de la cláusula arbitral parece ser vital para los efectos de la aplicación de la Convención de Nueva York. En teoría, los países miembros deberán ajustarse al texto de la norma antes transcrita, sin embargo, la realidad es que dicho precepto ha perdido vigencia en la actualidad, en tanto que no se adapta a la práctica actual del comercio y la intervención cada vez más frecuente de la tecnología y las comunicaciones electrónicas. Por esta y otras consideraciones, la CNUDMI recomendó[20] que el párrafo 2 del artículo II de la Convención de Nueva York se aplique **reconociendo que las circunstancias que describe no son exhaustivas.**

> Recomienda que el párrafo 2) del artículo II, de la Convención sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras, hecha en Nueva York el 10 de junio de 1958, **se aplique reconociendo que las circunstancias que describe no son exhaustivas;** 2. Recomienda que el párrafo 1) del artículo VII de la Convención sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales Extranjeras, hecha en Nueva York el 10 de junio de 1958, se aplique de forma que permita a toda parte interesada acogerse a los derechos que puedan corresponderle, en virtud de las leyes o los tratados del país donde se invoque el acuerdo de arbitraje, para obtener el reconocimiento de la validez de ese acuerdo de arbitraje.

Tratando de fusionar el párrafo 2 a la recomendación de interpretación de la CNUDMI, podríamos decir entonces que la expresión "acuerdo por escrito" denotará una cláusula compromisoria incluida en un contrato o un compromiso, firmada por las Partes o contenidos en un canje de cartas o telegramas, **aunque no totalmente.**[21]

2.3.2. Convención de Panamá de 1975.

La Convención Interamericana sobre Arbitraje Comercial Internacional, celebrada en 1975, tuvo nuestro País como sede, y por tanto lleva su nombre. Desarrolla temas como el Acuerdo Arbitral, nombramiento de árbitros, procedimiento arbitral, reconocimiento y ejecución de sentencias. Sobre el Acuerdo Arbitral contiene una redacción muy similar a la Convención de Nueva York. Establece en su artículo 1 "que es válido el acuerdo de las Partes en virtud del cual se obligan a someter a

[19] Tomado del texto de los objetivos de la Convención de Nueva York de 1958. Puede ser consultado en http://www.uncitral.org/uncitral/es/uncitral_texts/arbitration/NYConvention.html

[20] La recomendación relativa a la interpretación del párrafo 2) del artículo II y del párrafo 1) del artículo VII de la Convención de Nueva York, de 10 de junio de 1958, adoptada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional el 7 de julio de 2006 en su 39º período de sesiones.

[21] perfectamente, absolutamente, cabalmente, todos sinónimos de exhaustivamente.

decisión arbitral las diferencias que pudiesen surgir o que hayan surgido entre ellas con relación a un negocio de carácter mercantil. Así como la CNY, la Convención de Panamá menciona que el acuerdo de Arbitraje constará por escrito y deberá ser firmado por las Partes.

Dada la importancia de la comprensión adecuada del concepto de constancia por escrito, dedicaremos un punto especial para tratar este tema.3.

3. **Requisitos de validez del acuerdo arbitral.**

Toda vez que el convenio arbitral es un acto jurídico de carácter contractual, le son aplicables las reglas generales de dichos negocios.[22] Será necesario revisar los principios generales de los actos jurídicos contenidos en nuestro ordenamiento civil panameño, en conexión con la cláusula arbitral y así evaluar los requisitos de existencia y validez de la misma.

> Sobre la validez, el precepto citado como violado en la sentencia alude a la que pueda o no tener el contrato y esa referencia ha de ser entendida en relación con los elementos esenciales requeridos para la existencia de los contratos. Como se sabe esos elementos no son otros que el consentimiento de los contratantes, el objeto cierto, materia del contrato, y la causa de la obligación que se establezca.[23]

El Código Civil panameño en su artículo 1112 establece que para la validez de los contratos son requisitos esenciales:

1. El consentimiento de los contratantes,
2. El objeto cierto que sea materia del contrato, y
3. La causa de la obligación que se establezca.

La Corte Suprema de Justicia ha declarado que conforme al artículo anterior, se dispone taxativamente que hay nulidad absoluta en los actos o contratos cuando falta algún requisito o formalidad que la ley exige para el valor de ciertos actos o contratos, en consideración a la naturaleza del acto o contrato y no a la calidad o estado de la persona que en ellos interviene.[24]

3.1. El consentimiento.

El consentimiento no es más que la manifestación de la voluntad de las partes de celebrar un acto jurídico, lo cual implica una oferta por una de ellas y la aceptación por la otra.[25]
A propósito de los contratos consensuales y solemnes, el artículo 1109 del Código Civil Panameño establece la diferenciación entre uno y otro, como sigue:

> "Los contratos se perfeccionan por el mero consentimiento, y desde entonces obligan, no sólo al cumplimiento de lo expresamente pactado, sino también a todas las consecuencias que, según su naturaleza, sean conforme a la buena fe, al uso y a la ley.
> Se exceptúan los actos y contratos enumerados en el artículo 1131, los cuales no se perfeccionan mientras no consten por escrito, con especificación completa de las condiciones del acto o contrato y determinación precisa de la cosa que sea objeto de él."

[22] Entiéndase acto o negocio jurídico en el mismo sentido.
[23] Sentencia de 17 de abril de 2001, Sala Civil de la Corte Suprema de Justicia. Proceso Ordinario Carlos Eliseo Santana vs. Fernando Montes
[24] Ver comentarios a la Jurisprudencia (Sentencia de 17 de abril de 2001, Sala Civil de la Corte Suprema de Justicia. Proceso Ordinario Carlos Eliseo Santana vs. Fernando Montes) del artículo 1112 del Código Civil Panameño. Editorial Sistemas Jurídicos. 2009.
[25] Ver Artículo 1113 del Código Civil Panameño.

Se desprende de este artículo una regla general aunada a una excepción. Se trata de que los contratos son consensuales, a no ser que se encuentren dentro de aquéllos enumerados en el artículo 1131 del propio Código Civil, esto es: 1. La cesión o transmisión de bienes inmuebles, 2. Los arrendamientos de inmuebles mayores a seis años, 3. Las capitulaciones matrimoniales, 4. Cesión de derechos hereditarios, y 6. Cesión de derechos de un acto consignado en escritura pública.

El convenio arbitral no se encuentra dentro del listado del artículo 1131 del Código Civil, por tanto, no es un contrato solemne. Debemos remitirnos a la Ley de arbitraje comercial y a los convenios internacionales, para examinar si existe formalidad en lo que se refiere a la cláusula arbitral.

No podemos dejar de mencionar que las partes deberán estar en capacidad legal para prestar su consentimiento, de lo contrario sería causal de nulidad del acto jurídico. Asimismo el consentimiento prestado por error, violencia, intimidación o dolo anularán el acto.[26]

3.2. Objeto cierto.

Establece nuestro Código Civil que pueden ser objeto de contrato todas las cosas que no están fuera del comercio, las cosas o servicios posibles, todo lo cual debe ser determinado o determinable –de referirse a una cantidad-.[27] En el caso del convenio arbitral, el objeto es la o las controversias que puedan surgir por motivo de una determinada relación jurídica, que puede ser o no contractual. Hacemos énfasis en el hecho de que la relación jurídica debe ser específica, determinada o definida, y también debe ser susceptible de ser ventilada en un arbitraje.[28]

3.3. Causa lícita.

En un convenio arbitral la causa es la promesa[29] de ambas partes de acudir a un arbitraje para resolver sus conflictos. Es un elemento de validez de los actos jurídicos que se refiere a la causa final, la razón objetiva, es decir, lo que se quiere alcanzar con el contrato. Dicha causa no puede ir en contra de las leyes o la moral,[30] ya que perdería su condición de licitud, dando lugar a la nulidad.

La causa del convenio arbitral va necesariamente ligada a la arbitrabilidad que tratamos en el capítulo I. Así, de pactarse un arbitraje sobre una cuestión que deba ser ventilada ante entidades estatales, tal es el caso de las acciones penales, competencia económica, temas de propiedad industrial, entre otros, dicho acuerdo arbitral perdería eficacia o validez.

4. Requisitos de forma del convenio arbitral.

4.1. La constancia “por escrito”

Según el Diccionario de la Real Academia de la Lengua Española –Drae-, el término “por escrito” significa “por medio de la escritura.”[31] A su vez la palabra escritura nos refiere a un documento. La

[26] Ver artículos 1113 al 1121 del Código Civil Panameño.
[27] Ver artículos 1122 a 1124 del Código Civil Panameño.
[28] Nos referimos al artículo II párrafo 1 de la Convención de Nueva York de 1958.
[29] Ver artículos 1125 a 1128 del Código Civil Panameño.
[30] Ver artículo 1126 del Código Civil Panameño.
[31] Del lat. *scriptūra.* 1. f. Acción y efecto de escribir. 2. f. Sistema de signos utilizado para escribir. Escritura alfabética, silábica, ideográfica, jeroglífica. 3. f. Arte de escribir. 4. f. Carta, documento o cualquier papel escrito. 5. f. Documento público, firmado con testigos o sin ellos por la persona o personas que lo otorgan, de todo lo cual da fe el notario. 6. f. Obra escrita.

Ley 51 de 22 de julio de 2008[32], modificada por la Ley 82 de 9 de noviembre de 2012, Ley de Documentos, Firmas y Comercio Electrónico de Panamá, define documento como los "escritos, escrituras, certificaciones…" y documento electrónico como "toda representación electrónica que da testimonio de un hecho, una imagen, un sonido o una idea, con independencia del soporte utilizado para su fijación".

En arbitraje, el concepto de constancia por escrito ha sufrido una evolución a través del tiempo. El antiguo Decreto Ley 5 de 1999,[33] establecía, no únicamente que el acuerdo de arbitraje debía constar por escrito, sino que debía contener además dos requisitos mínimos, la designación o forma de designación de los árbitros, y las reglas de procedimiento o su indicación por remisión a un reglamento preestablecido. Tal disposición, un tanto restrictiva y formalista, parecía condicionar la validez del acuerdo arbitral a estos dos requisitos.[34] Rigió por catorce años, y aun cuando estaba en vigencia, la Corte Suprema de Justicia, aplicando el principio pro validez, reconoció "que dentro de la forma escrita para la concertación de acuerdos arbitrales dentro de la contratación comercial moderna se aceptan diversas modalidades sin que sea imperativa la autografía o firma de los contratantes, que no son esenciales para la existencia del contrato, pero que constituyen una de las modalidades más usadas hoy en día."[35] Consecuentemente declaró injustificado el cargo relativo a la falta de escritura de la cláusula arbitral.

Hoy, la realidad es distinta. La esencia de la forma escrita está ligada tanto al concepto de escritura tradicional, como al lenguaje tecnológico actual. La moderna LAP establece en los dos primeros párrafos del artículo 16, que "se entenderá que el acuerdo de arbitraje es escrito cuando quede constancia de su contenido en cualquier forma, ya sea que el acuerdo de arbitraje o contrato se haya concertado verbalmente, mediante la ejecución de ciertos actos o por cualquier otro medio. El requisito de que un acuerdo de arbitraje conste por escrito se cumplirá con una comunicación electrónica o mensaje de datos, según lo previsto en el artículo 5, si la información en ella consignada es accesible para su ulterior consulta."

Lo anterior es en definitiva innovador, y como toda innovación, podría sonar un tanto disonante. Podemos rescatar del texto dos frases[36] determinantes para su correcta comprensión: el acuerdo de arbitraje es escrito "cuando quede constancia de su contenido" y "si la información es accesible para

[32]Artículo 1. Objeto. Esta Ley establece el marco regulador para la creación, utilización y almacenamiento de documentos electrónicos y firmas electrónicas, así como el proceso de registro y la fiscalización de los prestadores de servicios de almacenamiento tecnológico de documentos y de certificación de firmas electrónicas en el territorio de la República de Panamá. Además, establece el marco regulador para algunos actos de comercio realizados a través de Internet, principalmente en lo referente a la información previa y posterior a la celebración de contratos electrónicos y a las condiciones relativa a la validez y eficacia de dichos contratos; las obligaciones y responsabilidades de los prestadores de servicios comerciales a través de Internet, incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de comunicación; el intercambio de información y documentación comercial por vía electrónica, incluidas las ofertas, las promociones y los concursos; y el régimen sancionador aplicable a los prestadores de servicios comerciales a través de medios electrónicos.

[33] Derogado por la Ley 131 de 31 de diciembre de 2013, que regula el Arbitraje Comercial Nacional e Internacional en Panamá.

[34]GONZÁLEZ ARROCHA, Katherine, SANCHEZ ORTEGA, Liliana. Arbitraje Comercial Internacional en Panamá: Marco Legal y Jurisprudencial. Pág. 5. Consultar en: http://www.cecap.com.pa/files/ARBITRAJE%20COMERCIAL%20INTERNACIONAL%20EN%20PANAMA.%20MARCO%20LEGAL%20Y%20JURISPRUDENCIAS.pdf

[35] Sentencia de Apelación, 1 de junio de 2005, la Sala Civil de la Corte Suprema de Justicia de Panamá. MAERSKS SEALAND TRADING NAME OF THE AP MOLLER GROUP DAMPSKIBSSELSKABET WERNDBORG contra el Auto No. 87 del 12 de mayo de 2003 dictado por el Segundo Tribunal Marítimo en el Proceso Ordinario Marítimo AGROWEST, S.A. DOS VALLES, S.A. Y COMEXA, S.A.

[36] Nótese que ambas son oraciones condicionales.

su ulterior consulta". El acuerdo de arbitraje podrá concertarse en cualquier forma, bajo la condición de que se deje constancia de su contenido.[37]

Según el artículo 5 de la LAP, comunicación electrónica es toda comunicación que las partes hagan por medio de mensajes de datos.[38] Mensaje de datos[39] es la información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares, como el intercambio electrónico de datos, el correo electrónico, el telegrama, el télex o el telefax, entre otros. Se aprecia la evolución con respecto a la normativa anterior y también de cara al artículo II.2 de la CNY, que únicamente hace referencia al canje de cartas o telegramas.[40] La jurisprudencia internacional ha reconocido la validez del acuerdo arbitral concertado mediante comunicaciones electrónicas.[41] La importancia de la nueva disposición radica en que ya no se exige la firma de las partes ni un intercambio de comunicaciones entre ellas.[42]

4.2. Accesibilidad de ulterior consulta.

El convenio arbitral electrónico es la modalidad del acuerdo arbitral concertado mediante comunicaciones electrónicas o mensajes de datos.

Según el artículo 5 de la ley de arbitraje, comunicación electrónica es toda comunicación que las partes hagan por medio de mensajes de datos. Mensaje de datos es la información generada, enviada, recibida o archivada por medios electrónicos, magnéticos, ópticos o similares, como el intercambio electrónico de datos, el correo electrónico, entre otros.

[37] Nota explicativa de la secretaría de la CNUDMI-Ley Modelo sobre Arbitraje Comercial Internacional, p.30.
[38] Tomado de la Convención de la CNUDMI sobre la utilización de las comunicaciones electrónicas, artículo 4b, c, Nueva York, 2005.
[39] Ver ley Modelo de la CNUDMI sobre comercio electrónico de 1996.
[40] Artículo II.2. La expresión acuerdo por escrito denotará una cláusula compromisoria incluida en un contrato o un compromiso, firmada por las partes yo contenidos en un canje de cartas o telegramas.
[41] "De esta forma, como criterio interpretativo, resulta de interés la recomendación relativa a la interpretación del párrafo 2 del art. II del CNY aprobada por la omisión de las Naciones Unidas para el Derecho Mercantil Internacional CNUDMI) de 7 de julio de 2006, conforme a la cual, considerando lo extendido del comercio y de las comunicaciones electrónicas, el art. II ha de interpretarse en el sentido de que los mecanismos allí recogidos no son exhaustivos sino que debe incluirse entre los medios aptos para acreditar el acuerdo, la comunicación electrónica. Lo que por otra parte admite ya el artículo 9.3 de la Ley de Arbitraje española. Así las cosas y en aplicación del anterior contexto normativo-jurisprudencial, es de reseñar que de la documentación acompañada en la demanda y la complementaria aportada en el escrito de alegaciones presentada por el instante, encontramos una serie de comunicaciones electrónicas mantenidas entre los intermediarios de "ELBANA" y de "BIOTRADING" con las partes contratantes. De este modo, en los correos electrónicos objeto de los documentos núms. 2, 17 y 21 acompañados por la actora (folios 14 al 17, 126 al 132 y 139 al 151, respectivamente), resulta con fuerza de evidencia no sólo la realización del contrato de fletamento entre las partes ahora en litigio y la intermediación del bróker de fletamentos "NOVA CHARTERING, SrL", llegándose a un acuerdo de "cierre" el día 5 de octubre de 2012, a las 16,36 horas, respecto del buque tanque FALESIA, para el transporte de 1.000 TM de biodiesel desde el puerto de Sevilla hasta el puerto de Génova, sino también que el referido contrato de fletamento quedó sujeto al derecho inglés y a arbitraje en Londres, como consta en cada uno de ellos. Así, "NOVA CHARTERING, SrL", con referencia a la póliza de fletamento MT FALESIA, de fecha 5 de octubre de 2012, confirma al armador ELBANA DI NAVIGAZIONE que: "El cierre contenía una cláusula de arbitraje a Londres y los términos de la póliza de fletamento Asbatankvoy, que contiene el clausulado completo de las cláusulas de arbitraje en Londres. Estos términos son ampliamente conocidos para todos los fletadores incluyendo Biotrading 2007, que regularmente fleta buques para el transporte de cargamentos líquidos y tenía sus propios términos y condiciones también incorporadas en el cierre". Y añade, además, tanto que "BIOTRADING" "confirmó su aceptación al cierre", como que "abonó el flete a los armadores" y "pagó la comisión de corretaje acordada". Solicitud de reconocimiento de laudo extranjero, ELBANA DE NAVIGAZIONE, SpA. Contra BIOTRADING 2007 SLNE. Sala de lo Civil y Penal del Tribunal Superior de Justicia de Cataluña. 2014.
[42] Ver nota explicativa de la secretaría de la CNUDMI-Segunda Parte- Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional Pág. 30.

Alguien definió comunicación electrónica como un servicio de transmisión a cambio de una remuneración o no, que consiste en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión.[43]

En los últimos años ha habido una revolución de los medios de comunicación. La gran mayoría de las personas utilizan medios electrónicos, canales digitales, aplicaciones, y todo un completo entorno cibernético que goza actualmente de gran popularidad y que continúa en desarrollo. Como ejemplo de la evolución tecnológica en cuanto a la mensajería de datos, los lectores recordarán las plataformas más populares de la década de los 90, que fueron el beeper, ICQ, SMS o mensajería instantánea usando datos móviles. Surge el *BlackBerry Messenger* y la posibilidad de mantener un intercambio de mensajes de forma ininterrumpida directa y simultánea, y esta a su vez actualizándose y abriendo un matiz de diferentes plataformas conocidas hoy (Telegram, WhatsApp, Criptext, entre otras). Una de las plataformas tecnológicas más utilizadas por los empresarios para llevar a cabo negociaciones a distancia, es Skype, creado en el año 2003, y cuyo servicio de mensajería tuvo buena acogida, en especial por la capacidad de este programa de redefinir las comunicaciones grupales por voz y video de forma gratuita.

Son tales los avances de la tecnología en nuestros días, que aún las reuniones hechas vía Skype o mediante alguna otra plataforma, pueden operar con realidad virtual 360°: Es una forma de representar la vida real de manera digitalizada**.** Es llevar aquello que nos rodea a imágenes que pueden verse en una pantalla de ordenador o en un *smartphone* y que van acompañadas de unas gafas especiales que hacen la visualización de las imágenes mucho más realistas. En dispositivos específicos como el HTC Vive, u Oculus Rift, puedes grabar en directo desde la tarjeta de video con una aplicación de Nvidia Geforce Experience. Lo que te permite tener acceso a la información, para futuras consultas.

En cuanto a la consulta de los documentos electrónicos o mensajería de datos, existen diversas maneras de obtener los datos para los efectos de comprobar la existencia del convenio arbitral, básicamente con programas o aplicaciones que manejados por técnicos idóneos será posible la consulta de tal archivo tecnológico.

La jurisprudencia internacional ha reconocido la validez del acuerdo arbitral concertado mediante una comunicación electrónica.

> "De esta forma, como criterio interpretativo, resulta de interés la recomendación relativa a la interpretación del párrafo 2 del art. II del CNY aprobada por la omisión de las Naciones Unidas para el derecho mercantil internacional CNUDMI) de 7 de julio de 2006, conforme a la cual, considerando lo extendido del comercio y de las comunicaciones electrónicas, el art. II ha de interpretarse en el sentido de que los mecanismos allí recogidos no son exhaustivos sino que debe incluirse entre los medios aptos para acreditar el acuerdo, la comunicación electrónica. Lo que por otra parte admite ya el artículo 9.3 de la Ley de Arbitraje española. Así las cosas y en aplicación del anterior contexto normativo-jurisprudencial, es de reseñar que de la documentación acompañada en la demanda y la complementaria aportada en el escrito de alegaciones presentada por la instante, encontramos una serie de comunicaciones electrónicas mantenidas entre los intermediarios de "ELBANA" y de "BIOTRADING" con las partes contratantes. De este modo, en los correos electrónicos objeto de los

[43] www.derecho.com/c/Comunicación electrónica

> documentos núms. 2, 17 y 21 acompañados por la actora (folios 14 al 17, 126 al 132 y 139 al 151, respectivamente), resulta con fuerza de evidencia no sólo la realización del contrato de fletamento entre las partes ahora en litigio y la intermediación del bróker de fletamentos "NOVA CHARTERING, SrL", llegándose a un acuerdo de "cierre" el día 5 de octubre de 2012, a las 16,36 horas, respecto del buque tanque FALESIA, para el transporte de 1.000 TM de biodiesel desde el puerto de Sevilla hasta el puerto de Génova, sino también que el referido contrato de fletamento quedó sujeto al derecho inglés y a arbitraje en Londres, como consta en cada uno de ellos.
> Así, "NOVA CHARTERING, SrL", con referencia a la póliza de fletamento MT FALESIA, de fecha 5 de octubre de 2012, confirma al armador ELBANA DI NAVIGAZIONE que: "El cierre contenía una cláusula de arbitraje a Londres y los términos de la póliza de fletamento Asbatankvoy, que contiene el clausulado completo de las cláusulas de arbitraje en Londres. Estos términos son ampliamente conocidos para todos los fletadores incluyendo Biotrading 2007, que regularmente fleta buques para el transporte de cargamentos líquidos y tenía sus propios términos y condiciones también incorporadas en el cierre". Y añade, además, tanto que "BIOTRADING" "confirmó su aceptación al cierre", como que "abonó el flete a los armadores" y "pagó la comisión de corretaje acordada" (folios 126 y 130)[44]

De igual forma, el Tribunal Superior de Justicia de Cataluña, en Sentencia de la Sala de lo Civil y de lo Penal, el 15 de marzo de 2012, señaló que era válida la cláusula arbitral concertada por medios electrónicos.

> La razón principal por la que se impugnaba la ejecución era la presunta inexistencia de un acuerdo escrito de arbitraje. En ese punto, el tribunal consideró que dicho argumento era incongruente con el contenido de los correos electrónicos intercambiados por las partes. El tribunal recordó la jurisprudencia establecida de España, conforme a la cual fue partidario de un enfoque antiformalista; es decir, se dio por entendido que el requisito previsto en la Convención de Nueva York de 1958 de que hubiese un documento escrito tenía como única finalidad que quedara constancia de que había un acuerdo. De manera análoga, se había adoptado un criterio interpretativo en la Recomendación2 de la CNUDMI relativa a la interpretación del artículo II, párrafo 2, de la CNY, en el sentido de que los mecanismos previstos en esa disposición no eran exhaustivos, por lo que debían incluir los medios electrónicos, lo que, además, se reconocía en el artículo 9 3) de la Ley de Arbitraje 60/2003, de 23 de diciembre de 2003. A ese respecto, el tribunal se refirió a los correos electrónicos intercambiados por las partes, en particular a aquellos en que se referían a condiciones ya acordadas de las relaciones comerciales anteriores y por los que se modificaban, complementaban o eliminaban algunas de ellas, pero no la cláusula 61 que contenía el acuerdo de someterse a arbitraje en Londres (London Maritime Arbitrators' Association (Asociación de Árbitros Marítimos de Londres) y a la legislación inglesa. Además, en uno de los correos electrónicos enviados por la parte que se oponía a la ejecución figuraba una referencia expresa al arbitraje, por lo que no cabía

[44] Solicitud de reconocimiento de laudo extranjero, ELBANA DE NAVIGAZIONE, SpA. Contra BIOTRADING 2007 SLNE. Sala de lo Civil y Penal del Tribunal Superior de Justicia de Cataluña. 2014.

invocar la inexistencia o el desconocimiento de una cláusula compromisoria.[45]

5. La firma en el convenio arbitral electrónico.

Bajo el antiguo Decreto Ley 5 de 1999, el convenio arbitral no sólo debía constar por escrito, sino que además, debía estar firmado por las partes, o en un documento en donde se acreditara la voluntad inequívoca de las mismas.[46] Esto fue abolido con la nueva LAP. El inconveniente aparente, no únicamente para Panamá, sino para todos los países que adoptaron la LMA, lo es la Convención de Nueva York de 1958 –CNY-, la cual establece el requerimiento de firma del convenio arbitral en su artículo II.2 - La expresión "acuerdo por escrito" denotará una cláusula compromisoria incluida en un contrato o un compromiso, firmada por las Partes o contenidos en un canje de cartas o telegramas. Para ello, la CNUDMI encontró una solución práctica: recomendar[47] que el párrafo 2 del artículo II de la CNY se aplique reconociendo que las circunstancias que describe no son exhaustivas. Las consideraciones registradas por la CNUDMI al hacer tal recomendación, fueron: 1. El extendido uso del comercio electrónico[48], y 2. La necesidad de promover el reconocimiento y ejecución de los laudos arbitrales.

El comercio electrónico, también conocido como *e-commerce*, está definido en la Ley de Documentos, Firmas y Comercio Electrónico de Panamá como toda forma de transacción o intercambio de información con fines comerciales en la que las partes interactúan utilizando Internet, en lugar de hacerlo por intercambio o contacto físico directo. Define firma electrónica como el método técnico para identificar a una persona y para indicar que esa persona aprueba la información que figura en un mensaje de datos o documento electrónico.[49] Bajo principios de neutralidad tecnológica, compatibilidad internacional y equivalencia funcional[50], dicha ley rige la prestación de servicios de almacenamiento tecnológico de documentos, de certificación de firmas electrónicas y de servicios de comercio a través de internet; reconoce la Ley el valor legal de los documentos electrónicos al dejar claramente establecido en su artículo 4, que "cuando la ley requiera que la información conste en un

[45] Caso 1418: CNY [II]; V 1) a); [V 2) b)]; Recomendación relativa a la interpretación del artículo II, párrafo 2) y del artículo VII, párrafo 1), de la CNY España: Tribunal Superior de Justicia de Cataluña (Sala de lo Civil y de lo Penal, sección 1ª) 15 de marzo de 2012 Original en español Resumen preparado por Pilar Perales Viscasillas, corresponsal nacional

[46] Siguiendo la versión original de la Ley Modelo de Arbitraje de la CNUDMI de 1985, de la disposición relativa a la definición y forma del acuerdo de arbitraje.

[47] Con base en la autoridad otorgada mediante la resolución 2205 (XXI) de la Asamblea General, de 17 de diciembre de 1966, por la que fue establecida la Comisión con el objeto de promover la armonización y unificación progresivas del derecho mercantil internacional, concretamente fomentando métodos y procedimientos para asegurar la interpretación y aplicación uniformes de las convenciones internacionales y de las leyes uniformes en el campo del derecho mercantil internacional.

[48]Teniendo en cuenta los instrumentos jurídicos internacionales, como la Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional de 1985, y sus revisiones posteriores, en particular con respecto al artículo 7, la Ley Modelo de la CNUDMI sobre Comercio Electrónico, la Ley Modelo de la CNUDMI sobre las Firmas Electrónicas, y la Convención de las Naciones Unidas sobre la Utilización de las Comunicaciones Electrónicas en los Contratos Internacionales

[49] Importante es diferenciar los conceptos de firma electrónica simple y firma electrónica calificada. Esta última está definida en el numeral 21 de la Ley 82 de 2012"21. Firma electrónica calificada. Firma electrónica cuya validez es respaldada por un certificado electrónico calificado que: a. Permite identificar al firmante y detectar cualquier cambio posterior de los datos firmados. b. Está vinculada al firmante de manera única y a los datos a que se refiere. c. Ha sido creada utilizando dispositivos seguros de creación de firmas electrónicas, los cuales mantiene el firmante bajo su control exclusivo. d. Ha sido creada a través de la infraestructura de un prestador de servicios de certificación registrado ante la Dirección Nacional de Firma Electrónica."

[50] El concepto legal de equivalencia funcional contemplado en el numeral 42 del artículo 2 de la Ley 82 de 9 de noviembre de 2012, que modifica la Ley 51 de 2008: "42. Equivalencia funcional: las actuaciones, trámites o documentos que se realicen a través de medios físicos o tradicionales se podrán desarrollar a través de medios electrónicos, con las mismas consecuencias jurídicas y probatorias."

documento escrito, se le reconocerá validez, efectos jurídicos y fuerza obligatoria a los actos, poderes y contratos y a todo documento que haya sido otorgado o recibido a través de mensajes de datos, de conformidad con esta Ley y sus reglamentos, siempre que la información que este contiene sea accesible para su posterior consulta." Otorga valor legal a la firma electrónica[51] siempre que se cumplan las dos condiciones establecidas en el artículo 8 de la Ley 82 de 2012, esto es, empleado un método de identificación del iniciador y aprobación del contenido de un mensaje de datos, y que se haya utilizado un método confiable y apropiado para el propósito de la comunicación.".

Así como el concepto de escrito ha evolucionado, y está relacionado, tanto a lo tradicional como al lenguaje tecnológico actual, de igual forma la evolución alcanza a la firma en términos tecnológicos. Tenemos entonces el concepto usual firma, identificado como el nombre y apellidos escritos por una persona de su propia mano en un documento, con o sin rúbrica, para darle autenticidad o mostrar la aprobación de su contenido, y tenemos también el concepto de firma digital, que es la información cifrada que identifica al autor de un documento electrónico.[52] Los conceptos de firma[53] y firma digital, aunque se diferencian en la forma o medio de expresión, pues en uno el autor utiliza su propia mano y letra, y en el otro podría usar un certificado electrónico[54], ambos tienen el mismo propósito: identificar al autor para darle autenticidad y/o aprobación al acto jurídico y a su contenido. Ejemplos de firma electrónica simple utilizados en el día a día de las personas, lo son el *Entrust ST* que utilizamos para validar las transacciones bancarias, por la denominada banca electrónica[55]; el *QR Code*[56] que le permite ingresar al *WhatsApp web;* al utilizar su tarjeta de crédito o débito en una tienda; la firma que produce el introducir su usuario y contraseña para ingresar a su cuenta de correo electrónico y enviar mensajes de datos, lo cual es probablemente el ejemplo más antiguo; o el *microchip*, que se encuentra entre las últimas tendencias en portabilidad y transmisión de información.[57]

6. Reconocimiento y Ejecución de Laudos Arbitrales.

La vida del convenio arbitral electrónico está sujeta a la observancia de los requisitos de forma, en el caso de Panamá, contenidos en el artículo 16 de la LAP. Sin embargo, la cuestión de la validez puede y debe analizarse desde dos perspectivas opuestas pero complementarias: el principio y el fin del convenio arbitral.[58] Para alcanzar plena validez y eficacia jurídica el laudo debe ser ejecutable, y ello está íntimamente ligado al convenio arbitral. La Corte de Casación Francesa, en Sentencia de 27 de julio de 1937, señaló que "los laudos arbitrales que se basan en un acuerdo de arbitraje constituyen

[51] Ver Artículo 8 de la Ley 51 de 22 de julio de 2008, de documentos y firmas electrónicas de Panamá.
[52] Diccionario de la Real Academia de la Lengua Española.
[53] En su sentido literal o convencional.
[54] Certificado electrónico. Documento electrónico expedido por un prestador de servicios de certificación de firmas electrónicas, que vincula los datos de verificación de una firma electrónica a un firmante y confirma su autenticidad.
[55] banca en línea, online banking, entre otras denominaciones.
[56] Quick Response Code: Son un tipo de códigos de barras bidimensionales. A diferencia de un código de barras convencional la información está codificada dentro de un cuadrado, permitiendo almacenar gran cantidad de información alfanumérica. Los códigos QR son fácilmente identificables por su forma cuadrada y por los tres cuadros ubicados en las esquinas superiores e inferior izquierda, son capaces de abrir la URL de una página web o perfil social, leer un texto, enviar un email, enviar un SMS o mensaje de texto, realizar una llamada telefónica, guardar un evento en la agenda, ubicar una posición geográfica en un google maps.
[57] Se trata de un dispositivo del tamaño de un grano de arroz que se inserta en la piel a nivel subcutáneo, el cual contiene información relevante para el dueño o contratante del servicio, eliminando de esta forma métodos de transmisión como tarjetas magnéticas, huellas digitales, escaneos oculares, llaves, control policial, control sanitario, información de identidad personal.
[58] Organización de Estados Americanos. Departamento de Derecho Internacional. Arbitraje Comercial Internacional. Reconocimiento y Ejecución de Sentencias y Laudos Arbitrales Extranjeros. GOSIS, Diego B., El Acuerdo Arbitral: Los requisitos de su validez. Pág. 205

una unidad con aquél, y con él comparten su naturaleza contractual."[59] La Convención de Nueva York, CNY, recoge la noción de acuerdo arbitral en el párrafo 1 del artículo II, que establece: "1. Cada uno de los Estados Contratantes reconocerá el acuerdo por escrito conforme al cual las Partes se obliguen a someter a arbitraje todas las diferencias o ciertas diferencias que hayan surgido o puedan surgir entre ellas respecto a una determinada relación jurídica, contractual o no contractual, concerniente a un asunto que pueda ser resuelto por arbitraje." El artículo IV, establece que entre los requisitos para obtener el reconocimiento y la ejecución de laudos extranjeros, el interesado debe aportar el original del acuerdo arbitral o una copia auténtica del mismo. Tal Convención, que por muchos años había establecido un armónico régimen internacional con relación a los acuerdos de arbitraje, los procedimientos y los laudos arbitrales,[60] parece haber perdido vigencia. Orientada a resolver esta problemática, motivada por la necesidad de unificar la interpretación de ciertos puntos de la CNY, y con el objetivo de situar al convenio arbitral en línea con las prácticas comerciales internacionales,[61] la CNUDMI, en ejercicio de su autoridad otorgada en la Resolución 2205 de la Asamblea General,[62] emitió la recomendación interpretativa que antes mencionamos, que el párrafo 2 del artículo II de la CNY se aplique reconociendo que las circunstancias que describe no son exhaustivas. De este modo se consolida el principio de libertad de forma de la cláusula arbitral, entendiéndose que el requisito por escrito que está en la CNY, no es perfecto o absoluto. Se puede interpretar en lo más amplio del concepto, a tono con las prácticas comerciales internacionales.

7. Conclusiones.

En los últimos años hemos venido experimentando una revolución de los medios de comunicación conocidos hasta el momento. Actualmente muchas personas desarrollan sus relaciones básicas, así como sus transacciones mercantiles a través de medios o canales electrónicos, como las aplicaciones. Esto ha evolucionado en un completo entorno cibernético que no se detiene en su desarrollo. El uso del *e-commerce* se hace cada vez más frecuente en nuestra sociedad, y del mismo modo los conflictos entre las partes de una relación comercial van surgiendo.

El arbitraje es una buena alternativa para dirimir conflictos comerciales. La correcta comprensión del concepto de acuerdo de arbitraje y de sus características determinará el éxito del arbitraje, pues de allí parte el procedimiento que llevará a las partes a obtener una decisión que ponga fin a la controversia, decisión que quedará plasmada en el laudo arbitral.

La moderna Ley de Arbitraje de Panamá, inspirada por la Ley Modelo de Arbitraje de la CNUDMI, adoptó la libertad de forma del convenio arbitral, abriendo espacio al convenio arbitral electrónico.

El requisito de que el convenio arbitral deberá constar por escrito continúa vigente, sin embargo, no se entenderá en el sentido estricto o tradicional de "por escrito", sino más bien adaptándose a la actualidad de las transacciones comerciales, considerando el uso del comercio electrónico.

Los requisitos de forma del acuerdo de arbitraje se resumen básicamente en dos: 1. Que quede constancia de su contenido, y, 2. Que la información sea accesible para su consulta.

El requisito de firma del convenio arbitral electrónico queda rezagado, con la recomendación de la CNUDMI sobre la interpretación del Artículo II.2 de la Convención de Nueva York. La norma

[59] Roses C. Moller et Cie., publicado en 1 DALLOZ 25 (1938). Traducción de Diego B. Gosis.
[60] Organización de Estados Americanos. Departamento de Derecho Internacional. Arbitraje Comercial Internacional. Reconocimiento y Ejecución de Sentencias y Laudos Arbitrales Extranjeros. SANDLER OBREGÓN, Verónica, El Acuerdo Arbitral y sus Efectos en el Reconocimiento y Ejecución de Sentencias o Laudos Arbitrales Extranjeros. Pág. 257.
[61] PERALES VIZCASILLAS, Pilar. Derecho Comercial Internacional, Tomo II. Pág. 674.
[62] Por la cual se estableció la CNUDMI.

contenida en el artículo 16 de la LAP, indica que ya no se exige la firma de las partes en el convenio arbitral, ni un intercambio de comunicaciones entre ellas.[63] El espíritu de la norma es garantista del reconocimiento de la validez del acuerdo de arbitraje al amparo de la Convención de Nueva York.

Por el principio de la equivalencia funcional contenido en la Ley de Documentos, Firmas y Comercio Electrónico de Panamá, hoy el convenio arbitral electrónico tiene las mismas consecuencias jurídicas y probatorias que el convenio arbitral tradicional. Las leyes comentadas operan en armonía con las tendencias y prácticas del comercio internacional, y con los modernos medios de concertación de contratos.

El reconocimiento de la validez y eficacia jurídica del acuerdo arbitral electrónico no excluye el factor cultural: una cultura digital o tecnológica, sumada a una cultura arbitral, que asimile la conveniencia de la aplicación del principio a favor de la validez del acuerdo arbitral,[64] nos ayudará a avanzar de la mano con la agilidad del comercio y de la economía mundial.

[63] Ver Ley Modelo de la CNUDMI sobre Arbitraje Comercial Internacional. Segunda parte. Nota explicativa de la secretaría de la CNUDMI. Pág. 31.

[64] El principio pro-arbitraje, contenido en el Artículo II de la Convención de Nueva York, así como en la LMA, es aquél que trata de apegarse a la regla a favor de la validez del laudo arbitral. La exigencia en cuanto a la prueba de la invalidez debe ser altamente estricta, es decir, que sólo en extremas circunstancias se debe presumir nulo el acto.

LA APLICACIÓN DEL DERECHO AL OLVIDO PARA CANDIDATOS A PUESTOS POPULARES EN ÉPOCA DE ELECCIONES.

Por: ***Alejandro Loredo Álvarez***
México

El ejemplo es el único argumento efectivo en la vida civil
Edmund Burke

Todo pueblo para no desaparecer necesita ser gobernando
con inteligencia y con autoridad.
Cicerón

Cada periodo de renovación de los poderes ejecutivo y legislativo es pertinente escoger a aquellos candidatos que recogen las necesidades más urgentes y den, en consecuencia, las mejores soluciones a la población. En nuestro sistema político actual entre las propuestas destacan, las orientadas a perfeccionar la selección de candidatos electorales en el seno de los partidos políticos. No obstante, La opinión generalizada es que, en nuestro ordenamiento y a pesar de lo que afirma la teoría clásica de la representación, los votantes no eligen personas sino partidos. Sus candidatos son las caras de estos e instrumento de aplicar las políticas públicas emanadas de esos partidos[1].

Por otro lado, las circunscripciones plurinominales y las listas cerradas y bloqueadas provocan que la inclusión en una candidatura no dependa tanto del perfil y capacidad los resultados que cabe esperar del candidato como de las relaciones que este mantenga dentro de su propia formación. Y por consiguiente los partidos distan de ser transparentes ante el electorado.

Es más, en algunas ocasiones, parece importar más la obediencia a la disciplina del partido o los vínculos de lealtad establecidos con la cúpula directiva que la capacidad de los candidatos y los apoyos que este pueda recibir del resto de los afiliados. Para hacer frente a problemas de este tipo, se habla de potenciar elecciones internas.

Como lo expone Paloma Biglino, la mayor parte de estas críticas se centralizan en las cúpulas directivas de los partidos. Según esta opinión, son los dirigentes quienes, desde el aislamiento de sus despachos, hacen oídos sordos a las demandas populares con tal de conservar el control de la formación en beneficio propio y de quienes les son leales. Estas críticas a los partidos políticos no son ni nuevas ni originales Entre las denuncias a la casta y los reproches contenidos en la famosa ley de hierro de las oligarquías no hay demasiada diferencia. Como en los años 20, la crisis económica ha favorecido que la opinión pública personifique su malestar en un conjunto de dirigentes a quienes se considera responsables de la actual situación[2].

A lo largo de la historia los filósofos y políticos más sobresalientes, han defendido el gobierno representados por los mejores hombres sea desde una república, o gobierno parlamentario. Tanto los

---

[1] Argumento en contrario, es el expuesto por Max Weber al hace la distinción entre el político y el científico, reconociendo el papel del líder carismático en los procesos políticos. Weber entiende por carisma la cualidad que pasa por extraordinaria, condicionada mágicamente en su origen, de una personalidad por cuya virtud se la considera en posesión de fuerzas sobrenaturales o sobrehumanas, o por lo menos específicamente extra cotidianas y no asequibles a cualquier otro, o como enviado de Dios, o como ejemplar, y en consecuencia como jefe, caudillo, guía o líder. *Véase* el político y el científico.

[2] Biglino, Paloma. *Intervención del legislador y selección de candidatos por los partidos políticos: una perspectiva comparada*.Dialnet-IntervencionDelLegisladorYSeleccionDeCandidatosPor-5099951.pdf

autores del Federalista[3], como los constituyentes franceses estaban convencidos de que el único gobierno democrático apropiado para un pueblo de hombres fuese la democracia representativa, que es la forma de gobierno en la que el pueblo no toma las decisiones que le atañen, sino que elige a sus representantes que deben decidir por él; pero de ninguna manera pensaban que instituyendo una democracia representativa degenerarse el principio del gobierno popular. Prueba de ello es que la primera constitución escrita de los Estados Unidos, la de Virginia (1776)- pero la misma fórmula también se encuentra en las constituciones posteriores – dice: "Todo el poder reside en el pueblo, y en consecuencia emana de él"; y el artículo 3 de la Declaración del 1789 repite: "El principio de toda soberanía reside esencialmente en la nación. Ningún cuerpo, ningún individuo puede ejercer una autoridad que no emane expresamente de ella." Aparte del hecho de que el ejercicio directo del poder de decisión por parte de los ciudadanos no es incompatible con el ejercicio indirecto mediante representantes elegidos, como lo demuestra la existencia de constituciones como la italiana vigente, que prevé el instituto de referéndum popular aunque solamente con sentido abrogativo. Tanto la democracia directa como la indirecta, derivan del mismo principio de la soberanía popular aunque se distinguen por la modalidad y las formas en que es ejercida esa soberanía[4].

Marco Tulio Cicerón, mucho tiempo atrás ya pensaba lo mismo, en su magnífica obra la Republica, expresa:
XXXIV… Si [la Ciudad] abandona al azar [la elección de sus gobernantes] se hundirá tan presto como una nave a cuyo timón estuviera un piloto designado por la suerte de entre los pasajeros, pero si un pueblo es libre, elige a quienes se ha de confiar y, dado que él desea su propia conservación, elige a los mejores y así se tiene por seguro que la salud de los Estados o Ciudades está confiada a la prudencia de los mejores, y sobre todo por cuando la naturaleza ha hecho no solo porque aquellos hombres superiores en virtud y en animo gobiernen a los más débiles, si no también que estos deseen obedecer a los hombres superiores [5].

Por lo demás, la democracia respectiva nació también de la convicción de que los representantes elegidos por los ciudadanos son capaces, de juzgar cuales son los intereses generales mejor que los ciudadanos, demasiados cerrados en la contemplación de sus intereses particulares, y por tanto la democracia indirecta es más apropiada para lograr los fines para los cuales había sido predispuesta la soberanía popular. También bajo este aspecto la contraposición entre democracia de los antiguos y democracia de los modernos termina por ser desorientadora, en cuento a la segunda se presenta, o es interpretada, como más perfecta que la primera con respecto al fin. Para Madison la delegación de la acción de gobierno a un pequeño número de ciudadanos de probada sabiduría habría "hecho menos probable el sacrificio del bien del país a consideraciones particularistas y transistorizas" [6] A condición de que el diputado una vez elegido no se comportarse como hombre de confianza de los electores que lo habían llevado al parlamento sino como representante de toda la nación. Para que en sentido estricto la democracia fuese representativa era necesario que fuese excluido el mandato obligatorio del elector frente al elegido que en cambio era la característica del Estado estamental, en el que los estamentos, las corporaciones, los cuerpos colectivos trasmitían al soberano mediante sus delegados sus exigencias particulares. También en esta materia la enseñanza venia de Inglaterra. Burke había dicho[7]:

[3] Ensayo político escrito por Hamilton, Alexander, James Madison y John Jay. Publicado el 22 de noviembre de 1787
[4] Bobbio, Norberto, *Liberalismo y democracia*, edit. FCE breviarios, pág. 35
[5] Cicerón, *La República*, edit. Gernika, México,1993, pág. 36
[6] Hamilton, Alexander, James Madison y John Jay. *El Federalista*/Alexander Hamilton, James Madison y John Jay; trad. y pról. de Gustavo R. Velasco—2ª ed. México, FCE, 2001. Pág. 96, citado en Liberalismo y democracia, Bobbio, Norberto, *Op. cit.* nota 3.
[7] E. Burke, *Speech at the Conclusions of the Polls after his being declared duly elected*, The Works, J. Dodsley. 1972, vol. II, P. 15.

Es derecho de todo hombre expresar su opinión; la de los electores es una opinión que pesa y debe respetarse. El representante debe escuchar con buen ánimo tal opinión… Pero las instrucciones imperativas, mandatos a los cuales el miembro de los Comunes debe, expresa y ciegamente obedecer, estas cosas son desconocidas por completo para las leyes de esta tierra.

Para formalizar la separación del representante del representado, los constituyentes franceses, siguiendo la opinión eficazmente presentada por Sieyès (1748-1836), introdujeron en la constitución de 1791 la prohibición de mandato imperativo con el artículo 7 de la sección III del capítulo I del título III que estipula: "Los representantes nominados en los departamentos no serán representantes de un departamento particular, sino de toda la nación, y no se les podrá imponer a ellos mandato alguno." Desde entonces, la prohibición hecha a los representantes de recibir un mandato imperativo por parte de sus electores se volverá un principio esencial para el funcionamiento del sistema parlamentario, el cual, precisamente en virtud de este principio, se distingue de los viejos Estados estamentales europeos. [8]

La figura clásica de la superioridad, y en cierto sentido, de la necesidad del gobierno del hombre sabio frente al de las buenas leyes, está representada por el gran legislador, tal como lo explica Bobbio. Esta figura es necesaria porque se inserta en el punto débil de la tesis favorable al gobierno de las leyes, la cual debe responder a la pregunta: ¿De dónde vienen las leyes? [9]

El legislador sabio es el que realiza el buen gobierno introduciendo buenas leyes: el gobierno de las leyes para ser un buen gobierno presupone al hombre justo que es capaz de interpretar las necesidades de su ciudad.

El contrato social es la culminación de Juan Jacobo, es la utopía de todos los hombres, que son iguales los unos de los otros, si el poder político tiene que apoyarse en la decisión libre de los ciudadanos, su proceso de formación se identifica con el contrato, y éste, a su vez, con su legitimidad dos veces milenaria, es la mejor justificación del poder[10]. En uno de los capítulos más sorprendentes y controvertidos del contrato social: "se necesitarían dioses para dar leyes a los hombres"[11]. Bajo todos los aspectos el legislador es un hombre extraordinario cuya misión histórica es nada menos la de cambiar la naturaleza humana, de trasformar a cada individuo que en sí es un todo perfecto y aislado, en parte de un todo más grande.

La superioridad del hombre se cimienta en el supuesto del buen gobernante cuyo ideal para los antiguos es el gran legislador, en efecto, si el gobernante es sabio ¿Qué necesidad hay de constreñirlo en redes de las leyes generales que le impiden sopesar los méritos de cada uno? Cierto, ¿pero si el gobernante es malo, no es mejor someterlo al imperio de las normas generales que impiden, a quien detesta el poder, juzgar a criterio de su arbitrio lo justo o lo injusto?

El legislador omnipotente un segundo principio general que Maquiavelo da por supuesto, es la suprema importancia que tiene el legislador. Un estado que tiene que ser fundado por un solo hombre y las leyes y el gobierno por él creados determina el carácter nacional de un pueblo. La virtud moral

[8] *Op. cit*. Bobbio Norberto, pág. 37
[9] Bobbio, Norberto, *El futuro de la democracia*, edit. FCE, 1986, pág. 122
[10] De la cueva, Mario, La idea del estado, FCE, México, 19998, pág. 106
[11] Rousseau hace esa exclamación al explicar que para encontrar las mejores reglas de sociedad que convengan a las naciones, seria menester una inteligencia superior, que viese todas las pasiones de los hombres sin estar sujeta a ellas; que no tuviese ninguna relación con nuestra naturaleza y que la conociese a fondo; cuya dicha no dependiese de nosotros, y que sin embargo quisiese ocuparse en la nuestra; en fin que procurándose para futuros tiempos una lejana gloria, pudiese trabajar en un siglo y disfrutar en otro. Sería necesario que hubiese dioses para poder dar leyes a los hombres. Capitulo VII, del legislador, de su obra el contrato social.

y cívica surge de la ley, y cuando una sociedad se ha corrompido, no puede nunca reformarse por sí misma, sino que tiene que tomarla en sus manos un legislador que pueda restaurarla a los sanos principios establecidos por su fundador[12].

El político mexicano Emilio Rabasa, resalta la importancia de la integración de un poder legislativo fuerte. No siempre la tarea de hacer la ley es de las más importantes. En ocasiones interesa que el Poder Legislativo sea la genuina expresión de la opinión pública nacional. El parlamento es la mejor tribuna de un país para tratar sus más graves problemas. En su seno deben plantearse, debatirse y sugerir los temas de la actualidad política. De este modo se logra una importante colaboración política y se hace participar al pueblo en forma responsable y consciente[13].

Lo dicho por Rabasa, nos obliga a traer a Cicerón de nuevo, al exponer ¿Qué puede haber más admirable que una república gobernada por la virtud cuando el que manda a los otros no es el mismo esclavo de ninguna concupiscencia, cuando no establece ni propone a sus conciudadanos nada a lo que el mismo no se sienta vinculado, pues no es posible que imponga leyes al que el mismo no obedezca [14]. Así, si me permiten sentencia Dante.[15]

La elección de candidatos afines a los ideales de una sociedad se hace más que necesarios en nuestro tiempo. La correcta elección de las personas que nos representan hacen que tengamos que saber no solo sus ideales políticos, maneras de gobernar, si no conocer: origen, ámbito personal; familia, amigos, compañeros de grupo político, puestos anteriores, reputación profesional, entre otros factores. Saber a quién la damos nuestra representación para que gobierne en nuestro nombre es fundamental para construir y vivir en el espacio territorial que queremos.

Se vuelven imprescindibles las palabras de Burke[16]:

"Antes de que se confíen a los hombres los puestos de confianza del Estado, deberían de haber obtenido por su conducta un grado tal de estimación en su país que pudiera servir de garantía al pueblo y de seguridad de que no han de abusar de su confianza"

En pocas palabras, como refiere Yutang, podemos decir que en los tiempos de Hanfeitsé había dos conceptos opuestos del Gobierno, como lo hay en nuestros tiempos: el concepto confuciano del gobierno por los caballeros y la concepción legalista del gobierno por la ley más que por las personas. El sistema confuciano presume que todo gobernante es un caballero y procede a tratarle como caballero. El sistema legalista presume que todo gobernante es un pillo y procede a establecer reglas del sistema político que le impidan cumplir sus malas intenciones. Evidentemente, el primero es el criterio tradicional, y el segundo el criterio occidental, y también el criterio de Hanfeitsé[17].

En otras palabras, en lugar de esperar que nuestros gobernantes sean caballeros y caminen por el sendero de la rectitud, debemos presumir que son convictos en potencia, e idear medios y arbitrios de impedirles que roben al pueblo y vendan la nación. Es fácil ver que este último sistema tiene más

[12] Idea expuesta por Matheus Nascimiento en Manual de teoría política: https://issuu.com/mtcezare/docs/manualteoriapolitica/20

[13] Rabasa Emilio. *La constitución y la dictadura*, edit. Porrúa, México 2011. Prologo XXIX

[14] *Op. Cit* Cicerón, pág. 37

[15] En la Divina Comedia, Dante describe al infierno conformado por nueve círculos concéntricos a donde van a parar los pecadores a recibir sus castigos. En la quinta fosa del octavo círculo sitúa a los políticos corruptos y a los malversadores de los dineros públicos. En esta son condenados aquellos que se aprovecharon de manera ilícita de sus cargos y como castigo son sumergidos en un lago de brea hirviente, resguardado por un grupo de diablos que castigan con sus ganchos a quienes intentan salir.

[16] Burke Edmund, *El descontento político*, edit. FCE, fondo 2000, pág. 25

[17] Yutang Lin, *Mi patria y mi pueblo*, traducción de Román A. Jiménez, edit. Sudamericana, Buenos Aires, 1944, pág. 254

probabilidades de resultar efectivo como freno a la corrupción política que el sistema de esperar que esos caballeros cambien de manera de ser[18].

Una de las herramientas al alcance que tenemos los ciudadanos, los votantes para conocer a nuestros candidatos son la TICS. El uso de la tecnología pasa imperceptible en nuestros sentidos, sin percatarnos que incorporamos en el Internet parte de nuestra vida, rasgos de nosotros mismos. Lo hacemos crecer aportando información para que crezca ese mundo virtual. Nosotros alimentamos al Internet sin saber que lo sabemos.

La incorporación de estos nuevos medios a la vida económica y social supone una serie de ventajas, como por ejemplo, mayor eficiencia empresarial, aumento de elección de usuarios así como nuevas fuentes de ingresos. Sin embargo también se crean incertidumbres en el mundo jurídico, por desconocimiento mismo de manejo del propio fenómeno. Uno de estos aspectos es el uso que le damos los usuarios a nuestras datos personales, referencias de nuestra vida propia, en el entorno digital.

El derecho a la privacidad supone, el derecho a poder estar solo, en su espacio íntimo, con el alcance que cada uno desee, incluso completamente solo, sin sufrir injerencias no deseadas y sin interferir en el derecho de los demás [19] . Se confirma, así, los datos personales somos nosotros. Nuestra personalidad, y modo de vida y ser, pueden ser leídos desde el mundo digital como libre información y, por lo que toda vulneración o mal uso es un atentado a nuestra intimidad [20] .

Recaséns Siches, citando a Ortega y Gasset, afirma que "La vida es una intimidad con nosotros mismos", traduciéndose en un "hacer algo, determinado, positivo o negativo, un determinar qué voy a hacer, por consiguiente, en este sentido un hacer"[21] .

Internet y, en particular, las redes sociales constituyen el quinto poder. Sin embargo, es necesario rescatar el lugar del ciudadano como agente de los procesos sociales.[22]

Castells amplía este argumento para explicar la naturaleza de la sociedad digital: como nunca antes en la historia, la esfera pública se construye sobre la base de las redes de comunicación. El espacio virtual que conforma la sociedad red se convierte en una de las expresiones concretas de esta esfera pública[23].

En un trabajo publicado por el Instituto Electoral de la Ciudad de México[24], se concluye que la naturaleza interactiva de la red permite transgredir los órdenes del mundo físico, se materializa a

[18] *Ibídem*
[19] Amitai Etzioni, *The limits of Privacy*: http://www.gwu.edu/~ccps/lop.html
[20] El Diccionario para juristas de Juan Palomar de Miguel, define a la Intimidad como: Amistad íntima. Zona espiritual reservada e íntima de una persona o de un grupo, sobre todo de una familia. Se insiste en la naturaleza del dato personal que es algo íntimo, intrínseco a la persona, de su parte espiritual.
[21] Burgoa Origuela Ignacio, Las garantías constitucionales, edit. Porrúa. México 1990, pág. 16
[22] Contrastar las diversas coyunturas históricas, los contextos sociales, culturales y políticos específicos que permiten evaluar el impacto, las posibilidades y las limitaciones del uso de la tecnología como instrumento para el desarrollo democrático. Visiones más críticas sostienen que la participación en el ciberespacio reproduce y amplía las características de los contextos sociopolíticos preexistentes. P. Norris, *Preaching to the Converted? Pluralism, Participation and Party Websites*, Party Politics 9, núm. 1, 2003, pp. 21-45.
[23] M. Castells, *The New Public Sphere: Global Civil Society, Communication Networks, and Global Governance*, The Annals of the American Academy of Political and Social Science, núm. 616, 2008, p. 78.
[24] Se enfatiza que: Utilizando la tecnología como herramienta, los ciudadanos pueden disentir de manera directa y en tiempo real, o casi real, de las opiniones, la información y las acciones provenientes de los grupos de poder: el Estado, los partidos políticos, los legisladores, los medios, las empresas. Carlos Arango, Jacob Bañuelos Paola Ricaurte Quijano, Gabriel Sosa

través del cuestionamiento directo de los roles tradicionales, jerárquicos, monológicos, impositivos de los actores políticos, de los medios, de las empresas. Algunas de esas interpelaciones ciudadanas se han dirigido a las empresas mediáticas por el cerco informativo y el monopolio mediático; al Estado para demandar el respeto a los derechos humanos, la transparencia y la rendición de cuentas; a los políticos, por prácticas deshonestas y por su vinculación con intereses privados, el derroche de recursos públicos, la desatención de las demandas sociales.

En ese contexto, el hecho de que datos personalísimos queden a disposición de terceros en la red coloca en condición de vulnerabilidad a sus legítimos titulares, pues quedan expuestos a un uso abusivo y muchas veces ilícito de esa información personal, de manera que se genera la necesidad de reservar esos datos personales contra el abuso de terceros o incluso de eliminarlos, como derecho irrenunciable de su titular, lo cual nos plantea el derecho al olvido. En el entendido que es una potestad del sujeto de derecho – léase candidato- o de la sociedad el determinar si esa información personal se inserta o se excluye de la red digital.

De acuerdo con la Agencia española de protección de datos, el denominado 'derecho al olvido' es la manifestación de los tradicionales derechos de y cancelación y oposición aplicados a los buscadores de internet. El 'derecho al olvido' hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. Adicionalmente, la Comisión Europea elaboró, con fecha de noviembre del año 2010, una Comunicación titulada *A comprehensive approach on personal data protection in the European Union*, en la que se recoge la preocupación por reforzar los derechos de acceso, rectificación, oposición y cancelación de los datos personales frente a los avances tecnológicos en el marco de la reforma de la normativa europea sobre protección de datos. Se introduce por vez primera una definición del derecho al olvido digital; se plantea la necesidad de clarificarlo fundamentando su existencia en el principio del consentimiento, esto es, el derecho a cancelar, acceder y oponerse a los tratamientos de datos personales cuando estos han sido divulgados o tratados sin el consentimiento de su titular.

En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia *ni interés público* [25],(en oposición al interés personal) aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información).

Estos derechos esenciales se reconocen por el mero hecho de ser persona; son contemporáneos con la personalidad jurídica que el Derecho concede en la actualidad a todo ser humano por el hecho del nacimiento. Esta connotación de corresponder a todo ser humano les caracteriza también como derechos innatos.

El tribunal español ya ha resuelto importantes sentencias sobre la naturaleza y características de la información recabada sobre la persona[26]: La idoneidad como condición Sine qua non. Al reflexionar

Plata, Coaut. *Esfera pública y tecnologías de la información y la comunicación*. Colección. Instituto electoral del distrito federal, México, 2012.

[25] Es el interés tutelado por el Estado por concernir al patrimonio común de la sociedad. Diccionario Jurídico, O*p. cit.*

[26] De las primeras y que marca una guía de estudio, se encuentra la que se emitió conforme al litigio iniciado entre Google Spain, S.L. y Google Inc., contra el señor Costeja González, de fecha 13 de mayo de 2014, que en su caso tomamos de estudio para el desarrollo de este tema. La Litis planteada concretamente es: un ciudadano español ya no quiere que aparezca en el buscador de Google España, información sobre embargos contra su patrimonio realizados hace 10 años, por no cubrir la seguridad social. Google, por su lado, dice que ellos simplemente se limitan a mostrar al usuario dónde encontrar información sobre la persona requerida, pero que no son responsables de los datos que haya colgados en esa web; y que si quieren que esos detalles personales desaparezcan, que se lo digan al propietario/editor de esa página para que los

sobre pertinencia y vigencia de los datos por el transcurso del tiempo. A saber, se expone en la sentencia cuando la difusión de estos datos por la intermediación de éste le perjudica y de que sus derechos fundamentales a la protección de dichos datos y de respeto a la vida privada, que engloban el «derecho al olvido», prevalecen sobre los intereses legítimos del gestor de dicho motor y el interés general en la libertad de información, ya que en razonamientos de casos similares siguientes por la Audiencia Nacional, en su resolución del Recurso 0000725/2010, ésta ha dilucidado en forma diáfana por medio de un gran ejercicio de ponderación, que el derecho a la protección de datos personales va más allá que el sólo respeto al derecho a la intimidad, ya que el derecho a la protección de datos extiende su garantía no sólo a la intimidad, "sino en la esfera de los bienes de la personalidad que pertenecen a la vida privada, inseparablemente unidos al respeto de la dignidad de la persona". Pero siempre reconociendo los derechos de libertad de expresión e información.

¿Porque decimos esto? Como exprese antes, en un acucioso e impecable ejercicio de ponderación de derechos, el razonamiento de la resolución del Recurso 0000725/2010 en su punto de derecho décimo segundo señala:

> Con carácter general y como reflexión previa al concreto juicio de ponderación de los derechos e intereses en conflicto que haremos más adelante, debe ponerse de manifiesto que la libertad de información, en principio, se encuentra satisfecha por su subsistencia en la fuente, es decir, en el sitio web donde se pública la información por el editor. Cuestión distinta es si cabe apreciar la existencia de un interés del público en encontrar la información en relación con la cual se ejercita el derecho de oposición en una búsqueda que verse sobre el nombre del afectado que deba prevalecer sobre el derecho a la protección de datos personales de este.

Conforme a este razonamiento el Tribunal español mantiene el derecho a la información vigente al señalar que los datos personales del promovente se mantienen en el sitio web, pero la vinculación directa de sus datos con base en un interés público no probado ya no se permite, esto es, al escribir el nombre del afectado ya no ubicara la información sobre sus antecedentes de forma inmediata. Todos los derechos fundamentales quedan a salvo y ocupan un lugar respectivo [27] Éste es el caso, en particular, cuando son inadecuados, no pertinentes o excesivos en relación con estos fines y el tiempo transcurrido."

La licitud de tratamiento de datos, nos indica Vega V., debe acomodarse a unos principios, o lo que es lo mismo, debe encajar dentro de unos límites cuyo uso determine la legalidad del tratamiento, recogida y posterior uso, aquí reproducimos los propuestos por dicho autor [28] .

a) Principio de finalidad: Los datos de carácter personal solo podrían recogerse para su tratamiento. Y únicamente podrán someterse a dicho tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que hayan obtenido.
b) Principio de exactitud: Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado

"descuelgue". Que ellos se limitan a enlazarla. Así que se niegan a dejar de "indexar" esas páginas. Así las cosas, el asunto versa sobre interpretar la Directiva 95/46/CE sobre datos personales y su libre circulación.

[27] En el punto décimo tercero, se expresa el sentido de la ponderación de los derechos al señalar: 8) El equilibrio puede depender, en supuestos concretos, de la naturaleza de la información, del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de la información, que puede variar en función del papel que esa persona desempeñe en la vida pública; en este caso, el interés preponderante del público debe basarse en razones concretas que ha de comprobar, en su caso, el órgano judicial (apartados 81 y 98 de la Sentencia del TJUE).

[28] Vega V. José Antonio, Contratos electrónicos y protección de los consumidores. Edit. Reus, Madrid, 2005. Pág. 373

c) Principio de *necesariedad*: Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubiera sido recabados o registrados.
d) Principio de legitimación: El tratamiento de los datos de carácter personal no está prohibido, pero requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga de otra cosa.

Se observa que el principio de necesariedad expuesta por Vega, coincide con las reiteradas características de idoneidad, pertinencia, proporcionalidad y vigencia que deben de tener los datos recabados por terceros para su divulgación. Sin cualquiera de estos rasgos procede pedir su cancelación por dejar de ser útil al ente almacenador y terceros que tengan acceso a estos.

El pasado 25 de mayo de 2016 entró en vigor el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento y libre circulación de datos personales, derogándose así la Directiva 95/46/CE (Reglamento General De Protección De Datos, RGPD). El Reglamento fue publicado en el Diario Oficial de la Unión Europea (DOUE) el pasado 4 de mayo de 2016.

En su considerando (65), Se inserta por primera vez diáfanamente el concepto de derecho al olvido:
(65) Los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un «derecho al olvido» si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones.

Y:
Artículo 17
Derecho de supresión («el derecho al olvido»)
1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes:

a) Los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;
b) El interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;
c) El interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;

d) los datos personales hayan sido tratados ilícitamente;
……

Sin embargo, la excepción a este derecho deviene del mismo ejercicio del cargo público del interesado, al señalar:
3. Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario:
a) para ejercer el derecho a la libertad de expresión e información;
b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable;

Nuestro antecedente jurídico patrio se encuentra en la reforma realizada en el año 2007 al artículo 6° constitucional. Se sientan las bases respecto al derecho a la información (transparencia), incluyendo la protección de datos personales por parte de las entidades públicas, reconociendo los derechos de acceso y rectificación.
El Artículo 16 constitucional establece que toda persona tiene derecho a la protección de sus datos personales.

La reforma constitucional a los dispositivos señalados se acota al contexto del uso de la protección de datos *perse*. No se le involucra en forma directa con el respeto a la dignidad humana como el del honor y propia imagen, conceptos sin duda incluidos en el artículo primero de nuestra carta magna. Hagamos de España nuestra referencia próxima, y en el mismo idioma.

Nuestra ley Federal de Protección De Datos Personales en Posesión de Particulares, es una ley de orden público, incluye los ya populares derechos ARCOS; sin embargo, no está clara dónde se regula y cómo se ejerce el derecho al olvido, conforme a ésta. Existe la regulación pero no es clara, hay que intuir el camino, hay que "rascarle" a la ley para encontrar el camino.

En el dictamen de Decreto que expide la ley, se indica que:
"El llamado "derecho al olvido", se incorpora en un tercer párrafo del artículo 11. "Debido a que es un elemento que favorece la confianza de los particulares respecto al tratamiento de su información, se sugiere contemplar este derecho, cuya finalidad es establecer la obligación de los responsables de la base de datos de eliminar los datos personales después de un plazo razonable posterior, a que se presente algún incumplimiento. Con ello se refuerzan los derechos de los particulares a la intimidad y a la protección de su información. Asimismo, se homologa el régimen a lo establecido en la Ley para Regular a las Sociedades de Información Crediticia. Sobre el particular, se sugiere que el plazo antes mencionado, es decir, el del artículo 11, sea de 72 meses a efecto de que se le dé un tratamiento igual al que se establece en la referida Ley."

"En esa virtud, el citado párrafo queda como sigue: "El responsable de la Base de Datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento" .

Finalmente la redacción del artículo 11, fue:

Artículo 11.- El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados.

Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados.

El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento.

Esta redacción no es aplicable en cuanto al uso de datos en la red digital. El legislador en su dictamen nunca se refiere a la información manejada en internet. La ley como está no permite dilucidar de manera inmediata la acción de desvinculación de los datos de una persona en Internet. Aunado a que el mismo uso de datos de la persona van concatenados al aviso de privacidad. Nada que ver con el ejercicio al derecho al olvido.

Si es el deseo del legislador y así también del espíritu de la ley, contemplar el derecho al olvido, se debe hablar del uso de la información en el entorno digital; de la figura del proveedor de contenidos; tratamiento de datos personales; su vinculación con el derecho de libertad de expresión e información y los límites a estos que puede haber cuando todos se confrontan. Hoy se tiene que recurrir a la analogía o los principios generales de derecho.

Sin embargo, hay una ventana recién abierta: en materia electoral. El Acuerdo de Consejo General Del Instituto Nacional Electoral por el que aprueba el Reglamento del Instituto Nacional Electoral en materia de Protección de Datos Personales, recoge la opinión del INAI solicitada por éste en el cual se dice:
"El derecho que tiene el titular de elegir la vía a través de la cual ejercerá sus derechos ARCO cuando las disposiciones aplicables a determinados tratamientos de datos personales establezcan un trámite específico para el ejercicio de estos derechos, ya sea a través del procedimiento general, o bien, el trámite específico.

Sobre esta última prerrogativa, conviene manifestar que no siempre las leyes en materia de datos personales resultan ser la vía idónea para atender las peticiones de los titulares respecto al ejercicio de los derechos ARCO, no obstante que la petición esté relacionada específicamente con el tratamiento de datos personales.
Así, dependiendo de las implicaciones que el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales produzca en un contexto jurídico determinado se estará en posibilidades de calificar la idoneidad de la vía.

En este sentido, si el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales implica que se generen una serie de efectos que impacten sustantivamente en la definición de cuestiones jurídicas vinculadas a aspectos civiles, administrativos, mercantiles, electorales, entre otros, la petición del titular, no obstante, que a primera vista se trate de un ejercicio de derechos ARCO, debe ser conocida y resuelta por la instancia o autoridad competente que corresponda, ya que de otro modo se correría el riesgo de que las autoridades garantes de protección de datos personales conozcan sobre cuestiones que desborden su competencia."

Se obliga una reforma que aclare este derecho. En el cajón de los derechos ARCOS supusieron nuestros legisladores que cabría todo.

En este contexto, no está de más analizar cómo otros países europeos han abordados problemas similares a los nuestros. Resulta también conveniente pasar revista a los criterios establecidos por algunas organizaciones, a la Organización para la Seguridad y Cooperación en Europa (OSCE), la

Oficina para las Instituciones Democráticas y Derechos Humanos (ODHIR) y la Comisión para la Democracia a través del Derecho, (Comisión de Venencia), adscrita al Consejo de Europa. Estas organizaciones han elaborado documentos de soft law que constituyen recomendaciones y códigos de buenas prácticas que, aunque no tienen naturaleza vinculante, ejemplifican medidas que han dado buenos resultados en otros países y pueden ser de utilidad a la hora de enfocar posibles soluciones. Estos textos son fundamentalmente, al *Code of Good Practice in the Field of Political Parties*, adoptado por la Comisión de Venencia en 2008-20093 y a las G*uidelines on Political Party Regulation*, elaborados por la OSCE/ODIHR y la Comisión de Venecia en 2010 [29]

Ahora bien, nuestra Constitución General de la República, en su artículo 35, establece:

Artículo 35. Son derechos del ciudadano:

I. Votar en las elecciones populares;
II. Poder ser votado para todos los cargos de elección popular, teniendo las calidades que establezca la ley. El derecho de solicitar el registro de candidatos ante la autoridad electoral corresponde a los partidos políticos así como a los ciudadanos que soliciten su registro de manera independiente y cumplan con los requisitos, condiciones y términos que determine la legislación;

Excepciones deben establecerse en el Derecho Mexicano exclusivamente con fines políticos electorales a fin de saber el perfil psicológico y sociológico de los candidatos a elegir; su fuente de financiamiento, si es del partido mismo, si es mediante recursos propios o aportaciones externas, y en su caso, que vinculo tiene con los que financian su candidatura, etc. [30]. Y así conciliar el derecho a la intimidad con las normas que rigen la libertad de expresión.

Coincidimos en los argumentos esgrimidos en la sentencia española analizada ya que en un ejercicio de ponderación jurídica, los derechos de la persona prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de una persona que disputa un cargo de elección popular.

Al efecto, citamos la tesis más idónea del Tribunal Electoral del Poder Judicial de la Federación. DATOS PERSONALES. LOS TITULARES ESTÁN FACULTADOS PARA DECIDIR SU DIFUSIÓN Reconocen el derecho a la vida privada de las personas, conforme al cual, deben reservarse sus datos personales y la demás información relativa a su vida privada que estén en poder de algún ente público o de particulares, y protegerse de la posible utilización indebida por terceros. Ese derecho concede a su titular, la atribución de resguardar ese ámbito privado, garantizándoles el poder de decidir sobre la publicidad de los datos de su persona, lo que supone la facultad de elegir cuáles pueden ser conocidos y cuáles deben permanecer en reserva, además de designar quién y bajo qué modalidades pueden utilizarlos, dado que la protección de datos personales incluye el derecho de autodeterminación informativa como uno de los fines para propiciar la confiabilidad en el manejo y cuidado de las referencias concernientes a las personas en el ámbito de su vida privada, así el Estado

[29] Biglino, Paloma, O*p. cit.*
[30] En un ejercicio de derecho comparado, en 2010, en el caso *Citizens United vs Federal Election Comission*, la Suprema Corte de Estados Unidos emitió un fallo en contra de las prohibiciones gubernamentales a las contribuciones corporativas a súper PACS, comités de acción política conformados para apoyar un candidato. Al calificar a estas prohibiciones como restricciones del derecho de expresión y otorgar a las corporaciones el estatus de personas con un derecho incondicional al discurso político, la resolución permite que el dinero invada el proceso de elección. Esto, nos dice Brown, permite que grandes corporaciones financien las elecciones, el icono definitivo de la soberanía popular en la democracia neoliberal. *Véase*, Brown Wendy, *El pueblo sin atributos, la secreta revolución del neoliberalismo*. Edit. Mal Paso Ediciones, Barcelona, 2016.

a través de sus órganos adoptará las medidas tendentes a hacer efectiva la tutela del referido derecho. Jurisprudencia 13/2016.

El poder desvincular la información sobre el nombre del afectado, en una búsqueda en internet sin violentar otros derechos fundamentales es el fin del derecho analizado.

La protección de datos, siendo como es un derecho fundamental, es asimismo requisito para que otras libertades sean respetadas. Impide (debería impedir) que la información disponible sobre las personas pueda ser utilizada en contra de sus derechos y libertades en el mundo "físico y digital".

Sin embargo, tal no sería el caso si la persona buscada es parte de la vida pública al ser funcionario o representante popular. La injerencia en sus derechos fundamentales está justificada por el interés preponderante de los ciudadanos en tener, a raíz de esta inclusión, acceso a la información y determinar su aptitud para representar a un grupo de ciudadanos en el puesto a ocupar mediante el proceso de votación.

Cabe recordar a Tocqueville que dedica el capítulo séptimo de la primera parte de la Democracia en América a la tiranía de la mayoría. El principio de mayoría es un principio igualitario en cuanto pretende hacer prevalecer la fuerza del número sobre la de la individualidad; reposa sobre el argumento de "que hay más cultura y sabiduría en muchos hombres reunidos que en uno solo, en el número más que en la calidad de los legisladores. Es la teoría de la igualdad aplicada a la inteligencia."

EL USO DE TICS (TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN) PARA RESOLUCIÓN DE CONFLICTOS DE CARÁCTER LABORAL EN BRASIL

Por: ***Flávia Neves Nou de Brito***
Brasil

INTRODUCCIÓN

El objetivo de esta ponencia es evaluar el uso de TIC (tecnologías de la información y de comunicación) en resolución de conflictos de naturaleza laboral.

La justificación de tal estudio está en la constatación de que Brasil es uno de los países más avanzados del mundo con respecto al proceso en la plataforma digital, el llamado proceso electrónico[1], pero, por otro lado, incipiente en el desarrollo de soluciones de mediación, principalmente con empleo de TIC(s), pre-procesal[2] y/o autónomas al Poder Judicial.

Sin embargo, además de la ausencia de herramientas y estímulos consolidados para la composición antes y durante el proceso judicial, hay también dos peculiaridades en Brasil que incitan al presente estudio como una forma de optimización en la solución de conflictos: el hecho de que Brasil es el país con más abogados del mundo[3] [4] y los datos estadísticos de costo del Poder Judicial Laboral (*Tribunal Superior do Trabalho de Brasil*).

De acuerdo con el sitio web CONSULTOR JURÍDICO, el 0,5% de la población brasileña está formada por abogados, lo que hace un promedio de 01 abogado por cada 205 brasileños. Por otro lado de esta ecuación, están los magistrados de juicio laboral, cuya relación matemática es de 3600 magistrados para 100.441.546 brasileños, que comprenden la población económicamente activa (PEA)[5], según los datos del informe de 2016 elaborado por el *Conselho Nacional de Justiça*[6] de Brasil. Así, se observa fácilmente que hay una masa de profesionales deseosos por ser agentes en la composición de los conflictos[7], sin enjuiciamiento de proceso para la Justicia Laboral brasileña, cuyos recursos son limitados frente la creciente necesidad de la población.

---

[1] BRITO, Flávia Neves Nou. **O Chamado Processo Eletrônico Brasileiro e o Princípio do Devido Processo Legal:** O Embate Entre O Sistema De Normas Jurídicas E Os Sistemas Informáticos. Disponible en: <http://www.migalhas.com.br/arquivos/2015/8/art20150821-01.pdf>. Consulta: 15 ago. 2017.

[2] La Unión Europea publicó en 2013 la Directiva 2013/11/EU sobre la solución alternativa de controversias para el consumo, y el Reglamento (UE) no 524/2013, que tiene en ODR *(Online Dispute Resolution)*, con la puesta en marcha del portal europeo para el 2016 de enero, fecha en la que se va a aplicar el Reglamento Europeo, mientras que en Brasil todavía no hay legislación disciplinaria sobre este tema, donde ya existe una plataforma digital implementada Por el Consejo de justicia nacional brasileño en operación desde el 2017 de junio.

[3] CONSULTOR JURÍDICO. **Total de advogados no Brasil chega a 1 milhão, segundo a OAB.** [Consulta: 15 ago. 2017]. Disponible en: http://www.conjur.com.br/2016-nov-18/total-advogados-brasil-chega-milhao-segundo-oab

[4] REIS, Adacir. "Mediação e impactos positivos para o judiciário". In: ROCHA, Carlos Cesar Vieira, SALOMÃO, Luís Felipe (coord.). **Arbitragem e Mediação.** São Paulo: Editora Atlas S.A., 2015. p. 221.

[5] Número de personas que se consideran activas en el mercado de trabajo, grupo que incluye a todos aquellos de 10 años de edad o mayores que estaban buscando ocupación o trabajo en la semana de referencia de la encuesta nacional por muestra de hogares (*Pesquisa Nacional de Amostra de Domicílios* - PNAD/IBGE), estimado a partir de los dados de la investigación. (IPEA. [Consulta: 25 ago. 2017] Disponible en: http://www.IPEADATA.gov.br/ExibeSerie.aspx?serid=486696855)

[6]CONSELHO NACIONAL DE JUSTIÇA. **Justiça em números 2016:** ano-base 2015/Conselho Nacional de Justiça, Brasília: CNJ, p. 11 - 404, 2016. [Consulta 22 ago. 2017] Disponible en: http://s.conjur.com.br/dl/justicaemnumeros-20161.pdf.

[7] MAIA NETO, Francisco. O papel do advogado na mediação. In: ROCHA, Carlos Cesar Vieira, SALOMÃO, Luís Felipe (coord.). **Arbitragem e Mediação.** São Paulo: Editora Atlas S.A., 2015. p. 237.

Se eligió, como corte metodológico, el estudio destinado a la resolución de conflictos laborales mediante el uso de TIC(s). Esta elección fue motivada por no estar de acuerdo con la resistencia demostrada por jueces y tribunales laborales[8] [9] [10] al uso de métodos de resolución de conflictos cuando manejados por árbitros y mediadores privados, con el pretexto de que los derechos laborales no serían disponibles/ negociables, resistencia que es aún peor cuando se utilizan TIC(s) para ampliar y facilitar los métodos de resolución de conflictos.

Se buscó presentar métodos de resolución de conflictos, centrándose en los métodos que utilicen los TIC (s), los principios norteadores y marco legal brasileño acerca del tema. Al final, se hace consideraciones para demostrar las ventajas obtenidas por los métodos de resolución de conflicto con uso de TIC(s) para resolver conflictos laborales y críticas al posicionamiento contrario a este método por parte de jueces laborales brasileños.

2. MÉTODOS DE RESOLUCIÓN DE CONFLICTOS

Los conflictos pueden resolverse por la auto tutela o por la autocomposición/heterocomposición, dependiendo de quién determina la resolución del conflicto. Se llama auto tutela cuando una de las partes impone su voluntad al otro, haciendo que sus intereses prevalezcan unilateralmente. Por otro lado, si las partes, conjuntamente y sin intervención de terceros, ponen fin al conflicto, se dice que la solución ocurrió por medio de la autocomposición. Sin embargo, si la resolución del conflicto se obtuvo a través de la acción de un agente, esta solución se produjo por medio de la heterocomposición.[11] [12] [13]

En la autocomposición (también conocida como negociación**)**, las partes buscan pacificar sus diferencias a través del diálogo directo sin interferencia de ninguna tercera parte[14]. La negociación es guiada por la competencia, por la cooperación o ser una mezcla de ambos, en este caso, llamado híbrido.[15] [16] La negociación competitiva es aquella en la que las partes son tratadas como oponentes y no hay transparencia de información, generando un comportamiento de blefe e ganga[17]. La negociación cooperativa se basa en el comportamiento de la Unión de los esfuerzos para encontrar una solución satisfactoria para todas las partes.[18] El ejemplo clásico para entender la diferenciación de los dos tipos de negociación es la disputa de dos hermanos por una naranja. La madre, tercer mediador, divide la naranja por la mitad y entrega cada mitad a un niño. El primero, come el bagazo y tira el zumo; el segundo, bebe el jugo y tira el bagazo. La lección que se obtiene de esta historia es

---

[8] MARTINS, André Chateaubriand. "A arbitragem nas relações de trabalho: proposta de tratamento legislativo" In: ROCHA, Carlos Cesar Vieira, SALOMÃO, Luís Felipe (coord.). **Arbitragem e Mediação.** São Paulo: Editora Atlas S.A., 2015. p.21.

[9]VIANNA, Ana Cláudia Torres. **Mediação na Justiça do Trabalho:** Buscando identidade Experiências dos Centros Integrados de Conciliação da 15ª Região. Disponible en:
<http://www.migalhas.com.br/dePeso/16,MI240024,61044-
Mediacao+na+Justica+do+Trabalho+Buscando+identidade+Experiencias+dos> Consulta: 25 ago. 2017.

[10] CARMONA, Carlos Alberto. **Arbitragem e Processo:** um comentário à lei nº 9.307/96. 2. ed. São Paulo: Editora Atlas S.A., 2006, p.60

[11] PINHEIRO, Rogério Neiva. **Técnicas e Estratégias de Negociação Trabalhista**. 2.ed. São Paulo: Editora Ltda., 2017**,** p. 22.

[12] SENA, Adriana Goulart de. **Formas de resolução de conflitos e acesso à justiça,** Belo Horizonte, v.46, n.76, p.93 e 94, 2007. [Consulta: 25 ago. 2017.] Disponible en:
http://www.trt3.jus.br/escola/download/revista/rev_76/Adriana_Sena.pdf

[13] DELGADO, Maurício Godinho. **Curso de Direito do Trabalho**. 9. ed. São Paulo: Editora LTR, 2010, p. 1342.

[14] Op. cit. ECKSCHMIDT, Thomas (lugares de Kindle 334-337).

[15] Op. cit. Pinheiro, pág. 24.

[16] Ibidem, p. 37.

[17] Ibidem, p. 24 y 25.

[18] Ibidem, pág. 31.

que los intereses podrían conciliarse si hubiera habido diálogo entre las partes, porque el conflicto era evidente.[19]

La heterocomposición ocurre cuando hay la intervención de uno tercero en la solución del conflicto. La calidad y el modo de acción de esta tercera parte es que determinará el tipo de heterocomposición, que podrá ser arbitraje, mediación, conciliación y simulacro de juicio. En el arbitraje el tercero actúa de acuerdo con la convención privada establecida por las partes en conflicto, resolviendo el acuerdo sobre la base de este convenio y sin intervención del estado, teniendo tal decisión la misma efectividad de la sentencia judicial.[20] En la mediación, el tercero actúa de manera neutra con el objetivo de restablecer el diálogo entre las partes y alentarlos a encontrar una solución a la disputa. La mediación difiere del arbitraje, porque no es parte del trabajo del mediador decidir la disputa si las partes no llegan a un acuerdo, como es el caso del árbitro. La mediación tampoco se confunde con la conciliación, porque el conciliador tiene un papel activo en la sugerencia de los resultados al impasse entre las partes, mientras que el mediador busca trabajar la comunicación entre las partes para llegar a un consenso.

Por fin, hay el método de resolución de conflictos llamado "simulacro de juicio" o "resumen de juicio del jurado", método que es bastante común en los Estados Unidos. Consiste en una vista previa de cómo sería el proceso judicial por medio de una simulación, en la cual las partes presentan sus opiniones a los miembros del jurado, que sugieren una decisión, que puede llegar a ser obligatoria, si así que piden a las partes.[21] En Brasil, no es un método adoptado para la resolución de conflictos.

Los conflictos aún se pueden resolver a través de la jurisdicción del estado[22] (proceso judicial) o por medios alternativos, entendido aquí por exclusión, es decir, todos los métodos posibles de solución de conflictos alternativos al proceso judicial, conocida como Métodos Alternativos de Resolución de Conflictos.[23]

Los métodos de resolución de conflictos han tenido un mayor prestigio en los últimos años[24] con el desarrollo de los Estados democráticos de derecho, en los que prevalece la idea de bienestar social, en él se entiende la promoción del fin de las controversias por medio de soluciones eficaces, rápidas, menos costosas y socialmente valiosas, permiten mejorar la relación futura entre las partes.[25] Y Brasil no ha sido ajeno a esta tendencia global, llamado por algunos autores a partir de “Reajuste funcional

[19] Ibidem, p. 33.
[20] Op. cit. CARMONA, p. 51
[21] Op. cit. ECKSCHMIDT, (lugares de Kindle 322-326).
[22] GRINOVER, Ada Pellegrini. **A inafastabilidade do controle jurisdicional e uma nova modalidade de autotutela** (parágrafos únicos dos artigos 249 e 251 do Código Civil. Revista Brasileira de Direito Constitucional, n. 10, p. 13, jul. /de. 2007. [Consulta: 15 ago. 2017]. Disponible en: http://www.esdc.com.br/RBDC/RBDC-10/RBDC-10-013-Ada_Pellegrini_Grinover.pdf
[23] “La mera expresión ‘medios alternativos de solución de conflictos’ nos plantea a siguiente interrogante: ¿alternativos respecto a qué? La respuesta que se ha venido dando a la misma connota que es en relación al proceso legal o judicial” (BERNARDO, María Valeria. Medios alternativos de resolución de conflictos en Argentina. **Negocios Processuais.** In: DIDIER JR., Fredie (coord.). Salvador: *Jus*PODIVM, 2016, p. 697).
[24] BUITONI, Ademir. Mediar e conciliar: as diferenças básicas. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 15, n. 2707, 29 nov. 2010. [Consulta: 15 ago. 2017]. Disponible em: https://jus.com.br/artigos/17963.
[25] Op. Cit. BERNARDO, p.695.

del procedimiento civil", desjudicialización [26] o Deslegalización[27], ya que se explicará aún más.

3. MÉTODOS INNOVADORES DE RESOLUCIÓN DE CONFLICTOS CON EL USO DE TIC'S

Es un requisito previo para que la resolución de conflictos tenga una comunicación eficaz entre las partes, ya sea por iniciativa propia o por interferencia de uno tercero, que puede ser, como ya se ha visto, un mediador, conciliador o árbitro.

Es innegable que el desarrollo de nuevas tecnologías relacionadas con el campo de las comunicaciones ha cambiado completamente las relaciones humanas en todos sus aspectos: social, afectivo, comercial, político, etc. El máximo exponente de estas tecnologías, sin duda, es la red mundial de ordenadores, internet, que ha proporcionado el fenómeno de la posmodernidad que SANTOS bautizó de los problemas fundamentales del espacio-tiempo[28].

A partir de estas premisas para el análisis de la resolución de conflictos con el uso de las TIC (s), la comunicación puede ser sincrónica o asincrónica. Esta tipología es importante, porque la sincronización de la interacción entre las partes influye en la velocidad de resolución de los conflictos. La comunicación sincrónica es aquella en la que las TIC's eliminan la barrera espacio-temporal, haciendo que las partes interactúen en tiempo real, independientemente de dónde se encuentren físicamente. Esto es lo que sucede en reuniones programadas para videoconferencias y *chats* a través de internet. Hay, sin embargo, la posibilidad de comunicación asincrónica para la búsqueda de resolución de conflictos, cuando la comunicación es llevada a cabo por el intercambio de mensajes a través de correo electrónico o plataforma virtual, esto es, con la interacción de las partes en diferentes momentos, según su disponibilidad o preferencia personal. Y la comunicación es mixta, cuando se utiliza varias TIC(s) para agilizar la resolución del conflicto, de acuerdo con la conveniencia de las partes y el procedimiento establecido, proporcionando tiempos en que la comunicación es asincrónica intercalada con comunicación sincrónica.[29]

Además de la comunicación eficiente y rápida, hay uno tercero factor importante a ser considerado para la amplitud de las posibilidades de éxito en la resolución de conflictos, que es el costo de esta comunicación. Estos tres factores (eficiencia, velocidad y costo) son tan relevantes, que el derecho brasileño legisló en su nuevo Código de procedimiento civil, promulgado en 2015, la posibilidad de notificaciones y citaciones por correo electrónico [30] [31] oída de testigos en otras localidades a través de

[26] "En los últimos decenios del siglo pasado, en la primera década de este, la doctrina más autorizada ha venido observando y planteando una serie de ideas o propuestas para adaptar los diferentes instrumentos procesales de tutela de los derechos a las nuevas realidades, necesidades e problemas que se han manifestado en nuestra sociedad. Estas nuevas orientaciones tienes singularmente por objetivo a la 'readaptación funcional del proceso civil'. Algunas de las más relevantes de estas corrientes son, a nuestro entender, la desjudicialización, esto es, la proliferación de mecanismos de resolución de controversias alternativos a la tutela judicial; la implantación y aplicación de las nuevas tecnologías de la información y la comunicación en la Administración de Justicia; y, por último, la especialización funcional y material de procedimientos para adaptarlos a las controversias, reclamaciones y asuntos de una menor cuantía pero una mayor frecuencia en la realidad forense. Gran parte de estas tendencias, podemos observar que confluyen, actualmente, en una institución o, mejor expresado, novedoso concepto: las ODR, acrónimo del sintagma inglés *Online dispute resolution."*. (GAIPO, Julio Pérez. **Nuevas Tecnologías y Formas De Resolución de Controversias:** Una Visión Crítica Desde Algunos Principios Procesales. In: MATA, Federico Bueno de (coord.). **Fodertics 3.0**, Granada: Editorial Comares, 2015, p. 45 e 46).

[27] Op. cit. GRINOVER, p.14.

[28] SANTOS, Boaventura de Sousa. **Pela Mão de Alice:** o social e o político na pós-modernidade. 8ª ed. São Paulo: Cortez Editora, 2001, p.281.

[29] Op. Cit. ECKSCHMIDT, Thomas, (Locais do Kindle 1856-1871).

[30] Art. 246. *A citação será feita: [...] V - por meio eletrônico, conforme regulado em lei.*

[31] Art. 236. *Os atos processuais serão cumpridos por ordem judicial. [...] § 3º Admite-se a prática de atos processuais por meio de videoconferência ou outro recurso tecnológico de transmissão de sons e imagens em tempo real.*

videoconferencia[32] [33]. Más recientemente, después de una provocación sobre la legalidad o no del uso de teléfono y aplicaciones como *WhatsUp* para citaciones judiciales, el Consejo Nacional de Justicia brasileño se ha posicionado favorablemente[34], estimulando los tribunales de los estados federados brasileños a reglar esto uso, a ejemplo del Tribunal de Justicia de Bahía, que expedía el Decreto 684, de 27 de julio de 2017[35], y el Tribunal de Justicia de Maranhão, por medio de la Portaria nº. 11/2017[36]. De todo modo, las TIC (s) se pueden utilizar en la resolución de conflictos en dos momentos, tanto en la esfera pre-procesal como procesual. Las partes en autocomposición pueden utilizar las TIC(s); al igual que el Estado, en el ejercicio de su función de decir el derecho (poder judicial); particulares, en la calidad de terceros encargados de intermediar una solución al conflicto; o, en un cuarto nivel, como se verá adelante, por una máquina dotada de inteligencia artificial.

4. MEDIOS ELECTRÓNICOS PARA RESOLUCIÓN DE CONFLICTOS EN LÍNEA O ODR (*ONLINE DISPUTE RESOLUTION*)

ODR (*Online Dispute Resolution*) - acrónimo que se hizo popularizado entre los eruditos del tema, porque se utiliza en 1996 en el primer artículo legal[37] - no es fácil de definir ante la gran variedad de entendimientos en la doctrina. La definición más simple para ODR sería el método de resolución alternativa de conflictos por medio del uso de mecanismos dispuestos en Internet.[38] [39] Una definición más precisa de ODR fue presentado en abril 2017 por la UNCITRAL **(**United Nations Commission on International Trade Law/Comisión de Derecho Mercantil Internacional de las Naciones Unidas). ODR sería un mecanismo para resolver conflictos mediante el uso de comunicaciones electrónicas u otra tecnología de información y comunicación[40].

---

[32] Art. 385. *Cabe à parte requerer o depoimento pessoal da outra parte, a fim de que esta seja interrogada na audiência de instrução e julgamento, sem prejuízo do poder do juiz de ordená-lo de ofício. [..] § 3º O depoimento pessoal da parte que residir em comarca, seção ou subseção judiciária diversa daquela onde tramita o processo poderá ser colhido por meio de videoconferência ou outro recurso tecnológico de transmissão de sons e imagens em tempo real, o que poderá ocorrer, inclusive, durante a realização da audiência de instrução e julgamento.*

[33] La crítica que este autor hace en este momento es el desajuste entre la norma y la estructura del poder judicial, ya que, como abogada en proceso judicial, requirió la prerrogativa de escuchar a los testigos en otra ubicación por videoconferencia en lugar de escuchar por carta precatoria a otro juicio, pero su petición fue negada por el magistrado del proceso, lo que justificó no ser posible por falta de equipamiento para llevar a cabo la videoconferencia y registrarlo en el sistema de proceso judicial electrónico (E-SAJ).

[34] Procedimiento de control administrativo (PCA) nº 0003251-94.2016.2.00.0000 del CNJ por el cual se cuestiona la decisión de los asuntos internos del Tribunal de Justicia de Goiás (TJGO), que prohibía el uso del WHATSUP en el distrito de Piracanjuba/Go. (CONSELHO NACIONAL DE JUSTIÇA. WHATSAPP puede ser usado para citaciones judiciales. [Consulta em:15 ago. 2017]. Disponible en: Http://www.CNJ.jus.br/noticias/CNJ/85009-WhatsApp-pode-ser-usado-para-intimacoes-judiciais).

[35] Según la información preparada en el sitio del TJBA, se gastaron R$4,3 millones con citaciones por correo, además de r $1,9 millones con citaciones, en el período de enero a julio 2017. (Tribunal de Justicia de Bahía. **Sistema de citación telefónica promueve la velocidad, la sostenibilidad y la reducción de costos**. [Consulta en: 25 ago. 2017] Disponible en: http://www5.tjba.jus.br/index.php?option=com_content&view=article&ID=97467:sistema-de-intimacoes-por-Telefone-promove-rapidez-sustentabilidade-e-diminuicao-de-Custos&CATID=55&Itemid=202

[36] CONSELHO NACIONAL DE JUSTIÇA. WHATSAPP puede ser usado para citaciones judiciales. Disponible en: Http://www.CNJ.jus.br/noticias/CNJ/85009-WhatsApp-pode-ser-usado-para-intimacoes-judiciais Acceso: 15 ago. 2017.

[37] "En 1996, el primer artículo sobre ODR apareció en una revisión de la ley, el centro nacional para la investigación automatizada de la información (NCAIR) patrocinó la primera Conferencia devoción a ODR, y la financiación de NCAIR lanzó los primeros proyectos ODR significativos. (KATSH, Ethan; Ala, Leah. **Diez años de resolución de conflictos en línea: mirando el pasado y construyendo el futuro,** Nueva York, v. 38, p. 101-126, 2006. [Consulta en: 25 ago. 2017]. Disponible en: Http://www.Ombuds.org/Articles/Toledo.pdf.

[38] Op. Cit. GAIPO, p. 45 – 46.

[39] BETANCOURT, Julio César; ZLATANSKA, Elina. **Online Dispute Resolution (ODR): What Is It, and Is It the Way Forward?** 79 International Journal of Arbitration, Mediation and Dispute Management, Issue 3, 2013. [Consulta en: 15 ago. 2017]. Disponible en: **https://ssrn.com/abstract=2325422**., p. 256.

[40] "Online dispute resolution, or "ODR", is a "mechanism for resolving disputes through the use of electronic communications and other information and communication technology". The process may be implemented

El ODR es uno método de resolución de conflictos[41] relativamente nuevo y que a veces es confundidos con su especie, a ejemplo de la mediación electrónica, también llamada Resolución de Conflictos en Línea[42]. Por eso es importante desmitificar los propósitos a los que se propone este estudio, tener en vista la intención de demostrar que todos los tipos de ODRs son útiles para aliviar el poder judicial, dar más velocidad y eficacia a la resolución de los conflictos así como reducir los costos con la estructura disponible para el procedimiento. De hecho, ODR es el género que puede ser categorizado en tres especies: 1) Resolución de controversias en línea o simplemente E-mediación, Mediación *online* o Mediación electrónica*;* 2) Sistemas para ayudar a analizar los problemas legales o ayudar en la negociación; y, 3) Plataformas de mediación conducidas por inteligencia artificial (negociaciones en línea).

Según SUSSKIND[43], Asesor del Ministro inglés de justicia y profesor reconocido de la zona, dos son los grandes beneficios en el uso de ODRs: a) economía de recursos para las partes en conflicto y el poder judicial, por lo tanto un mayor acceso a la justicia[44], por tener un costo menor; b) medio ambiente virtual de uso amistoso con las partes involucradas.

Sin embargo, hay debilidades en el uso de ODR(s) para la resolución de conflictos y que merecen ser resaltadas, porque interfieren con la seguridad jurídica y por esto deben ser enfrentadas por los legisladores y ejecutores de ODR(s).

En primer lugar, hay el análisis de la funcionalidad en términos técnicos de la plataforma o aplicación utilizada como herramienta para la implementación de ODR. Debe haber sistemas de seguridad para que la información no pueda ser violada con la mitigación de la confidencialidad de las partes en el proceso de resolución del conflicto. La credibilidad de ODR puede ser comprometida por el error humano en el uso incorrecto del sistema o por el fallo tecnológico, como los correos electrónicos perdidos, los actos de piratería, los virus informáticos.[45] En segundo lugar, debe haber una garantía de quiénes son las partes involucradas en el ODR, que se refiere a la idea de que el uso de la firma digital[46], o instrumento de identificación que le hace[47], debe ser parte del procedimiento ODR. En tercer lugar, está la Preocupación con la Viabilidad de lo que se definió al final de la ODR y el efecto de la cosa juzgada de la decisión que emana de un órgano de gestión de ODR.[48]

---

differently by different administrators of the process, and may evolve over time". (UNITED NATIONS: United Nations Commission on International Trade Law. **UNCITRAL Technical Notes on Online Dispute Resolution**. 2017. Nova York. [Consulta en: 10 set. 2017] Disponible en: http://www.uncitral.org/pdf/english/texts/odr/V1700382_English_Technical_Notes_on_ODR.pdf , p. 4.

[41] Se recomienda leer el primer artículo sobre el tema ODR, *Ten Years Of Online Dispute Resolution: Looking At The Past And Constructing The Future*, verdadero clásico, escrito por Ethan Katsh Y Leah Ala, profesores y directores del centro de tecnología de la información y ODR de la Universidad de Massachusetts (MIT).

[42] CONFORTI, Oscar Daniel Franco. **Mediación Electrónica (e-Mediación)**. Diario La Ley, Espanha, 2015 [Consulta em: 15 ago. 2017]. Disponível em: https://www.academia.edu/12092519/Mediaci%C3%B3n_Electr%C3%B3nica_e-Mediaci%C3%B3n_ , p. 9.

[43] SUSSKIND, Richard. Los abogados de mañana: una introducción a su futuro (Local del Kindle 1489-1492). Oup Oxford. Edición El Kindle

[44] Op. cit. ECKSCHMIDT, Thomas. (Local del Kindle 846-847).

[45] GALLEGO, José María Asencio. Las Ventajas de la Mediación Online y la Superación de sus Inconvenientes. In: MATA, Federico Bueno de (coord.). **Fodertics 3.0**, Granada: Editorial Comares, 2015. p. 7.

[46] Ibídem GALLEGO, pág. 7.

[47] Identificación del iris de los ojos, huellas dactilares, ADN, Biochips, etc.

[48] COROMINAS BACH, Sergi. El Nuevo Sistema Europeo de Online Dispute Resolution (ODR): Una Tutela Efectiva de los Daños Contractuales Masivo e de Baja Cuantía? In MATA, Federico Bueno (Dir.); PULIDO, Irene González (coord.). **Hacia Una Justicia 2.0**. Salamanca: Ratio Legis Ediciones, 2016, p.256.

4.1. RESOLUCIONES DE DISPUTA EN LÍNEA O SIMPLEMENTE E-MEDIACIÓN, MEDIACIÓN ONLINE O MEDIACIÓN ELECTRÓNICA

La E-mediación rompe con el espacio-tiempo del mundo real. Las partes pueden programar una reunión virtual, sin importar el lugar o la hora a la que se someten, pero sólo que haga una estructura eficiente de transmisión de datos a través de internet.

El desplazamiento de las partes tiene un costo que deja de existir con las audiencias virtuales, que pueden extenderse a los mediadores también, si se implementa el teletrabajo[49] en residencia. También deja de existir la necesidad de una estructura física, representando ahorro en el gasto con la propiedad donde se llevaría a cabo la audiencia. Además, las partes pueden estar en una etapa avanzada de litigio, que no apoyan la presencia física del otro, el entorno virtual es una opción menos agresiva y emocionalmente más segura para ambos.[50] [51]

Es innegable que las mediaciones electrónicas proporcionan economía y velocidad para la resolución de conflictos, seguridad física y emocional para las partes, además de ser más convenientes, porque permiten a las partes participar en la elección del lugar y el tiempo que se Participar en la plataforma digital, características que consisten en el mundo postmoderno. Hay autores que defienden, incluso, que las mediaciones electrónicas pueden disminuir el impacto del conflicto y generar una armonización en la relación entre las partes, que es muy útil en situaciones en las que las partes seguirán interactuando, el ejemplo de los conflictos familiares o entre vecinos, por ejemplo.[52] [53] [54]

La E-mediación puede ser sincrónica o asincrónica, dependerá del caso y de la disposición del las partes celebrarán la reunión virtual por videoconferencia. Se Asincrónica, la negociación puede producirse mediante el intercambio de mensajes escritos o grabados en audio a disposición de las partes de la plataforma, que pueden acceder a ellos en el momento que mejor sea conveniente para ellos. [55]

Los creadores de la mediación en línea pensaron que, se la relación jurídica se ha establecido a través de Internet, nada más lógico que la solución también se produzca de la misma manera. Basándose en esta premisa, el E-Bay desarrolló de la primera plataforma de resolución de conflictos a través de ODR en 1996, que en ese momento era revolucionario. Las insatisfacciones de los clientes de E-Bay empezaron a resolverse rápidamente y en una vía de comunicación directa entre la empresa y sus consumidores. Hoy hay una cantidad significativa de plataformas en todo el mundo para resolución conflictos por medio de ODR(s), como se verá adelante. Frente a este escenario, fue feliz el legislador brasileño de la Ley de mediación promulgada en 2015, en resolver posibles dudas sobre la legalidad de las mediaciones *online*, mediante la estandarización expresa de este tipo de resolución alternativa de conflictos a través de ODR(s). Así: *"Art. 46. A mediação poderá ser feita pela internet ou por*

---

[49] El poder judicial brasileño reguló el teletrabajo en 2016 de sus servidores. CONSELHO NACIONAL DE JUSTIÇA. **Resolução 227 de 15/06/2016: Regulamenta o teletrabalho no âmbito do Poder Judiciário e dá outras providências.** [Consulta en: 15 ago. 2017]. Disponível em: http://www.cnj.jus.br/atos-normativos?documento=2295

[50] Op. Cit. BETANCOURT, p. 260 y 261.

[51] LEONE, Giuseppe. Resolución de conflictos en línea gestionando la mediación online. [Consulta en: 25 ago. 2017]. Disponible en: https: www.virtualmediationlab.com/virtual-mediation-lab-usa-international/online-mediation-explained-in-9-minutes/=

[52] Ibíd.

[53] Op. cit. BERNARDO, p. 703.

[54] RODRÍGUEZ, Almudena Gallardo. Mediación Online Aplicada a Situaciones de Rupturas Matrimoniales. In: MATA, Federico Bueno de (coord.). **Fodertics 3.0**, Granada: Editorial Comares, 2015. p. 25.

[55] Op. cit. GALLEGO, pág. 7

outro meio de comunicação que permita a transação à distância, desde que as partes estejam de acordo. Parágrafo único. É facultado à parte domiciliada no exterior submeter-se à mediação segundo as regras estabelecidas nesta Lei".

4.2 SISTEMAS PARA AYUDAR A ANALIZAR PROBLEMAS LEGALES O AYUDAR EN LA NEGOCIACIÓN

La compañía americana IBM desarrolló un algoritmo de inteligencia artificial que se puede acoplar a múltiples aplicaciones para dar respuesta a preguntas formuladas por los usuarios dentro del área de interés. Este algoritmo, llamado IBM Watson, se utilizó por primera vez como un sistema de apoyo en el campo de la medicina [56] [57] y ahora está siendo usado por abogados. El bufete de abogados Baker & Hostetler publicó en mayo de 2016 que 50 abogados de su división de bancarrota comenzaron a utilizar un software derivado del algoritmo de Watson. Este software, que se llama Ross, tiene la capacidad de procesar 500 gigabytes en sólo un segundo, el equivalente de aproximadamente 1 millón de libros, lo que le permite mantener una amplia base de datos de información legal, el ejemplo de la legislación, jurisprudencia y doctrina. El gran diferencial de Ross es que – como está interactuando con los abogados, que pueden hacer preguntas en lenguaje natural, como lo que sucede con el uso de la tecnología Siri y Google Now[58] en los *smartphones* – Ross va aprendiendo[59] y mejorando sus respuestas más y más.[60]

Hay también el aplicativo de Google, Google photos, que identifica y ordena las fotos de los usuarios mediante el uso de un algoritmo de inteligencia artificial, que se puede utilizar para el análisis de documentos. Estos algoritmos, utilizados en plataformas para la resolución consensuada del conflicto en un ODR, dan al mediador, árbitro o conciliador información valiosa. Un ejemplo es el análisis de las expresiones faciales de las partes litigantes. El algoritmo puede calcular la predisposición de las partes de aceptar o rechazar una propuesta, reconocer los intereses o causas del conflicto, por la forma en que las personas se expresan y así ayudar al intermediario a reformular el propósito y las técnicas utilizadas en el proceso de composición. Eso es lo que hace el software *Emotion Explore Lab*, que se puede utilizar para los varios propósitos, entre ellos mediación en ODR (http://www.emotionexplorerlab.net). [61]

4.3 PLATAFORMAS DE MEDIACIÓN REALIZADAS POR INTELIGENCIA ARTIFICIAL: NEGOCIACIÓN ONLINE

La mediación también puede realizarse sin la participación de un agente humano, es decir, mediante

---

[56] Ibm. **IBM Watson Health**. Disponible en: <https://www.IBM.com/Watson/Health/#solutions> Acceso: 03 set. 2017.
[57] Op. cit. KURZWEIL, (Local del Kindle 201-208).
[58] Siri es una aplicación desarrollada por Apple, dotada de una inteligencia artificial rudimentaria, que tiene la capacidad de responder a preguntas pre-programadas mediante la identificación de palabras clave, tales como: "¿Qué día es hoy?" o "¿Cuál es la mejor manera de Cierto lugar? El software que corresponde a Siri desarrollado por Google para smartphones Android es Google OK.
[59] "Some observers have argued that Watson does not really "understand" the Jeopardy! Queries or the encyclopedias it has read because it is just engaging in "statistical analysis." A key point I will describe here is that the mathematical techniques that have evolved in the field of artificial intelligence (such as those used in Watson and Siri, the iPhone assistant) are mathematically very similar to the methods that biology evolved in the form of the neocortex. If understanding language and other phenomena through statistical analysis does not count as true understanding, then humans have no understanding either (KURZWEIL, Ray. **Cómo crear una mente:** El secreto del pensamiento humano revelado (Local del Kindle 4055-4059). Gerald Duckworth & Co. Edición del Kindle) ubicaciones de Kindle 208-213).
[60] MELO, João Ozorio. **El bufete de abogados debuta primero como "robot-abogado" en los Estados Unidos.** Disponible en: Http://www.conjur.com.br/2016-Mai-16/escritorio-Advocacia-Estreia-primeiro-robo-advogado-EUA. Acceso: 03 set. 2017.
[61] LOPEZ, Andrés Vázquez. Realidad Virtual Y Resolución De Conflicto En Línea (Español Edición) (local Kindle 1088-1090). Alén Grupo de medios. Edición El Kindle

plataformas informatizadas conducidas 100% por inteligencia artificial.

La inteligencia puede definirse como la capacidad de resolver problemas con recursos limitados en el menor tiempo posible.[62] El nombre de la inteligencia artificial se da al estudio de automatización de la inteligencia humana. En el caso específico de la ley, la inteligencia artificial se relaciona con la construcción de computadoras (hardware) y aplicaciones (softwares), que, integrados, han capacidad para simular la inteligencia humana con fines legales.[63]

La negociación *online* es un método de resolución de conflictos en el que las partes interactúan a través de la plataforma digital sin la interferencia de los humanos. El concepto de negociación es el mismo, aquí el "*plus*" es la ayuda del sistema inteligente en clasificar y categorizar el problema. En la negociación *online* cada litigante lanza sus márgenes comerciales en el sistema, es lo que entienden como mejor y peor (pero posible) solución al conflicto sin que la otra parte lo sepa. Dicha información, disponible en formato de lista con asignación de nota para cada elemento, son aprobados, analizados y comparados por un algoritmo de sistema, permitiéndole identificar la posible zona comercial a través de cálculos. A partir de ahí el sistema logra formular opciones y caminos viables para sugerir a las partes dentro de una razonabilidad generada sobre la base de la información previa concedida por ellos y dentro de lo que perciben como aceptable para la solución del conflicto.[64] La doctrina ha llamado a esta participación del ordenador de cuarta parte en el procedimiento de resolución de conflictos.

LODDER Y ZELEZNIKOW[65] muestran lo útil que puede ser esta herramienta computacional, utilizando un caso concreto. Traen el ejemplo de una disputa que implica el derecho de los niños, que en muchos países tiene los intereses del estado, estando por encima de los intereses de los padres, el ejemplo de Brasil (en el caso de los autores están basados en el sistema legal australiano). Tal situación es perfecta para un tipo de negociación entre los padres con base al método de cooperación, porque aquí el objetivo no debe (al menos en teoría) ser ganar a la otra parte sino buscar la mejor solución al problema, promoviendo una convivencia pacífica y el bienestar del niño. En términos sencillos, el sistema funciona de la siguiente manera:

---

[62] "*Intelligence may be defined as the ability to solve problems with limited resources, in which a key such resource is time. Thus the ability to more quickly solve a problem like finding food or avoiding a predator reflects greater power of intellect. Intelligence evolved because it was useful for survival— a fact that may seem obvious, but one with which not everyone agrees. As practiced by our species, it has enabled us not only to dominate the planet but to steadily improve the quality of our lives*". (Op. CIT. KURZWEIL, Local Del Kindle 4055-4059).

[63] "Artificial Intelligence involves the study of automated human intelligence. This includes both practically-oriented research, such as building computer applications that perform tasks requiring human intelligence, and fundamental research, such as determining how to represent knowledge in a computer comprehensible form. At the intersection of Artificial Intelligence on the one hand and law on the other lies a field dedicated to the use of advanced computer technology for legal purposes: Artificial Intelligence and Law". (LODDER, Arno R.; ZELEZNIKOW, John. Artificial Intelligence and Online Dispute Resolution. In **Online Dispute Resolution:** Theory and Practice. A Treatise on Technology and Dispute Resolution. Org. Wahab, Mohamed S. Abdel; Katsh, Ethan; Rainey, Daniel. Eleven International Publishing, The Hague, Netherlands, 2011. [Consulta en: 25 ago. 2017] Disponible en: <http://www.ombuds.org/odrbook/lodder_zeleznikow.pdf.

[64] MARKIEWICZ, Sarah. De ellos Tribunales en Piedra hasta es Cibermediación y es Cibernegociación para el Comercio electrónico B2B. En mata, Federico bueno (Dir.); PULIDO, Irene González (coord.). **Hacia Una Justicia 2,0**. Salamanca: ratio Legis Ediciones, 2016, p. 381-382.

[65] "Both systems [Adjusted Winner] require users to rank and value each issue in dispute, by allocating the sum of one hundred points amongst all the issues. Given these numbers, game theoretic optimization algorithms are then used to optimize, to an identical extent, each user's desires. Adjusted Winner divides *n* divisible goods between two parties as fairly as possible. Adjusted Winner starts with the designation of the items in a dispute. If either party says an item is in the dispute, then it is added to the dispute list. The parties then indicate how much they value each item, by distributing 100 points across them. This information, which may or may not be made public, becomes the basis for fairly dividing the goods and issues at a later stage. Once the points have been assigned by both parties (in secret), a mediator (or a computer) can use Adjusted Winner to allocate the items to each party, and to determine which item (there will be at most one) may need to be divided". (Op. Cit. LODDER, Arno R.; ZELEZNIKOW, John, p. 5).

a) Los usuarios (partes: en este caso, los padres del niño) crean individualmente y secretamente de la otra parte una lista de cuestiones controvertidas;
b) Los usuarios clasifican e indicar cuánto valoran cada cuestión controvertida, distribuyendo 100 puntos entre ellos;
c) Mediante el análisis basado en la teoría de juegos, los algoritmos de sistema se utilizan para identificar los deseos de cada usuario;
d) un mediador (o un ordenador) establecerá las bases para la negociación en una etapa posterior sobre la base de esta información.

Más recientemente se ha lanzado una negociación entre dos ordenadores equipados con inteligencia artificial, que fueron desconectados por Facebook[66], porque desarrollaron un lenguaje propio, diferente del inglés, para ampliar la comunicación entre ellos, con mayor velocidad y eficiencia computacional. Según el desarrollador del software[67], el motivo de la desconexión fue la desvirtualización de la meta del experimento. Hecho es que más y más inteligencia artificial se desarrolla, impactando directamente en la vida cotidiana de las personas, dando margen, incluso, a la aparición de nuevas ramas del derecho, el ejemplo del derecho de la nueva tecnología llamada internet de las cosas.

5. PRINCIPIOS RECTORES DE LA RESOLUCIÓN DE CONFLICTOS EN BRASIL

En primer lugar, ¿qué es el principio? Según la doctrina de AVILA[68]: "*[O]s princípios são normas imediatamente finalísticas, primariamente prospectivas e com pretensão de complementariedade e de parcialidade, para cuja aplicação se demanda uma avaliação da correlação entre o estado de coisas a ser promovido e os efeitos decorrentes da conduta havida como necessária à sua promoção.* También explica este Autor que el fin a ser alcanzado por el principio es una idea que requiere orientación práctica, que sólo se lleva a cabo mediante la adopción de ciertos comportamientos. Los principios no son sólo valores cuya realización radica en la dependencia de las preferencias personales y tampoco se confunden con ellas.[69] Enseña este autor:[70]

> *Logo se vê que os princípios, embora relacionados a valores, não se confundem com eles. Os princípios relacionam-se aos valores na medida em que o estabelecimento de fins implica qualificação positiva de um estado de coisas que se quer promover. No entanto, os princípios afastam-se dos valores porque, enquanto os princípios se situam no plano deontológico e, por via de consequência, estabelecem a obrigatoriedade de adoção de condutas necessárias à promoção gradual de um estado de coisas, os valores situam-se no plano axiológico ou meramente teleológico e, por isso, apenas atribuem uma qualidade positiva a determinado elemento.*

En este sentido, el principio positivo es la forma en que el legislador ha encontrado dar fuerza normativa al propósito a promover, sin, sin embargo, prever los medios para su implementación o las consecuencias específicas de esta implementación.[71] La ley de mediación brasileña en su artículo 2, establece comportamientos prácticos que necesariamente deben ser promovidos en la búsqueda de la

[66] CHAUHAN, Douglas. **Facebook desactiva la inteligencia artificial que ha creado el lenguaje propio.** [Consulta en: 25 ago. 2017]. Disponible en: <https: www.tecmundo.com.br/software/120160-facebook-desativa-inteligencia-artificial-criou-linguagem-propria.htm=
[67] SANTINO, Renato. **Entender lo que realmente le pasó a la AI de Facebook que creó un idioma.** [Consulta en: 25 ago. 2017]Disponible en: <https: olhardigital.com.br/noticia/entenda-o-que-realmente-aconteceu-com-a-ia-do-facebook-que-criou-um-idioma/70155=
[68] ÁVILA, Humberto. **A Teoria dos Princípios**. 13ª Edição. São Paulo: Malheiros, 2012, p.85.
[69] Op. cit. Ávila, pág. 86.
[70] Op. cit. Ávila, pág. 87.
[71] Op. cit. Ávila, pág. 136.

resolución consensual del conflicto. De acuerdo con este artículo, la mediación se guiará por los siguientes principios: I-imparcialidad del mediador; II-isonomía entre las partes; III-oralidad; IV-informalidad; V-autonomía de la voluntad de las partes; VI-búsqueda de consenso; VII-confidencialidad; VIII-buena fe. Esta misma Ley, en su artículo 3, también delimita el objeto de la mediación. Puede ser objeto de mediación el conflicto que versa sobre los derechos disponibles o sobre los derechos indisponibles que admitan transacción, siempre que, en esta última hipótesis, esta transacción sobre derechos no disponibles sea aprobada en el Juicio Laboral después de oído el Fiscal público. Considerando que el presente estudio es el método de resolución de conflictos por medio de ODR(s), esto es, con el uso de Internet, la lectura y aplicación de los principios rectores de la mediación deben ser efectuadas en conjunción con los principios del marco legal de Internet, Ley 12.965/2014, por algunos adoctrinadores denominados la "Constitución de Internet".[72] [73] Según el art. 3º de la Ley 12.965/2014, el uso de Internet en Brasil debe seguir principios.[74]

De hecho, la preocupación de Brasil en la creación de líneas maestras para el desarrollo de Internet es loable. y las principios rectores del punto de referencia de Internet civil Llegan en un momento en que existe una gran preocupación por el desarrollo acelerado de la inteligencia artificial. En un ejemplo simple, las preguntas Si el uso de las imágenes utilizadas para La identificación de las emociones de los litigantes en una mediación por ODR sin la ciencia de éstos no perjudicaría un principio o un derecho, más específicamente los derechos que se protegerán en(s) los incisos VIII, IX, X y XI de artículo 7º del dicho marco jurídico.[75]

Las plataformas computarizadas deben seguir los principios. El arquitecto del sistema es que imprime el contenido de valor incrustado en los principios en el momento en que programa la plataforma del sistema. La gran pregunta aquí es: y cuando el propio sistema define sus principios por medio del aprendizaje desarrollada por medio de inteligencia artificial? Esta es una preocupación de los estudiosos del tema – que señalan la escasez de principios para el control del IA por los seres humanos, según lo contorneado por ASIMOV, porque los principios son finalísimos y no axiológicos, lo que puede representar un peligro para la humanidad.[76]

En febrero de 2017, el Parlamento Europeo hizo recomendaciones sobre la legislación civil en el campo de la robótica para dotar a los robots de personalidad jurídica (e-personalidad), que fue

---

[72] TEIXEIRA, Tarcísio. **Curso de Direito e Processo Eletrônico.** 3ª Edição, Saraiva, 2015, p.95.

[73] LOPES, Alan Moreira. **Lei 12.965, de 23.04.2014** – Estabelece Princípios, Garantias, Direitos e Deveres para o Uso da Internet no Brasil (Marco Civil da Internet). In TEIXEIRA, Tarcísio; LOPES, Alan Moreira (coord.). **Direito das Novas Tecnologias.** São Paulo, Ed. Revista os Tribunais, 2015.

[74] *Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.*

[75] *Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] VIII - as hipóteses de guarda obrigatória de registros previstas nesta Lei; XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;*

[76] DIARIOLALEY. **Dictamen Del Comité económico y social Europeo Sobre Es Inteligencia Artificial y Las Nada De Su Utilización**. [Consulta en:12 Sep. 2017] Disponible en: < Http://diariolaley.Laley.es/content/documento.aspx?params=H4sIAAAAAAAEAMtMSbH1czUwMDA0trAwN7RQK0stKs7Mz7M1MjA0N7A0MFTLy09JDXFxti3NS0lNy8xLTQEpyUyrdMlPDqksSLVNS8wpTlVLTcrPz0YxKR5mAgBQVBtEYwAAAA==WKE.

rechazada enérgicamente por el CESE[77] (Comité económico y social europeo).

6. RESOLUCIÓN DE CONFLICTOS EN BRASIL MEDIANTE EL USO DE LAS TIC(S): MARCO REGLAMENTARIO

Brasil ha estado siguiendo la tendencia mundial por la búsqueda de la resolución de conflictos de una manera más efectiva y rápida, así como menos costosa financiera y socialmente. Para esto, está adaptando la legislación procesal existente – a ejemplo del código de proceso civil brasileño de 2015 y de la Ley 13.129/2015, Ley que hizo cambios significativos en la Ley 9.307/96 (conocida como Ley del derecho arbitral) – y la creación de nuevas legislaciones y políticas públicas para fomentar la composición de las partes en conflicto, el ejemplo de la Ley 13.140/2015 (Ley de mediación) y de la Ley 12.965/1994, que creó el marco legal de Internet.

El nuevo código de procedimiento civil brasileño de 2015 (Ley 13.105/2015), a diferencia del código de procedimiento civil de 1973 (Ley 5.869/1973), dio protagonismo a la conciliación, mediación y arbitraje, lanzando estas especies de resolución de conflictos como reglas fundamentales del proceso Civil[78] en el artículo 3º. Otro punto que merece protagonismo, prueba que el legislador brasileño buscó dar medios para que la resolución de conflictos ocurriera con el menor daño social a las partes, fue la reversión del momento en que el acusado presentó su alegato. En la sistemática del código de procedimiento anterior, el acusado debería presentar su defensa, dependiendo del rito, o antes de la audiencia o hasta el momento de la audiencia. Con el nuevo Código de Procedimientos brasileño, artículo 335, ahora el acusado es citado para que aparezca a la audiencia de conciliación o mediación, siéndole concedido el plazo de 15 días después de la audiencia para presentar su defensa escrita.

El cambio legislativo es una corrección importante en la forma en que se buscó resolver los conflictos, cuya postura era un proceso más combativo que comunicativo, ya que las partes ya venían a la audiencia con predisposición de pelear, ya que el autor tuvo acceso en las actuaciones al alegato del acusado, quien, en atención al principio de procedimiento de la concentración de la defensa, se vio obligado a aportar todos los hechos y argumentos a su favor. Sin embargo, es evidente que el proceso civil brasileño antes de la entrada en vigor del código de 2015 alentó el litigio, porque las partes, antes mismo del diálogo en audiencia, ya estaban formalmente cambiando acusaciones por medio de las peticiones de sus abogados.[79]

---

[77] "El CESE defiende un **enfoque de la IA basado en el control humano** (*human-in-command*), con un marco de condiciones que regule el desarrollo responsable, seguro y útil de la IA de manera que las máquinas continúen siendo máquinas y los humanos conserven en todo momento el dominio sobre ellas.
El CESE pide que se elabore un **código deontológico para el desarrollo, despliegue y utilización de la IA**, de modo que durante todo su proceso de funcionamiento los sistemas de IA sean compatibles con los principios de la dignidad humana, la integridad, la libertad, la privacidad, la diversidad cultural y de género y los derechos humanos fundamentales. El CESE aboga por el desarrollo de un **sistema de normalización para la verificación, validación y control de los sistemas de IA**, basado en un amplio espectro de normas en materia de seguridad, transparencia, inteligibilidad, rendición de cuentas y valores éticos. El CESE aboga por una **infraestructura de IA europea de fuente abierta** (*open source*), que incluya entornos de aprendizaje respetuosos de la vida privada, entornos de ensayo en condiciones reales (*real life*) y conjuntos de datos de alta calidad para el desarrollo y la formación de sistemas de IA. El CESE destaca la ventaja (competitiva) que puede obtener la UE en el mercado mundial mediante el desarrollo y la promoción de «sistemas de IA de responsabilidad europea», provistos de un sistema europeo de certificación y etiquetado de la IA". (Ibídem DIARIOLALEY).

[78] DIDIER JR., Freddy. Principio de respeto por Autorregramento De la voluntad en el proceso civil. En: Didier Jr., Freddy (coord.). **Asuntos de procedimiento** Salvador: *Jus*PODIVM, 2016. p. 35.

[79] "*O novo CPC consagra, no particular, um sistema coerente e que reforça a existência de um princípio comum a diversas outras normas: o princípio do respeito ao Autorregramento da vontade no processo civil. Alguns exemplos. O CPC é estruturado de modo a estimular a solução do conflito por autocomposição: a) dedica um capítulo inteiro para regular a mediação e a conciliação (arts. 165-175); b) estrutura o procedimento de modo a pôr a tentativa de autocomposição como ato anterior ao oferecimento da defesa pelo réu (art.s 334 e 695); c) permite a homologação judicial de acordo extrajudicial de qualquer natureza (art.515, III; art. 725, VIII); d) permite que, no acordo judicial, seja incluída matéria estranah ao*

Con respecto a los jueces de los estados federados, fue creado en 2014 el Foro Nacional de Mediación y Conciliación (FONAMEC)[80], compuesta por los coordinadores de los núcleos permanentes de métodos consensuales de resolución de conflictos de los estados federados (NUPEMEC) y por los magistrados gobernantes de los centros judiciales de solución de conflictos y ciudadanía (CEJUSC) con el objetivo de Promover discusiones, intercambiar experiencias y mejorar los métodos de resolución de conflictos.

En Abril 2015, las declaraciones emitidas por FONAMEC promovieron oficialmente el uso de TIC(s) para la resolución de conflictos:[81] En octubre de 2015, o FONAMEC emitió la declaración 43[82], donde señala claramente la posibilidad de uso de ODRs: *ENUNCIADO nº 43 – Os CEJUSCs poderão* ***divulgar plataformas on-line voltadas à resolução consensual de conflitos*** *e recomendar sua utilização para o público em geral.* Semejantemente, el Consejo Federal de Justicia, con el objetivo de estimular las políticas públicas y privadas de mediación, conciliación y arbitraje, publicó en agosto 2016 declaraciones, en el que podemos identificar claramente el deseo por el uso de Tic integrados a los métodos tradicionales de resolución de conflictos.[83]

En el área laboral, por otra parte, no ha habido apoyo para los métodos alternativos de resolución consensuada de conflictos, manteniendo la justicia laboral el carácter concentrador y garante, prohibiendo expresamente las disposiciones relativas a las cámaras privadas de conciliación, Mediación y arbitraje y normas relativas a la conciliación extrajudicial y a la mediación y Pre-procedimiento previsto en el NCPC. De eso se trata el artigo 7 de la Resolución 174 del *Conselho Nacional de Justiça do Trabajo* (CNJT).[84] En relación con el uso de TIC, la Justicia Laboral brasileña también perdió la oportunidad de avanzar.

---

objeto litigioso do processo (art.515, §2º); e) permite acordos processuais (sobre o processo, não sobre o objeto do litígio) atípicos (art.190). Ibidem DIDIER JR., Fredie, p. 35.

[80] CONSELHO NACIONAL DE JUSTIÇA. Disponible en:< Http://www.CNJ.jus.br/programas-e-ACOES/conciliacao-e-mediacao-Portal-da-conciliacao/movimento-conciliacao-mediacao/fonamec>. Acceso: 15 ago. 2017.

[81] *ENUNCIADO nº 03 - É viável a realização de sessão de conciliação ou mediação* ***por videoconferência****, inclusive para prepostos.*

ENUNCIADO nº 09 - Nas comarcas em que há jurisdição de competência delegada da Justiça Federal, os CEJUSC da Justiça Estadual poderão elaborar rotinas de trabalho para promoção da conciliação em processos previdenciários, com a organização de evento com a presença de Procurador do INSS com poderes para transigir, ***ainda que por videoconferência.***

ENUNCIADO nº 10 - Os CEJUSC poderão elaborar rotinas de trabalho na área de benefícios acidentários, com a organização de evento com a presença de Procurador do INSS com poderes para transigir e de peritos, ***ainda que por videoconferência.*** (CONSELHO NACIONAL DE JUSTIÇA. Consulta en:15 ago. 2017] Disponible en: Http://www.CNJ.jus.br/files/conteudo/destaques/arquivo/2015/05/f5faf9126900ab4f10d9702bcdbc77de.pdf

[82] CONSELHO NACIONAL DE JUSTIÇA. Consulta em: Acceso: 15 ago. 2017 Acceso: 15 ago. 2017, Disponible en: Http://www.CNJ.jus.br/files/conteudo/arquivo/2016/02/a233219a89b8b0bbbf4d00f328d3e9c8.pdf

[83] *20. Em quanto não for instalado o Centro Judiciário de Solução de Conflitos e Cidadania (Cejusc), as sessões de mediação e conciliação processuais e pré-processuais poderão ser realizadas por meio audiovisual, em módulo itinerante do Poder Judiciário ou em entidades credenciadas pelo Núcleo Permanente de Métodos Consensuais de Solução de Conflitos (Nupemec), no foro em que tramitar o processo ou no foro competente para o conhecimento da causa, no caso de mediação e conciliação pré-processuais.*

58 A conciliação/mediação, em meio eletrônico, poderá ser utilizada no procedimento comum e em outros ritos, em qualquer tempo e grau de jurisdição.

70 Quando questionada a juridicidade das decisões tomadas por meio de novas tecnologias de resolução de controvérsias, deve-se atuar com parcimônia e postura receptiva, buscando valorizar e aceitar os acordos oriundos dos meios digitais.

82 O Poder Público, o Poder Judiciário, as agências reguladoras e a sociedade civil deverão estimular, mediante a adoção de medidas concretas, o uso de plataformas tecnológicas para a solução de conflitos de massa.

[84] *Art. 7º. Os CEJUSC-JT contarão com um magistrado coordenador e, sendo necessário, juiz(es) supervisor(es), todos entre Juízes com atuação nas respectivas sedes, indicados fundamentadamente em critérios objetivos pelo Presidente do respectivo Tribunal, aos quais caberá a administração, supervisão dos serviços dos conciliadores e mediadores e a homologação dos acordos.* ***[...]*** *§ 6º. As conciliações e mediações realizadas no âmbito da Justiça do Trabalho somente terão validade nas hipóteses previstas na CLT, aí incluída*

Tímidamente se limitó a crear un portal para conciliación laboral con poca interacción con las partes involucradas en el conflicto laboral.[85] Por lo expuesto, se observa que existe un deseo de incentivar la resolución consensual de conflictos y uso de TIC(s) en el ámbito del poder judicial brasileño, pero en diferentes grados y ritmos. Mientras que los jueces de los estados federados y los jueces federales de otras especialización del derecho están más abiertos a los mediadores externos al poder judicial, el uso de Tic(s) y ODR, la justicia federal especializada en conflictos laborales se muestra centralizadora, adversa al reconocimiento de particulares actuando como intermediarios para solución de conflictos laborales entre empleados y empleadores y al uso de TIC(s) y ODR.

PLATAFORMAS BRASILENÃS PARA LA RESOLUCIÓN ALTERNATIVA DE CONFLICTOS POR MEDIO DE ODR: EL PORTAL DE CONCILIACIÓN DEL CONSEJO NACIONAL DE JUSTICIA Y PLATAFORMAS PRIVADAS

A diferencia del portal creado por CNJT, CNJ ha desarrollado una plataforma de ODR cuya operación se inició en junio de 2016 con un enfoque en las causas de consumidor bancario, estando posteriormente disponible para todos aquellos consumidores que estén interesados en utilizar la plataforma. Es una plataforma intuitiva y funcional asincrónica, es decir, las partes interactúan en el momento que deseen mediante el envío de mensaje dentro del sistema y/o por teléfono.

Fuente: http://www.CNJ.jus.br/mediacaodigital/

Siguiendo la tendencia global de la promoción de la composición consensuada entre las partes, algunas empresas y entidades ya ofrecen el servicio de ODR en Brasil. CLAMARB – Cámara Latinoamericana de Mediación y Arbitraje (www.clamarb.com.br), la plataforma ODR de la

*a homologação pelo magistrado que supervisionou a audiência e a mediação pré-processual de conflitos, sendo inaplicáveis à Justiça do Trabalho as disposições referentes às Câmaras Privadas de Conciliação, Mediação e Arbitragem, e normas atinentes à conciliação e mediação extrajudicial e pré-processual previstas no NCPC. (*CONIMA**.** **CJF publica por completo de las 87 declaraciones aprobadas en el I viaje prevención y solución extrajudicial de litigios.** [Consulta en: 30 Ago. 2017] Disponible en: http://www.Conima.org.br/arquivos/13695)

[85] *Art. 14. Fica criado o Portal da Conciliação Trabalhista, a ser disponibilizado no sítio do CSJT na rede mundial de computadores, com as seguintes funcionalidades, entre outras: I - publicação das diretrizes da capacitação de conciliadores e mediadores e de seu código de ética; II - relatório gerencial do programa, por Tribunal Regional do Trabalho, detalhado por unidade judicial e por CEJUSC-JT; III – compartilhamento de boas práticas, projetos, ações, artigos, pesquisas e outros estudos; IV – fórum permanente de discussão, facultada a participação da sociedade civil; V – divulgação de notícias relacionadas ao tema; e PODER JUDICIÁRIO JUSTIÇA DO TRABALHO CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO VI – relatórios de atividades da "Semana da Conciliação Trabalhista". Parágrafo único. A implementação do Portal será de responsabilidade do CSJT.*

Fundación Getúlio Vargas para la mediación y el arbitraje (http://mediacao.fgv.br/), ITKOS (http://www.itkos.com.br/) e ResolvJá (www.resolvja.com.br). El sistema de mediación y arbitraje de FGV fue contratado por el grupo OI, uno de los más grandes grupos empresariales del mundo en el ramo de telecomunicaciones, para negociar con miles de pequeños acreedores del mayor proceso de recuperación judicial que se ha escuchado en la historia de Brasil[86]. Este procedimiento no tiene precedentes, porque es la primera vez que el poder judicial, en el caso, representado por el Tribunal de Recuperación Judicial del estado federado de Río de Janeiro, aceptó mediación entre una empresa en recuperación judicial y sus acreedores.

Además, otro factor de ineditisimo es la mediación por medio de la plataforma de solución de conflictos en línea de la Fundación Getúlio Vargas (FGV). Estos pequeños acreedores, que tienen crédito de hasta R$ 50.000,00 para recibir, representan 53.000 de los 55.000 acreedores enumerados en la lista de acreedores del plan de recuperación judicial. Finalmente, y lo más emocionante para los entusiastas de ODR, es la inclusión de créditos resultantes de procesos laborales en el procedimiento consensuado de resolución de conflictos a través de ODR con el sello del Tribunal Laboral del estado federado de Rio de Janeiro (TRT01). La única diferencia entre las composiciones de créditos laborales de las composiciones de créditos de otra naturaleza es que, en el caso de créditos laborales, el acuerdo debe pasar por la aprobación de la Justicia Laboral.

Fuente: Https://www.credor.OI.com.br/login

EL USO DE LAS TIC(S) PARA RESOLVER CONFLICTOS LABORALES EN BRASIL: LA JUSTICIA DEL TRABAJO EN NÚMEROS

Existe un alto costo mantener la estructura de la Justicia laboral brasileña estructurada en 1.570 juicios, 41.747 empleados públicos y 14.946 trabajadores privados auxiliares. Este estudio mostró que el 91,9% de los costos de la justicia laboral en 2015 fue con el pago de los gastos de recursos humanos, 8,1% con gastos corrientes y de capital, totalizando R$16,5 millones de reales. Todavía,

[86] COCHE, Rodrigo. El poder judicial autoriza el uso de la mediación en el proceso de OI. Disponible en: <Http://www.valor.com.br/legislacao/5017754/judiciario-autoriza-uso-de-mediacao-em-processo-da-OI > Access on: 30 Ago. 2017.

de acuerdo con el informe de la justicia en números del año de 2016[87], el 31,1% de las sentencias dictadas en la justicia laboral son homologatorias de acuerdos, es decir que, a cada diez sentencias de justicia laboral, en promedio 03 fueron homologatorias de acuerdo.

Estos datos generan inevitablemente preguntas prácticas. La primera es: ¿realmente necesitamos que estos acuerdos pasen a través de la aprobación de un juez estatal? ¿No hay posibilidad de que las partes lleguen a la composición mediante resoluciones alternativas (al poder judicial) para poner fin al conflicto? ¿la racionalización de los recursos humanos en la justicia del trabajo mediante la utilización de resoluciones alternativas de conflictos no reduciría los costos y daría más eficacia a la Justicia Laboral, cuyos empleados y jueces podían dedicarse a otras actividades judiciales, a ejemplo de procesar y juzgar los recursos?

LAS EXPERIENCIAS DE LA JUSTICIA LABORAL EN EL USO DE MÉTODOS DE RESOLUCIÓN DE CONFLICTOS

Gran parte de los magistrados y tribunales de trabajo abogan por la supremacía ilimitada del poder judicial en la prestación de validez jurídica a las composiciones extrajudiciales en materia laboral. [88] Algunos argumentan que el juez no estaría obligado a aprobar la conciliación, porque esto no sería un derecho de las partes, sino un acto judicial que proviene de la libre convicción del magistrado, que debe presentar su motivación si entiende no aprobar la composición. [89] SCHIAVI[90] llega al extremo de poner la aprobación del acuerdo extrajudicial por el magistrado como una excepción que se llevará a cabo con mucha cautela, en sus palabras: *"De outro lado, pensamos que o Juiz do Trabalho deva tomar algumas cautelas para homologar eventual transação extrajudicial. Deve designar audiência, inteirar-se dos limites do litígio e ouvir sempre o trabalhador. Acreditamos que somente em casos excepcionais deve o juiz homologar acordo extrajudicial envolvendo matéria trabalhista"*. SENA[91], en un artículo sobre formas de resolución de conflictos y acceso a la justicia, concluye que la *"juiz do trabalho não é um mero 'homologador passivo' de todo e qualquer acordo que lhe seja submetido pelos litigantes (arts. 125, III e 129 do CPC), nem muito menos um espectador do que as partes querem e pretendem fazer no e do processo".* Cabe señalar que, en el caso de SENA, ni siquiera se considera una aprobación de un acuerdo sin proceso, es decir, una solicitud espontánea hecha por las partes de aprobación de conformidad con el poder judicial para dar mayor certidumbre jurídica con el sello del Poder Judicial. Y aquí hay una primera crítica. La forma de actuar del poder judicial, resultante de este pensamiento erróneo, fomenta empleados y empleadores a llevar a cabo procesos simulados.

Con respecto al uso de arbitraje en los conflictos laborales individuales, no hay unanimidad de entendimiento. Hay aquellos que entienden que el arbitraje es posible, mediante la aplicación de la ley de arbitraje brasileña; otros que admiten el arbitraje, pero mantienen que es necesario legislación diferenciada para el derecho laboral; los que niegan cualquier posibilidad de empleo de arbitraje y los que admiten el arbitraje siempre que no se refieran a los derechos no disponibles consagrados en la *Consolidação das Leis Trabalhistas* brasileñas.[92] [93]

---

[87] Ibidem p. 180
[88] Op. cit. MARTINS, p. 25.
[89] SCHIAVI, M. **Manual de derecho procesal de trabajo**. 11. ed. Sao Paulo: LTR, 2016, p. 42-46.
[90] Ibidem, p. 46.
[91] SENA, Adriana Goulart de. **Formas de resolução de conflitos e acesso à justiça,** Belo Horizonte, v.46, n.76, p. 93 - 114, 2007. [Consulta en: 25 ago. 2017]. Disponible en: <http://www.trt3.jus.br/escola/download/revista/rev_76/Adriana_Sena.pdf>, p. 114.
[92] Op. cit. CARMONA, P. 57 y 58.
[93] La doctrina y la jurisprudencia abogan por la limitación del uso del arbitraje en las operaciones laborales basadas en los artículos 9, 444, 468 y 477 de la consolidación de las leyes laborales.

Hasta el momento de la preparación del presente trabajo académico, se pudo constatar que o TST - Tribunal Superior Laboral brasileño, órgano máximo de esta justicia especializada en Brasil, acepta el arbitraje en el área laboral de manera extremadamente restringida, aceptando solamente en conflictos colectivos[94], excluyendo el reconocimiento de la arbitraje en conflictos individuales, de acuerdo con varios juzgados del TST, que no reconocen la sentencia arbitral en estos casos[95]. Contrariamente a la jurisprudencia del TST, se destaca la reciente decisión del Tribunal Regional Laboral de primera región (TRT1, que comprende el estado federado del Rio de Janeiro), proceso nº 0010989-82.2015.5.01.0003 (RO), reportado por el juez Enoc Ribeiro dos Santos, en el que se reconoce validez de la cláusula de arbitraje[96] e llama atención sobre el empleo de Arbitraje en asuntos laborales en varios países, verdadera recopilación de experiencias positivas en el mundo.[97]

Se puede ver que los métodos alternativos de resolución de conflictos y ODR(s) están de moda en el derecho internacional y brasileño. Por otro lado, es evidente la resistencia de la mayoría de los jueces de trabajo y del TST en el reconocimiento de la posibilidad de composición realizada por terceros, lo que disminuye la seguridad jurídica en estos métodos alternativos de resolución extrajudicial de los conflictos, debilitándoles. Eso es lo que explica CARMONA[98]:

> *Ainda uma última palavra sobre as restrições à arbitragem em matéria trabalhista: é indisfarçável uma certa antipatia (política, sobretudo!) Dos doutrinadores juslaboralistas em relação à solução arbitral de conflitos especializados, e isto apesar de larga utilização do instituto em paragens estrangeiras. Nos Estados Unidos da América o instituto é de*

---

[94] El arbitraje para solución de conflictos colectivos está expresamente previsto en el § 1 del artículo 114 del CRFB.

[95] TST. ***Tribunal Superior do Trabalho. (AIRR-633-96.2013.5.02.0382, Relator: José Roberto Freire Pimenta, fecha de juicio: 28/03/2017, 2ª clase, fecha de publicación: DEJT 31/03/2017);*** (AIRR-1357-93.2012.5.02.0040, fecha del juicio: 20/8/2014, Ministro Relator: Américo Bede Freire, 6ª clase, fecha de publicación: DEJT 22/8/2014); (E-RR-217400-10.2007.5.02.0069, fecha del juicio: 25/4/2013, Ministro Relator: Lelio Bentes Corrêa, subdivisión I se especializa en colectivo individual, fecha de publicación: DEJT 3/5/2013)

[96] TRT. Tribunal Regional do Trabalho. **Procedimientos extintos en caso de que no se apruebe por arbitraje**. [Consulta en: 03 set. 2017]. Disponible en: http://www.trt1.jus.br/web/Guest/destaque-completo?nID=60091154

[97] *a) Na Alemanha, o árbitro exerce função pública em instituições de natureza extrajudicial, os Contratos Coletivos de natureza jurídica são sujeitos a arbitragem. E os de âmbito geral são submetidos à livre negociação. Prevalece, na Alemanha, uma Comissão formada por trabalhadores ou por Delegados Judiciais que funcionam junto à Organização Interna da Empresa (disponível em: http://jus.com.br/artigos/38104/solucoes-alternativasde-conflitos-a-arbitragem-aplicada-aos-dissidios-trabalhistas); b) Na Espanha, a Lei nº 36/98 define que, por meio da Convenção arbitral, as partes obrigam-se ao juízo arbitral, excluindo do Judiciário as questões submetidas ao árbitro (disponível em: http://jus.com.br/artigos/38104/solucoes-alternativas-de-conflitos-aarbitragem-aplicada-aos-dissidios-trabalhistas); c) Na França, a Convenção Coletiva ou o Acordo Coletivo de Trabalho pode prever um procedimento contratual de arbitragem (arts. L-525-1 a L-525-9 Cod. Trabalho). Assim, a arbitragem é um ato de vontade dos representantes das categorias (disponível em: http://jus.com.br/artigos/38104/solucoes-alternativas-de-conflitos-a-arbitragem-aplicadaaos-dissidios-trabalhistas); d) Austrália e Nova Zelândia adotam o sistema arbitral compulsório (disponível em: http://jus.com.br/artigos/38104/solucoes-alternativas-de-conflitos-a-arbitragem-aplicadaaos-dissidios-trabalhistas); e) No México, a maior parte dos conflitos trabalhistas têm solução pela Junta de Conciliação e Arbitragem, que pertence ao Poder Executivo. Então, temos aqui uma arbitragem pública não exercida pelo Poder Judiciário, mas sim, pelo Executivo (disponível em: http://jus.com.br/artigos/38104/solucoes-alternativas-de-conflitos-aarbitragem-aplicada-aos-dissidios-trabalhistas); f) No Chile, a arbitragem foi Instituída pela Lei n. 19.069/91. A arbitragem é facultativa e pode ocorrer durante qualquer fase da negociação coletiva; obrigatória, no entanto, nos conflitos com greve em atividades essenciais (disponível em: http://jus.com.br/artigos/38104/solucoes-alternativas-de-conflitos-a-arbitragem-aplicadaaos-dissidios-trabalhistas); g) Na Argentina, a arbitragem foi promovida pelo Ministério do Trabalho através da Lei n. 14.786/58; após tentativa frustrada de mediação, o mediador convida as partes a que se submetam a uma arbitragem, tendo o laudo arbitral os mesmos efeitos das convenções coletivas. Existe, também, a eqüidade sobre conflitos como salário, condições de trabalho, que não sejam fixados por lei (disponível em: http://jus.com.br/artigos/38104/solucoesalternativas-de-conflitos-a-arbitragem-aplicada-aos-dissidios-trabalhistas); h) No Uruguai, reconhece-se a validade de cláusulas arbitrais desde o Tratado de Direito Processual de 1889. Posteriormente, o país foi o primeiro, entre os Membros do MERCOSUL, a ratificar os acordos internacionais relativos à arbitragem.*

[98] Op. cit. CARMONA, p. 60 y 61.

> *larguíssima utilização, sendo por todos reconhecida sua vantagem em relação à solução judicial dos conflitos. Chega-se mesmo a constatar que a arbitragem é o meio de solução de conflitos individuais de trabalho mais utilizado entre empregados sindicalizados e empregadores, tudo graças à tradição norte-americana que estimulou intervenção apenas subsidiária do governo nas relações trabalhistas. Diferentemente do que ocorreu no Brasil, os norte-americanos não receberam direitos, conquistaram-nos, de tal sorte que os sindicatos restaram historicamente fortalecidos, o que decididamente não aconteceu em nosso país.*

También es lúcida la crítica de DIDIER[99]:

> *É curioso, e um tanto contraditório, como processualistas estufam o peito para falar de democratização do processo, defendendo técnicas de facilitação do acesso à justiça, p. ex., e, simultaneamente, ignoram o papel da liberdade, pilar da democracia, no processo. Discurso que afasta a liberdade do ambiente processual tem ranço autoritário. Processo e liberdade convivem. Liberdade não é nem pode ser palavra maldita na Ciência do Direito Processual e no próprio Direito Processual Civil.*

Cuanto al uso de métodos alternativos de resolución de conflictos por medio de ODR en el campo laboral, aunque ODR sea reconocido en todo el mundo como método efectivo para la composición en todas las áreas del derecho, a ejemplo de derecho de familia y consumidor, lo que se observa es una desconfianza muy grande por parte del judiciario laboral brasileño.

8. CONSIDERACIONES FINALES

¿Cuál es la vida media de un trabajador brasileño? 60, 70, 80 años? ¿Cuál es la duración media de un proceso laboral hasta el resultado judicial efectivo? ¿05, 10, 15 años? Ahora, en un cálculo simple, ¿cuál es el significado de un ser humano perder de 10% a 30% del tiempo de su vida con las molestias, cuando no frustraciones, de un proceso judicial? ¿Cuál es el significado de hasta el 30% del tiempo de los empleados e jueces de la Justicia Laboral serán destinados a las actividades de resolución de conflictos que podrían ser manejados en una fase de pre-proceso o por particulares por medio de ODR(s)? Sin mencionar los gastos inherentes al mantenimiento de estos procesos. La respuesta a todas estas preguntas es que no ha sentido la pérdida de tanto tiempo y recursos. Sin embargo, el Poder Judiciario Laboral brasileño no coopera para que los trabajadores y los empleadores tengan una postura diferente en el litigio, ya que no garantiza la seguridad jurídica de los métodos alternativos de resolución de conflictos realizados por entidades ajenas al poder judicial Trabajo.

El entendimiento de la mayoría de los jueces de Justicia laboral es dotado de prejuicios sobre el *modus operandi* de las entidades privadas acreditadas para el procedimiento de arbitraje, en el sentido de no estarían siendo garantidos el debido proceso a los empleados, y, por lo tanto, sería un peligro para el principio de protección del trabajador y el principio de los derechos no disponibles. De hecho, en vista de un escenario tan desfavorable para la plena aceptación de métodos alternativos de resolución de conflictos por parte del poder judicial laboral brasileño, es realmente un desafío ampliar este debate para el uso de ODR(s). Ocurre que ODR(s) ya están entre nosotros, nos guste o no. Es una marcha adelante y acelerada, intrínseca al desarrollo de la sociedad. Aceptación del uso de TIC por la sociedad y por la propia Justicia Laboral en la solución de situaciones cotidianas es innegable, a veces de manera obvia, a veces no.

Varios servicios están a disposición de los ciudadanos en los portales gubernamentales y la Justicia Laboral reconoce el teletrabajo, incluso para sus servidores. De una manera no evidente para muchas

[99] Op. cit. Didier Júnior, p. 33.

personas, hay el uso de TIC en softwares como Facebook, donde hay una inteligencia artificial que consiste en un algoritmo que analiza las preferencias por medio de "*likes*", "*dislikes*" y por análisis de los textos escritos por los usuarios. Basándose en este análisis, el Facebook ofrece productos de una manera dirigida al público que muestre interés en un determinado tema, entre otras posibilidades de obtener ventajas, porque no sólo es económico, también hay la generación de un conocimiento que puede ser utilizado para otros propósitos. Otro ejemplo práctico es el servicio de robots/Interaction con el usuario en las plataformas de internet. Un buen ejemplo es la plataforma de Empresa de certificación de firma digital CERTISIGN, para clarificar dudas de consumidores, y la aplicación Tinder[100].

Además, hay otras posibilidades: ¿Y si la inteligencia artificial tiene la capacidad de mediar la buena relación entre las partes, incluso antes de la instalación de un conflicto, a través de una negociación de la naturaleza cooperativa, usando plataformas para identificar emociones por expresiones faciales? O ayudar a los departamentos de recursos humanos? Tales suposiciones no son ciencia ficción. Hay que tener en cuenta lo rápido que ha cambiado el mundo recientemente. En 1990 personas no utilizaron las redes sociales o los teléfonos celulares.[101] Facebook, por ejemplo, fue creado en 2004 y hoy es una de las empresas de tecnología líder en el mundo con 2 billones de usuarios. Según el científico, inventor y futurista KURZWEIL[102], el mundo va a cambiar aún más en un futuro próximo en una trayectoria exponencial hacia la evolución tecnológica, en un fenómeno en el que se describe cómo utilizar los ordenadores y herramientas de una época para crear una forma acelerada y exponencial de las máquinas de la siguiente generación en un proceso continuo. Ya se habla, incluyendo, de e-personalidad, de conformidad con las recomendaciones relativas a la legislación civil sobre robótica formulada por el Parlamento Europeo en febrero de 2017, en la actualidad repelida enérgicamente por el CESE (Comité económico y social europeo).[103]

Es necesario poner fin a la idea falsa que el Poder Judicial es la única solución posible para Conflictos laborales. Es necesario dar crédito a las instituciones que promueven la autocomposición, a los empleados y a los empleadores. Es cierto que algunos abusarán de la libertad que les será concedida, pero no hay progreso sin efectos secundarios. Para estos habrá una legislación con sanciones para los otros fallos cometidos. Una vez que esta resistencia del Poder Judicial se rompa en relación a las entidades responsables por el arbitraje y mediación de los conflictos entre empleados y empleadores, se piensa que será posible entrar en una nueva fase, la de las resoluciones consensuales de los conflictos laborales mediante el uso de TIC(s), principalmente ODR(s), proporcionando velocidad y economía para las partes, el estado, y en consecuencia, para la sociedad.

---

[100] Tinder es una aplicación diseñada para promover la interacción de las personas con fines de amistad, relaciones afectivas o sexuales. Algunos usuarios hacen uso de una aplicación de robots (llamado Bernie) que lanza automáticamente preguntas y respuestas genéricas, dando la sensación al interlocutor de que existe un diálogo continuo. El objetivo es prospectar la mayor cantidad de actores posibles, ampliando las posibilidades del usuario de tener éxito en la interacción deseada. "O **Bernie** é um aplicativo que busca conquistar usuários com uma premissa interessante – e futurista. Usando **inteligência artificial**, o programa busca entender sua preferência de parceiro romântico para **usar o Tinder automaticamente**. Segundo os criadores, o App opera 24 horas por dia para filtrar sugestões, dispensando pessoas indesejadas e aumentando suas chances de obter *match*. " (ALVES, Paulo. Bernie é uma inteligência artificial que usa o Tinder por você. [Consulta en: 15 ago. 2017]. Disponible en: https://www.showmetech.com.br/bernie-e-uma-inteligencia-artificial-que-usa-o-tinder-por-voce/#ixzz4sHHSOgYA

[101] Op. cit. KURZWEIL (local Kindle 3785-3791).

[102] Ibídem (lugares de Kindle 3805-3810).

[103] Op. cit. DIARIOLALEY.

¿ES EL CIBERESPACIO UN TERRITORIO? REFLEXIONES SOBRE LA INTERNACIONALIDAD DE LOS CONTRATOS INFORMÁTICOS

Por: ***Francisco Flores***
Panamá

PREFACIO

El presente trabajo propone una mirada analítica a la actualidad del mundo del Derecho Informático o de la Informática en una de sus aristas más conocidas mundialmente, a saber: el comercio electrónico y la contratación telemática o por medios tecnológicos.

Siendo la Internet la red de redes, el desarrollo tecnológico producto de la globalización ha creado la realidad virtual que se concreta en el denominado ciberespacio, ese intangible que está adentro de las computadoras u ordenadores y que dentro del cual por el envío y recepción de mensajes transcurre esa interacción entre individuos, empresas y organizaciones dentro del ámbito de un determinado Estado y a nivel internacional.

La realidad del comercio electrónico en la era de la globalización y la sociedad post-industrial evoca una gran dosis de internacionalidad en las relaciones jurídicas vinculadas a los contratos informáticos o electrónicos.

Dentro del marco de la celebración en Panamá del Vigésimo Segundo Congreso de FIADI, el Decano de la Facultad de Derecho y Ciencias Políticas de la Universidad de Panamá, Doctor Hernando Franco Muñoz, ha tenido a bien designarme como Presidente del Comité Organizador en función de enlace con los organizadores del gremio panameño APANDETEC. Es por esta razón que mi agradecimiento va al Decano de la Facultad de Derecho y Ciencias Políticas por haberme tomado en cuenta para esta tarea.

También deseo hacer constar mi agradecimiento a todos y cada uno de los miembros del gremio panameño de las Nuevas Tecnologías APANDETEC, muy en particular a quienes una vez fueron alumnos míos y hoy los considero amigos y colegas el Profesor Augusto Ho y la Magistra Joselín Vos por contagiarme su entusiasmo y energía en la promoción del Derecho Informático que me hizo recordar mis tiempos de estudiante del Doctorado en Derecho de las Nuevas Tecnologías que tomé allá por los años 2004 y 2005 en la Universidad Pablo de Olavide de Sevilla, España.

Igualmente una cordial bienvenida a todos los participantes en el Vigésimo Segundo Congreso FIADI que es para mí un honor colaborar con estas líneas en el debate académico del evento que estamos seguros será profundamente fructífero.

INTRODUCCIÓN

Habiendo expuesto en el Prefacio los motivos que llevaron a la preparación de la presente ponencia, nos corresponde aclarar el orden de exposición de la temática que nos ocupará.

Con una visión analítica y crítica hemos dividido el escrito en tres apartados fundamentales. A título de marco conceptual y teórico el primer apartado expone el contexto en que opera el Derecho

Informático y explicitaremos resumidamente los aspectos fundamentales, la etimología y el concepto de la globalización, con el propósito de situar al lector en el medio que opera el comercio electrónico.

En un segundo apartado analizaremos el concepto del ciberespacio y su relación y entronque con la contratación en general y, en particular, la conceptualización básica y los principios de la contratación electrónica.

A continuación en el tercer apartado analizaremos brevemente la temática del Derecho Internacional Privado y la normativa que en Panamá se aplicará a los contratos electrónicos o en línea de acuerdo con la Ley 61 de 2015 que aprueba el Código de Derecho Internacional Privado de la República de Panamá y haremos los comentarios pertinentes. Finalizando con algunas conclusiones finales y el listado de referencias bibliográficas.

Partiendo del criticismo kantiano, se aplicarán los métodos analítico, sintético, inductivo y comparativo. Las fuentes de información utilizadas fueron en su totalidad documentales y se tomaron en cuenta libros en soporte papel, libros electrónicos, revistas electrónicas. En las fuentes legislativas se utilizó el Código de Derecho Internacional Privado, la Ley Modelo de *UNCITRAL* sobre Comercio Electrónico, otros instrumentos internacionales como la Convención de Viena de 1980 sobre Compraventa Internacional de Mercaderías así como algunas legislaciones extranjeras, particularmente la española.

1. LA GLOBALIZACIÓN: CONCEPTO Y ASPECTOS FUNDAMENTALES

1.1 Etimología de la expresión

La primera vez que se usó esta expresión vino de un libro escrito en 1962 por un canadiense profesor de literatura inglesa quien en vida se llamó Herbert MARSHALL MCLUHAN titulado *La Galaxia Gutenberg Génesis del "Homo Typographicus"* seguido por otro que vio la luz en el año 1964 cuyo título es *Comprender los medios de comunicación Las extensiones del ser humano.* En ambas obras el autor desarrolla la tesis que la revolución tecnológica del uso de la electricidad, los progresos científicos en el electromagnetismo y su uso en los aparatos electrónicos habían creado una *aldea global* y la nueva *Edad de la Información* introduciendo además, en el lenguaje común, la terminología *medios de comunicación* y su concepto.

Como lo expresó en la primera obra mencionada (MCLUHAN, 1972, p. 48) <<Pero es cierto que los descubrimientos electromagnéticos han hecho resucitar el "campo" simultáneo en todos los asuntos humanos, de modo que la familia humana vive hoy en las condiciones de "aldea global">>. Y en la segunda obra, muy cercana a la primera en la línea de argumentación, afirma que (MCLUHAN, 1996, p. 27)<<Eléctricamente contraído, el globo no es más que una aldea. La velocidad eléctrica con que se juntaron todas las funciones sociales y políticas en una implosión repentina ha elevado la conciencia humana de la responsabilidad en un grado intenso>>.

La alusión a la *aldea global* derivó en la noción de *globalización,* la cual en sí misma no era nueva sino que se hizo una reinterpretación de la misma por los eventos que se desencadenaron a nivel mundial en los años posteriores a la publicación de estas dos obras y que comenzaron a manifestarse con mayor fuerza a partir de la segunda mitad del siglo veinte hasta nuestros días.

1.2 Origen histórico del fenómeno

De acuerdo con FERRER (1997) el actual proceso de globalización es parte de un proceso mayor iniciado en 1492 con la conquista y colonización de gran parte del mundo por parte de Europa.

Otros textos (GLOBALIZACIÓN, 2017) mencionan, por ejemplo, que pensadores como Rüdiger Safranski destacan que a partir de la explosión de la bomba atómica en Hiroshima en 1945 nació una comunidad global unida en el terror a un holocausto mundial. También se ha asociado el inicio de la globalización a la invención del chip electrónico (12 de septiembre de 1958), la llegada del hombre a la Luna, que coincide con la primera transmisión mundial vía satélite (20 de julio de 1969), o la creación de Internet (1 de septiembre de 1969). Pero en general se ubica el comienzo de la globalización con el fin de la Guerra Fría, cuando desaparece la Unión Soviética y el bloque comunista que encabezaba, cuyo experimento fallido de colectivismo representaba el ocaso de los proyectos de sociedades cerradas y economías protegidas. Si bien la autodisolución de la Unión Soviética se produjo el 25 de diciembre de 1991, se ha generalizado simbolizarla con la caída del Muro de Berlín el 9 de noviembre de 1989.

1.3 Elementos esenciales que integran el concepto

La doctrina más autorizada (CADENAAFANADOR, 2001, pp. 101-103) (FERRER, 1997, p. 13) (GLOBALIZACIÓN, 2017) sustenta que existen varios aspectos que pueden servir para caracterizar el fenómeno de la globalización, que se refieren a la influencia que el proceso ha tenido en distintas áreas de la vida humana que son los que a continuación se mencionarán.

1.3.1 Globalización y Economía

1.3.1.1 La "Nueva Economía"

En cuanto a la influencia de la globalización en la economía hoy día se habla de la "Nueva Economía" *(New Economy)*. En su sentido etimológico la palabra economía viene del latín *oeconomĭa*, y éste del griego οἰκονομία *oikonomía*, de οἶκος *oîkos*, «casa», y νόμος *nomos*, «ley» y el significado técnico genérico nos dice que es la ciencia social que estudia los siguientes asuntos: la extracción, producción, intercambio, distribución y consumo de bienes y servicios; la forma o medios de satisfacer las necesidades humanas mediante recursos que son escasos y pueden ser destinados a diferentes usos; y la forma en la que las personas y sociedades sobreviven, prosperan y funcionan, en este sentido es nuestro modo de relación con la Naturaleza.

En economía, el mercado es un conjunto de transacciones de procesos o intercambio de bienes o servicios entre individuos. El mercado no hace referencia directa al lucro o a las empresas, sino simplemente al acuerdo mutuo en el marco de las transacciones. Debe interpretarse como la institución u organización social a través de la cual los ofertantes (productores, vendedores) y los demandantes (compradores o consumidores) de un determinado tipo de bien o de servicio, entran en estrecha relación comercial a fin de realizar abundantes transacciones comerciales. Como es sabido, el concepto de mercado deriva etimológicamente del latín *mercatus* que significa comercio, negocio y tradicionalmente se define como un lugar público o una reunión periódica de vendedores y compradores.

Así como en la economía tradicional existe un punto de convergencia de los factores y fuerzas económicas, el entorno digital también tiene un nuevo mercado: el digital, que ha sido desarrollado por la revolución tecnológica de la aplicación de la electrónica a los medios de comunicación.

Por lo anterior es que MCLUHAN afirmó (1996, p. 41; 56) en sus obras, entre otras tesis, que <<Los medios tecnológicos son materias primas o recursos naturales, igual que el carbón, el algodón y el petróleo>> <<En la nueva Edad de la Información eléctrica y de producción programada, los bienes mismos asumen cada vez más un carácter de información; esta tendencia se manifiesta sobre todo en los presupuestos cada vez más importantes para publicidad>> y <<A medida que suban los niveles

de información eléctrica, casi cualquier material servirá a todo tipo de necesidad o función, empujando cada vez más al intelectual hacia un papel de mando social y al servicios de la producción>>.

La influencia que la revolución tecnológica ha tenido en la economía se ve, por ejemplo, en el aumento del comercio internacional de bienes tecnológicos, el aumento de las inversiones privadas en tecnología por las corporaciones transnacionales, el crecimiento enorme de los mercados financieros globales y la liberalización del marco regulatorio desde finales de la Segunda Guerra Mundial con la fundación del antiguo GATT hoy OMC para la reducción de los aranceles aduaneros aunque esto último es una paradoja dado que los países industriales mantienen barreras arancelarias y no arancelarias sobre los productos agrícolas de clima templado y otros bienes intensivos en el uso de mano de obra donde los llamados países en desarrollo tienen ventajas comparativas.

1.3.1.2 El comercio electrónico (e-commerce)

Este desarrollo es el que ha provocado la aparición del comercio electrónico que puede conceptualizarse, en términos generales, como el conjunto de intercambios comerciales mediados por la tecnología entre diversas partes (individuos, organizaciones o ambos), así como las actividades electrónicas dentro y entre organizaciones que facilitan esos intercambios. El comercio electrónico, también conocido como *e-commerce* (*Electronic commerce* en inglés) o bien negocios por Internet o negocios *online* o negocios en línea, consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas. Originalmente, el término se aplicaba a la realización de transacciones mediante medios electrónicos tales como el Intercambio electrónico de datos; sin embargo con el advenimiento de la Internet y de la *World Wide Web,* a mediados de la década de 1990 comenzó a referirse principalmente a la venta de bienes y servicios a través de Internet, usando como forma de pago medios electrónicos tales como las tarjetas de crédito. (COMERCIOELECTRÓNICO, 2018)

1.3.2 Globalización y Tecnología

1.3.2.1 Telecomunicaciones

De acuerdo con la fuente de información consultada (TELECOMUNICACIÓN, 2013)La telecomunicación, o telecomunicaciones indistintamente, es el estudio y aplicación de la técnica que diseña sistemas que permitan la comunicación a larga distancia a través de la transmisión y recepción de señales. Típicamente estas señales se propagan a través de ondas electromagnéticas, pero es extensible a cualquier medio que permita la comunicación entre un origen y un destino como medios escritos, sonidos, imágenes o incluso personas.

En la telecomunicación se incluyen muchas tecnologías como la radio, televisión, teléfono y telefonía móvil, comunicaciones de datos y redes informáticas, como Internet. Estas tecnologías son de vital importancia en el contexto socioeconómico actual, sobre todo si valoramos su utilidad en conceptos como la globalización o la sociedad de la información. De hecho, una gran familia de estas tecnologías, enfocadas a un consumo no profesional, ha convergido en las llamadas tecnologías de la información y la comunicación, que forman ya parte del currículo educativo en muchos países.

El término «telecomunicación» tiene su origen en el francés *Télécommunication,* palabra que inventó el ingeniero Édouard Estaunié al añadir a la palabra latina *communicare* —compartir— el prefijo griego *tele*, que significa distancia. Con este término pretendía usar una misma palabra para denominar a la «transmisión del conocimiento a distancia mediante el uso de la electricidad», que hasta ese momento era la telegrafía y la telefonía, y lo publicó por primera vez en *Traité Practique de Télécommunication Électrique (Télégraphie-Téléphonie)* de 1904.

La consolidación real del término a nivel internacional llegó con la constitución de la Unión Internacional de Telecomunicaciones (UIT) en la Conferencia de Madrid de 1932, en la que se definió «telecomunicación» como «toda comunicación telegráfica o telefónica de signos, señales, escritos, imágenes y sonidos de cualquier naturaleza, por hilos, radio u otros sistemas o procedimientos eléctrica o visual (semáforos)». El avance de la telecomunicación acabó por dejar desfasada esta definición y, en el actual Reglamento de Radiocomunicaciones, se redefine el término: ≪ Telecomunicación: Toda transmisión, emisión o recepción de signos, señales, escritos, imágenes, sonidos o informaciones de cualquier naturaleza por hilo, radioelectricidad, medios ópticos u otros sistemas electromagnéticos (CS). ≫ Por metonimia, el estudio de la telecomunicación o las telecomunicaciones se denomina «Telecomunicación» o «Telecomunicaciones» indistintamente.

1.3.2.2 Computadora u Ordenador

Una definición estandarizada que se puede encontrar en la red (COMPUTADORA, 2013) nos dice que una computadora o computador (del inglés *Computer* y éste del latín *computare* -calcular), también denominada ordenador (del francés *ordinateur,* y éste del latín *ordinator*), es una máquina electrónica que recibe y procesa datos para convertirlos en información útil. Una computadora es una colección de circuitos integrados y otros componentes relacionados que puede ejecutar con exactitud, rapidez y de acuerdo a lo indicado por un usuario o automáticamente por otro programa, una gran variedad de secuencias o rutinas de instrucciones que son ordenadas, organizadas y sistematizadas en función a una amplia gama de aplicaciones prácticas y precisamente determinadas, proceso al cual se le ha denominado con el nombre de programación y al que lo realiza se le llama programador.

La computadora, además de la rutina o programa informático, necesita de datos específicos (a estos datos, en conjunto, se les conoce como *"Input"* en inglés o de entrada) que deben ser suministrados, y que son requeridos al momento de la ejecución, para proporcionar el producto final del procesamiento de datos, que recibe el nombre de *"output"* o de salida. La información puede ser entonces utilizada, reinterpretada, copiada, transferida, o retransmitida a otra(s) persona(s), computadora(s) o componente(s) electrónico(s) local o remotamente usando diferentes sistemas de telecomunicación, que puede ser grabada, salvada o almacenada en algún tipo de dispositivo o unidad de almacenamiento.

La característica principal que la distingue de otros dispositivos similares, como la calculadora no programable, es que es una máquina de propósito general, es decir, puede realizar tareas muy diversas, de acuerdo a las posibilidades que brinde los lenguajes de programación y el *hardware.*

1.3.2.3 Internet

De la historia de Internet se puede decir (HISTORIADEINTERNET, 2013) que se remonta al temprano desarrollo de las redes de comunicación. La idea de una red de ordenadores diseñada para permitir la comunicación general entre usuarios de varias computadoras sea tanto desarrollos tecnológicos como la fusión de la infraestructura de la red ya existente y los sistemas de telecomunicaciones. La primera descripción documentada acerca de las interacciones sociales que podrían ser propiciadas a través del *networking* (trabajo en red) está contenida en una serie de memorándums escritos por J.C.R. Licklider, del *Massachusetts Institute of Technology,* en agosto de 1962, en los cuales Licklider discute sobre su concepto de *Galactic Network* (Red Galáctica).

En octubre de 1962, Licklider fue nombrado jefe de la oficina de procesado de información DARPA, y empezó a formar un grupo informal dentro del DARPA del Departamento de Defensa de los Estados Unidos para investigaciones sobre ordenadores más avanzadas. Como parte del papel de la oficina de

procesado de información, se instalaron tres terminales de redes: una para la *System Development Corporation* en Santa Mónica, otra para el Proyecto *Genie* en la Universidad de California (Berkeley) y otra para el proyecto *Multics* en el Instituto Tecnológico de Massachusetts. La necesidad de Licklider de redes se haría evidente por los problemas que esto causó.

Como principal problema en lo que se refiere a las interconexiones está el conectar diferentes redes físicas para formar una sola red lógica. Durante los años 60, varios grupos trabajaron en el concepto de la conmutación de paquetes. Normalmente se considera que Donald Davies *(National Physical Laboratory),* Paul Baran *(Rand Corporation)* y Leonard Kleinrock *(MIT)* han inventado simultáneamente el concepto.

Los orígenes de Internet se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos y se considera a sus fundadores a los investigadores Vint Gray Cerf (VINTCERF, 2013) quien inició el desarrollo de las direcciones IP para la transmisión de informaciones en la red y Robert Elliot Kahn quien desarrolló el protocolo de control de transmisión (TCP) que es el actual transmisor de datos en la red (ROBERTKAHN, 2013).

Internet es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial.

Uno de los servicios que más éxito ha tenido en Internet ha sido la World Wide Web (WWW, o "la Web"), hasta tal punto que es habitual la confusión entre ambos términos. La WWW es un conjunto de protocolos que permite, de forma sencilla, la consulta remota de archivos de hipertexto. Ésta fue un desarrollo posterior (1990) y utiliza Internet como medio de transmisión.

Existen, por tanto, muchos otros servicios y protocolos en Internet, aparte de la Web: el envío de correo electrónico (SMTP), la transmisión de archivos (FTP y P2P), las conversaciones en línea (IRC), la mensajería instantánea y presencial, la transmisión de contenido y comunicación multimedia-telefonía (VoIP), televisión (IPTV), los boletines electrónicos (NNTP), el acceso remoto a otros dispositivos (SSH y Telnet) o los juegos en línea, entre otros. (INTERNET, 2013)

Para finalizar este apartado podemos decir que si tomamos en cuenta que la Internet facilita la reunión de vendedores, prestadores de servicios, clientes y, en general, a todos los operadores que ofrecen una amplia gama de productos y servicios, ésta ha contribuido notablemente a la creación de un mercado electrónico o digital en el mundo actual.

1.3.3 Globalización y Sociedad: la Sociedad de la Información (SI)

Algunos antecedentes históricos que podemos mencionar de este fenómeno, según las fuentes consultadas, (ROJO VILLADA, 2003) (BECERRA, 1999) (BANGEMANN, 1994) tenemos en primera instancia el *Plan Gore* (1988-1992): conocido como el *Plan Marshall Global* fue diseñado por el ex Vice Presidente de los Estados Unidos en su libro *Earth in the Balance: Ecology and the Human Spirit* que da ideas específicas para salvar el ambiente global. En la parte de la tecnología recomienda el rápido desarrollo de tecnologías que sean apropiadas ambientalmente hablando, es decir, sostenibles y que no dañen el medio ambiente. Gore es el creador de la expresión *autopistas de la información.*

Luego aparece el Plan Delors (1993): surge a través del *Libro Blanco del empleo y los retos del siglo XXI* elaborado por la Comisión Europea. En este documento se adopta el término *autopistas de la*

información acuñado por Gore inicialmente con su actuación en fondos y fomento por parte de la Comisión hacia el uso transnacional y difusión de la información a través de la red.

Posteriormente en 1994 aparece el Informe Bangemann titulado *Europa y la sociedad de la información: recomendaciones al Consejo Europeo* de 26 de mayo. Martin Bangemann fue Comisario de Telecomunicaciones y Vicepresidente la Comisión Europea y junto con otros expertos como Carlo de Benedetti, Pascual Maragall y Cándido Velásquez se dieron los primeros pasos y las bases para que la propia Comisión y el Consejo Europeo tomaran decisiones y destinaran fondos y actuaciones concretas para el fomento de la sociedad de la información, el uso de la red y la comunicación y transmisión libre de información como elemento generador de riqueza y conocimiento.

En el "Informe Bangemann", como se conoce comúnmente al informe elaborado por el grupo de expertos, se pone de manifiesto la urgencia de adoptar medidas inmediatas relativas a la creación de un entorno normativo favorable, así como la promoción de las nuevas potencialidades de estas nuevas tecnologías para la creación de mercados de productos y servicios tecnológicos. Las autoridades públicas tendrían, a partir de ese monumento, que desempeñar un papel fundamental en el desarrollo de la sociedad de la información en Europa, no solo invirtiendo en infraestructuras de telecomunicaciones, sino también acabando urgentemente con los monopolios nacionales y liberalizando los mercados de terminales y servicios para la entrada de nuevos competidores.

El Informe hacía hincapié en que la iniciativa privada sería importante para el desarrollo futuro de las nuevas tecnologías de la información, pero antes de esa labor de desarrollo, el entorno jurídico debía ser proclive a la penetración, en los diferentes mercados nacionales, de la iniciativa privada de la mano de operadores de telecomunicaciones y proveedores de servicios. Así pues, en el sector de las telecomunicaciones, la actuación de las autoridades públicas y de la iniciativa privada debían caminar a unísono y en paralelo, para conseguir un objetivo común: el desarrollo de una sociedad de la información en Europa.

Después del Informe Bangemann el Consejo Europeo adopta el 19 de julio de 1994 un Acuerdo, con fundamento en las conclusiones del informe Bangemann, que se muestra en un documento llamado *"Europa en marcha hacia la sociedad de la información".*

Luego la antigua Comunidad Europea hoy Unión Europea adopta la Decisión 98/253 de 30 de marzo de 1998 que crea el programa *Sociedad de la Información.*

Igualmente en el año 2000 el Consejo Europeo aprueba las Determinaciones de 23 y 24 de marzo de 2000 tituladas *Una Sociedad de Información para todos a través de la comunicación correspondiente de la Comisión Europea.*

El concepto sociedad de la Información comenzó a utilizarse en Japón durante los años sesenta del siglo veinte, considerándose al autor Yoneji Masuda como divulgador del término, a partir de una obra publicada en 1968. Así, será el autor Manuel Castells quien, de un modo más descriptivo que crítico, examine los caracteres del nuevo paradigma para acuñar, no ya la noción de Sociedad de la Información, sino la de era informacional, con Internet como fundamento principal a este nuevo modo de organización social en esferas tan dispares como las relaciones interpersonales, las formas laborales o los modos de construir la identidad propia.

La sociedad de la información puede definirse también como un estadio del desarrollo social caracterizado por la capacidad de sus miembros para obtener y compartir cualquier información,

instantáneamente, desde cualquier lugar y bajo diversas formas. (BERNAL-MEZA & MASERA, 2007, p. 93)

La sociedad de la información es aquella en la cual las tecnologías facilitan la creación, distribución y manipulación de la información y juegan un papel esencial en las actividades sociales, culturales y económicas. La noción de sociedad de la información ha sido inspirada por los programas de desarrollo de los países industrializados, y el término ha tenido una connotación más bien política que teórica, pues a menudo se presenta como una aspiración estratégica que permitiría superar el estancamiento social.

La sociedad de la información es vista como la sucesora de la sociedad industrial. Relativamente similares serían los conceptos de sociedad post-industrial (Daniel Bell), posfordismo, sociedad postmoderna, sociedad del conocimiento, entre otros. Este último concepto parecería estar emergiendo en detrimento de la sociedad de la información. (SOCIEDADDELAINFORMACIÓN, 2015)

1.3.4 Globalización y Política: el llamado "Nuevo Orden Mundial"

A partir de los hechos y fenómenos resumidos anteriormente, afirmamos que la tecnología permite la recogida, procesamiento, almacenamiento, recuperación y comunicación de grandes cantidades de información de cualquier tipo, tanto en texto, como en voz o imagen por que han cambiado los conceptos de tiempo y distancia apareciendo innovaciones tales como la televisión tridimensional, el reconocimiento de la voz, la inteligencia artificial, la conversión de voz a texto y viceversa, en una palabra ha nacido la realidad virtual.

Y así como lo expuso Herbert MARSHALL MCLUHAN, al transformarse la información y el conocimiento en energía eléctrica o impulsos *(bytes)*, ésta se ha tornado en una mercancía que se puede comprar y vender pasando a sustentar la nueva economía post-industrial y la creación de un *nuevo Mundo digitalizado,* al consistir la digitalización en la conversión de cualquier tipo de información a secuencias binarias de cero/uno y se da la sustitución del sistema analógico por el digital, que permite que soportes variados se transmitan por la red constituyendo un único documento multimedia. Los servicios (sector terciario de la economía) han adquirido nuevas y grandes dimensiones y se comienza a hablar de que el conocimiento configurará el sector cuaternario de la economía en el tercer milenio, donde para hacer compras comienza a hablarse de *bolsillos sin monedas* debido al proceso de sustitución, por ahora en el mundo digital, del dinero metálico o en papel por el electrónico (tarjetas de crédito, bitcoins o monedas electrónicas).

Este nuevo escenario internacional en el que gracias a las telecomunicaciones se hace posible una comunicación multidireccional y se multiplican las redes tecnológicas y sociales (las llamadas por Al Gore autopistas de la información) permiten al individuo estar conectado con todo el mundo pero con la paradoja de producir un individualismo excesivo ocasionado por la permanente y absorbente utilización del ordenador (computadora) y otras máquinas comienza a hablarse de una *Vida globalizada* **("aldea global", "economía global", "instituciones globales")** y el público es cada vez más concreto e individualizado con tendencia a la interactividad favoreciendo una tendencia a la eliminación de fronteras y límites difusos: lo que antes era territorial y sucedía en el marco de los países hoy no tiene límites definidos. Una noción que viene a clarificar o más bien definir este fenómeno es la del *ciberespacio o el ciberinfinito,* que es una realidad simulada que se encuentra implementada dentro de los ordenadores y de las redes digitales de todo el mundo. El término "ciberespacio" fue popularizado por la novela de William Gibson *Neuromante,* publicada en 1984, pero procede del relato del mismo autor Johnny *Mnemonic* (1981), incluido en el volumen Quemando Cromo (*Burning Chrome,* 1986). (CIBERESPACIO, 2013)

Todo lo anteriormente mencionado en este apartado propone el nacimiento de un *nuevo orden social global* que ofrece varios rasgos distintivos, que lo diferencian del anterior a la caída del comunismo y la desintegración de la antigua Unión Soviética. Se pueden mencionar, *grosso modo,* algunas características salientes del mismo y que evolucionan velozmente igual que los avances tecnológicos.

La primera de ellas es el papel que las grandes corporaciones y las instituciones financieras tienen en la economía globalizada dirigiendo y supervisando las decisiones de política económica de los países: las empresas transnacionales son el *spiritus rector* de la aldea global en que convierten al planeta (CHOMSKY, Noam & DIETERICH, 2004, pp. 13-46). En esta economía globalizada se atomiza el poder del Estado y los gobiernos van perdiendo funciones que antes se consideraban parte integrante de su soberanía. Como bien lo expresó MCLUHAN (1996, pp. 55-56)<<En condiciones de velocidad eléctrica, las soberanías departamentales se han disuelto tan rápidamente como las soberanías nacionales. La obsesión por los antiguos patrones de expansión mecánica y unidireccional desde un centro hacia los márgenes ha dejado de tener relevancia en nuestro mundo eléctrico. La electricidad no centraliza sino que descentraliza>>. Algunos han denominado a este fenómeno la *dictadura de los mercados* que se enmarca también, desde el punto de vista geopolítico, en el debate entre la unipolaridad de la superpotencia estadounidense y el surgimiento de nuevas potencias y bloques regionales dado que el capitalismo queda como el único régimen económico mayoritariamente aceptado a nivel global.

Por otra parte, en la política los gobiernos van perdiendo atribuciones en algunos ámbitos que son tomados por la sociedad civil en un fenómeno que se ha denominado *sociedad red*, el activismo cada vez más gira en torno a movimientos sociales y las redes sociales mientras los partidos políticos pierden su popularidad de antaño. La sociedad civil también toma protagonismo en el debate internacional a través de ONG internacionales de derechos humanos que monitorean la actividad interna o externa de los Estados, así como otras organizaciones privadas que se reúnen anualmente para respaldar el proceso globalizador como lo es el Foro Económico Mundial.

Otro fenómeno vinculado a la tecnología es lo que PÉREZ NUÑO (2004, p. 60) denomina *teledemocracia* que puede definirse en su acepción más genérica como la proyección de las Nuevas Tecnologías a los procesos de participación política de las sociedades democráticas.

Como lo sustenta una de las fuentes informativas consultadas (GLOBALIZACIÓN, 2017) esta potenciación del capitalismo como sistema económico y la democracia como mejor expresión de la participación ciudadana ha permeado el proceso de transición hacia la democracia de los antiguos regímenes despóticos que seguían el modelo soviético particularmente en la Europa del Este y en políticas públicas se destacan los esfuerzos para la transición al capitalismo en algunas de las antiguas economías dirigidas y la transición del feudalismo al capitalismo en economías subdesarrolladas de algunos países aunque con distintos grados de éxito.

En cuanto a las relaciones internacionales en este nuevo orden mundial, el mundo discute sobre cuáles pueden ser los mecanismos más aceptados por la comunidad internacional de intervención: entre el multilateralismo y el poder blando. En el ámbito militar surgen conflictos entre organizaciones armadas no-estatales (y transnacionales en muchos casos) y los ejércitos estatales (guerra contra el terrorismo, guerra contra el narcotráfico, etc.), mientras las potencias que realizan intervenciones militares a otros países (usualmente a los considerados como Estados fallidos: Irak, Libia, Siria en el escenario de la "primavera árabe") procuran ganarse a la opinión pública interna y mundial al formar coaliciones multinacionales y alegando el combate a alguna amenaza de seguridad, no sin amplios debates sobre la legitimidad de los conceptos de guerra preventiva e intervención humanitaria frente al principio de no intervención y de oposición a las guerras.

Finalmente, la globalización, siendo un proceso civil y de mercado, más bien tiende a ser vista como un orden espontáneo independiente de los organismos políticos y por eso difícil de controlar y generador de movimientos contrarios como el de la antiglobalización.

1.3.5 Globalización y Derecho. Breves apuntes

De acuerdo con CADENA AFANADOR (2001, pp. 102-104) la globalización del Derecho se plantea como un nuevo estilo de derecho y el surgimiento de un Nuevo Derecho, puesto que éste no es ajeno a la globalización pese a que es una de sus áreas menos vanguardistas y relaciona al fenómeno con la clásica *lex mercatoria* en el ámbito del comercio internacional y del Derecho Internacional Privado.

Otro especialista afirma (DRAETTA, 2001, pp. 1-21) que, después de la Segunda Guerra Mundial el crecimiento del comercio internacional, siempre en aumento rápidamente, desbordó la normativa ya en vigor tanto a nivel nacional como en los tratados internacionales existentes, lo que promovió en un inicio la aparición de usos o cláusulas estándar y este movimiento se tradujo en una progresiva erosión del monopolio estatal de regulación de las relaciones jurídico-privadas. Comenzó el fenómeno de la crisis del paradigma "Estadocéntrico" de la producción de normas jurídicas.

Esta erosión evolucionó hacia la aprobación de códigos de conducta y de autorregulación diseñadas para los operadores del comercio internacional que entran en la categoría del llamado *soft law* o derecho flexible que constituye el conjunto de normas no vinculantes pero que proponen soluciones basadas en la práctica, a problemas existentes en la comunidad internacional y, como exponen otros especialistas en la materia (FERNÁNDEZ ROZAS & SÁNCHEZ LORENZO, 2009, p. 24), las fórmulas de unificación o globalización *soft* como los Principios UNIDROIT sobre los contratos comerciales internacionales alcanzan al Derecho privado y al régimen de contratos e intercambios comerciales planteando soluciones de proyección universal.

Todas juntas han configurado la *lex mercatoria* que es el conjunto de principios generales y modelos contractuales aplicables a las relaciones comerciales internacionales y desarrollados en el marco de los operadores económicos internacionales sobre una base consuetudinaria luego de 1945; ejemplos de estas normas son, entre otros, las leyes modelo de la UNCITRAL, los Principios de UNIDROIT sobre Contratos Comerciales Internacionales y las Reglas Uniformes de la Cámara de Comercio Internacional de París o de la International Law Association.

Estas normas siguen la tendencia de los operadores del comercio internacional de desnacionalizar o deslocalizar sus relaciones contractuales buscando soluciones a-nacionales, sobre todo tomando en cuenta nuevos tipos contractuales no existentes en los ordenamientos nacionales como el de transferencia de tecnología.

A este conjunto de reglas de comercio internacional el autor citado anteriormente las denomina *derecho internacional de los particulares* para insistir en el origen no-estatal de ellas, para aclarar su contenido fundamentalmente mercantil y para definir su ámbito de aplicación a los operadores privados en el comercio internacional.

Otra característica de estas normas es su función transnacional para diferenciarlas tanto del derecho internacional como del derecho interno (*derecho internacional de los particulares, soft law, lex mercatoria*) y se considera como un derecho espontáneo producto del comercio internacional moderno. En síntesis, la *lex mercatoria* no ha sido creada por la globalización sino que más bien ha venido a relanzarse, evolucionar y actualizarse con los nuevos principios inspirados en la

particularidad específica del comercio electrónico y los avances tecnológicos.

1.4 Concepto de Globalización

Según una de las fuentes informativas consultadas (GLOBALIZACIÓN, 2017) la globalización se inicia en la Civilización occidental y que se ha expandido alrededor del mundo en las últimas décadas de la Edad Contemporánea (segunda mitad del siglo XX) recibe su mayor impulso y el fin de la Guerra Fría, y continúa en el siglo XXI. Se caracteriza en la economía por la integración de las economías locales a una economía de mercado mundial donde los modos de producción y los movimientos de capital se configuran a escala planetaria *(«nueva economía»)* cobrando mayor importancia el rol de las empresas multinacionales y la libre circulación de capitales junto con la implantación definitiva de la sociedad de consumo.

El ordenamiento jurídico también siente los efectos de la globalización y se ve en la necesidad de uniformizar y simplificar procedimientos y regulaciones nacionales e internacionales con el fin de mejorar las condiciones de competitividad y seguridad jurídica, además de universalizar el reconocimiento de los derechos fundamentales de ciudadanía.

En la cultura se caracteriza por un proceso que interrelaciona las sociedades y culturas locales en una cultura global *(aldea global)*, al respecto existe divergencia de criterios sobre si se trata de un fenómeno de asimilación occidental o de fusión multicultural.

En lo tecnológico la globalización depende de los avances en la conectividad humana (transporte y telecomunicaciones) facilitando la libre circulación de personas y la masificación de las TIC y el Internet. En el plano ideológico los credos y valores colectivistas y tradicionalistas causan desinterés generalizado y van perdiendo terreno ante el individualismo y el cosmopolitismo de la sociedad abierta. Los medios de comunicación clásicos, en especial la prensa escrita, van perdiendo su influencia social (cuarto poder) frente a la producción colaborativa de información de la Web 2.0 (quinto poder).

En síntesis la globalización puede definirse como un proceso económico, tecnológico, político, social y cultural a escala mundial que consiste en la creciente comunicación e interdependencia entre los distintos países del mundo uniendo sus mercados, sociedades y culturas, a través de una serie de transformaciones sociales, económicas y políticas que les dan un carácter global. Es a menudo identificada como un proceso dinámico producido principalmente por las sociedades, y que han abierto sus puertas a la revolución informática, llegando a un nivel considerable de liberalización y democratización en su cultura política, en su ordenamiento jurídico y económico nacional, y en sus relaciones nacionales e internacionales.

2. CIBERESPACIO Y CONTRATACIÓN

Manteniendo la vigencia del concepto de contrato en el Derecho Privado entendiendo por tal <<…todo negocio jurídico bilateral cuyo efecto consiste en constituir, modificar o extinguir una relación jurídica patrimonial>> (VALENCIA MORENO, 2012, p. 23), a continuación propondremos algunas consideraciones relativas a la relación existente entre los denominados contratos informáticos y el ciberespacio.

Se entiende por contrato informático <<…un acuerdo de voluntades que tiene por objeto bienes y/o servicios informáticos, preceptuado por la teoría general de las obligaciones y los contratos y guiado en lo especial por la informática>> (TORRES TORRES, 2002)

Precisando un poco más el concepto anteriormente expuesto, en sentido amplio el mismo abarca todos aquellos contratos por medios electrónicos y en sentido estricto se refiere particularmente a los contratos que se perfeccionan mediante el intercambio electrónico de datos (en inglés *Electronic Data Interchange*) de ordenador a ordenador (DE MIGUEL ASENSIO, 2000, p. 289). El intercambio electrónico de datos (en inglés Electronic Data Interchange o EDI) es la transmisión estructurada de datos entre organizaciones por medios electrónicos. Se usa para transferir documentos electrónicos o datos de negocios de un sistema computacional a otro. (INTERCAMBIOELECTRÓNICODEDATOS, 2018)

Existen distintas clasificaciones de los contratos informáticos, siendo una muy conocida y estándar encontrada en la red (CONTRATOINFORMÁTICO, 2018) la que indica que en cuanto al objeto los contratos informáticos pueden versar, bien sobre el *hardware* (elemento o soporte físico o material: las herramientas o máquinas), bien sobre el *software* (elemento o soporte lógico o inmaterial: los programas informáticos), bien sobre la prestación de servicios informáticos (por ejemplo, mantenimiento preventivo, correctivo o evolutivo de un programa informático; desarrollo y hospedaje de sitios web; prestación de servicios de certificación digital; creación o acceso a bases de datos; y otros análogos). Y nada impide como bien lo señala DE MIGUEL ASENSIO (2000, p. 289) que estos contratos puedan recaer sobre un bien material cuya entrega física es necesaria para su cumplimiento.

La doctrina identifica varios principios aplicables a los contratos informáticos (ILLESCAS ORTIZ, 2001, p. 216) (LANDÁEZ OTAZO & LANDÁEZ ARCAYA, 2007) (CULLELL MARCH, 2010) que son, en primer lugar el principio de la identidad negocial entre estos contratos y el resto de los contratos tradicionales; segundo la vigencia del principio de la autonomía de la voluntad de las partes en la materia de la contratación electrónica; en tercer lugar el principio de la inalterabilidad del derecho preexistente de las obligaciones y contratos privados aplicables al derecho del comercio electrónico; cuarto el de neutralidad tecnológica que supone que la legislación debe definir los objetivos a conseguir sin imponer ni discriminar el uso de cualquier otro tipo de tecnología para conseguir los objetivos fijados; y el de equivalencia funcional que consiste en atribuirle la eficacia probatoria o mismo valor probatorio a los mensajes y firmas electrónicas que los que la ley consagra para los instrumentos escritos.

Habiendo conceptualizado anteriormente la definición de ciberespacio (CIBERESPACIO, 2013), en este momento es importante agregar que este término se refiere a menudo a los objetos e identidades que existen dentro de la misma red informática mundial, así que se podría decir, metafóricamente, que una página web "se encuentra en el ciberespacio" y, en consecuencia, éste no debe confundirse con Internet ya que el primer concepto es más amplio que el segundo. Según esta interpretación, los acontecimientos que tienen lugar en Internet no están específicamente ocurriendo en los países donde los participantes o los servidores se encuentran físicamente, sino "en el ciberespacio", en ese intangible al que como por arte de magia podemos acceder todos quienes tenemos computadora en nuestros hogares o en nuestros lugares de trabajo. Éste parece ser un punto de vista razonable una vez que se extiende el uso de servicios distribuidos (como *Freenet*), y ya que por el momento la identidad y localización física de los participantes resulta imposible o muy difícil de determinar, debido a la comunicación generalmente anónima o o bajo pseudónimo. Por ello, en el caso de Internet, no se podrían o no se deberían aplicar las leyes de ningún país determinado.

Lo anterior supone una dificultad en los contratos informáticos, dado que no sería posible extender a éstos la protección legal que ofrecen los ordenamientos jurídicos a los contratos tradicionales en cuanto a sus etapas de formación, la expresión de la voluntad y su lugar de perfeccionamiento. Como bien sostiene el destacado autor español ILLESCAS ORTIZ (2001, p. 261), el lugar de perfeccionamiento del contrato informático es uno de los temas difíciles de la contratación electrónica

debido a la aterritorialidad del ciberespacio y de la posibilidad de que los sistemas de información de las partes se encuentren en lugares distintos a aquél que se considere como establecimiento principal de negocios de cada una.

Y es aquí donde entran las interrogante inicial de esta ponencia, a saber: ¿puede vincularse el ciberespacio a un territorio determinado para definir su condición jurídica? En la siguiente sección comentaremos la solución que el nuevo Código de Derecho Internacional Privado de Panamá ofrece a esta cuestión.

3. CONTRATOS ELECTRÓNICOS Y LA LEGISLACIÓN PANAMEÑA

Corresponde ahora referirnos a la solución que a la problemática planteada ofrece el Derecho Internacional Privado y comenzaremos recordando el concepto de la materia expuesto por el excelso maestro Gilberto BOUTIN (2002, p. 15) que expresa que se trata de <<…una disciplina que tiene por objeto la búsqueda de la ley aplicable a las relaciones de derecho privado internacional o con efectos extraterritoriales así como la coordinación de las legislaciones para la eficacia de las relaciones de carácter extraterritorial, extendiéndose a la coordinación de legislaciones en su dominio amplio, es decir, a sus fuentes de derecho consuetudinario que implican las leyes uniformes internacionales de carácter integral *(lex mercatoria)* y no tan sólo reduciéndolos a sus fuentes legislativas internas de cada Estado>>.

El objeto del Derecho Internacional Privado está compuesto, de acuerdo con la doctrina francesa como la expone el autor citado antes (BOUTIN, 2002, pp. 139-140), de los conflictos de leyes, los conflictos de jurisdicción, la condición jurídica de los extranjeros, la nacionalidad más el tema de los conflictos de autoridades adicionado en el siglo pasado por el insigne autor francés NIBOYET.

Gracias a la iniciativa, dedicación y perseverancia de la Asociación Panameña de Derecho Internacional Privado presidida por el profesor Doctor Gilberto BOUTIN, la Asamblea Nacional de Panamá aprobó la Ley 61 de 7 de octubre de 2015 que subroga la Ley 7 de 2014 que adopta el Código de Derecho Internacional Privado de la República de Panamá, la que apareció en la Gaceta Oficial N° 27885-A del jueves 8 de octubre de 2015 páginas 1 hasta la 34 inclusive y cuya entrada en vigor como legislación se inició a partir del 9 de octubre de 2015. Esta normativa se constituye como la Ley de Derecho Internacional Privado panameña y procederemos enseguida a considerar sus disposiciones refiriéndonos inicialmente a la determinación de la generalidad de los contratos internacionales y en segundo lugar a si la misma regula los contratos informáticos.

Como bien sustenta en su obra el profesor BOUTIN (2002, p. 594), la caracterización de un contrato como internacional va a depender de los elementos o factores de conexión que permitan justamente adjetivarlo o calificarlo así. Siendo así que la internacionalidad dependerá si el contrato está conectado con dos o más Estados distintos.

El Artículo 68 del Código de Derecho Internacional Privado de Panamá define la regla general para considerar un contrato como internacional de la siguiente forma:

> **Artículo 68.** Los contratos se reputan internacionales cuando las partes se encuentren domiciliadas en Estados diferentes y cuando:
> 1. El contrato contenga una prestación u obligación que recaiga sobre servicios, bienes o capital que produzcan sus efectos en el territorio de la República de Panamá, o
> 2. Los servicios, bienes o capital o su causa jurídica se hayan perfeccionado en el territorio de la República de Panamá, o
> 3. Las partes hayan incluido una cláusula atributiva de jurisdicción a favor de los tribunales panameños.

El criterio que utiliza el Código para internacionalizar un contrato es el domicilio *(lex domicilii)* combinado con los criterios, cuando se trate de la República de Panamá el lugar físico donde deban ocurrir, o bien la ley del lugar del cumplimiento, o la del lugar de perfeccionamiento del contrato y o el de la cláusula atributiva de jurisdicción al foro nacional.

En particular de los contratos informáticos el Código de Derecho Internacional Privado de la República de Panamá contiene una regla que es el Artículo 76 que dice lo siguiente:

> **Artículo 76.** Los contratos electrónicos, entendiendo por tales los realizados en línea o Internet, se perfeccionan en el momento de la recepción de la aceptación de la oferta. Igual criterio se aplicará en el caso de contratos internacionales entre ausentes.

La prueba de los contratos electrónicos se rige por el principio de la certeza y conservación de los documentos de acuerdo con las reglas, los principios y los usos de carácter internacional. La retractación en materia de contratos electrónicos internacionales deja sin efecto dicho contrato si ésta sobreviene en tiempo razonable. Se entiende por tiempo razonable el período de reflexión que le concede la ley al destinatario de la oferta.

Nos referiremos en esta ocasión al primer párrafo de la disposición legal y podemos decir que esta norma implica, dentro del contexto del Código de Derecho Internacional Privado panameño un reconocimiento importante y fundamental de la contratación electrónica. Igualmente cabe agregar que caracteriza a los contratos informáticos como internacionales y los denomina electrónicos y los define como aquellos que se celebran en línea o a través de la Internet.

Y la regla fundamental que instituye para los contratos electrónicos internacionales es que su perfeccionamiento ocurrirá en el momento de la recepción de la aceptación de la oferta. El lugar de perfeccionamiento del contrato informático o electrónico, al decir del autor español ILLESCAS ORTIZ, (2001, p. 267) es uno de los temas difíciles de la contratación electrónica, debido a la aterritorialidad del ciberespacio y de la posibilidad de que los sistemas de información de las partes se encuentren en lugares distintos al establecimiento considerado principal. La doctrina y el derecho positivo coinciden en establecer un orden jerárquico colocando en primer lugar la ley del lugar de expedición del mensaje de datos, subsidiariamente la ley del lugar de recepción del mensaje de datos, luego la ley del lugar del establecimiento de las partes o el lugar de emplazamiento de los sistemas de información de las partes y nos señala además que la Ley Modelo de Comercio Electrónico de la *Uncitral* en su artículo 15 recurre para evitar vacíos a los criterios provenientes del Derecho Internacional Privado del lugar que guarde una relación más estrecha con la operación de comercio a cuyo propósito se produce el mensaje de datos contenedor de la oferta emitida y subsidiariamente a la ley de la residencia habitual.

CONCLUSIONES FINALES

Es innegable la situación de los contratos informáticos en relación con el entorno digital en cuanto a que el ciberespacio es una realidad virtual intangible, pero ¿hasta dónde puede hablarse en este contexto de una dimensión a-territorial si los mensajes tienen que tener un punto de partida y de llegada? Lo que queremos decir es que las computadoras, las redes o los instrumentos de telecomunicaciones pueden ubicarse físicamente en un lugar donde puedan iniciarse las transmisiones, y es posible localizar los flujos como envíos de información. Por ello consideramos que los criterios actualmente admitidos para la determinación del lugar de perfeccionamiento de un contrato informático o electrónico son claros ya que se deducen claramente de la esencia del medio en que se desenvuelve el comercio electrónico, esto es, el ciberespacio.

Para responder a nuestra pregunta de reflexión, la misma es negativa puesto que el ciberespacio no es un territorio y la señal transmitida por un medio electrónico puede ser identificada territorialmente a través de, por ejemplo, la identificación e ubicación del proveedor de servicios de Internet (ISP en sus siglas en inglés), del procedimiento de verificación de procedencia que es una técnica para autenticar el origen del mensaje del propio iniciador, entre otros.

La distinción entre los contratos informáticos o electrónicos nacionales versus los internacionales ha sido establecida por los Artículos 68 y 76 del Código de Derecho Internacional Privado de Panamá a través del punto de conexión domicilio combinado con la celebración del contrato o ejecución de alguna prestación dentro del territorio de la República de Panamá junto a la cláusula de atribución de foro a un tribunal panameño. Lo anterior se ve reforzado precisamente por los Artículos 77 y 78 de la Ley N° 51 de 22 de julio de 2008 publicada en la Gaceta Oficial N°26,090 del jueves 24 de julio de 2008 (Ley de Comercio Electrónico, Documentos y Firmas Electrónicas y Prestación de Servicios de Almacenamiento de la República de Panamá) que utilizan el criterio de la residencia o domicilio social para calificar si una empresa que presta servicios tecnológicos en este campo se encuentra bajo la jurisdicción panameña o dentro de un Estado extranjero de la siguiente forma:

> **Artículo 77.** Criterio de territorialidad. Para los efectos de esta Ley, se entenderá que una empresa que realiza ventas de bienes o servicios a través de Internet está establecida en el territorio de la República de Panamá, cuando su residencia o domicilio social se encuentren en territorio nacional y mantenga efectivamente centralizada la gestión administrativa y la dirección de sus negocios y/o cuando la empresa, o alguna de sus sucursales que realice ventas de bienes o servicios en el territorio nacional, haya obtenido, una licencia comercial o industrial o haya realizado el Aviso de Operación ante el Ministerio de Comercio e Industrias.

Se considerará que una empresa opera mediante un establecimiento permanente situado en territorio nacional, cuando disponga en este, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que se realice, o se dé apoyo logístico a todas o parte de las ventas de bienes y servicios realizados en Panamá.

Las empresas que vendan bienes o servicios en Panamá, a través de Internet, estarán sujetos a las demás disposiciones de la legislación nacional que les sean aplicables en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización.

> **Artículo 78.** Venta de bienes y servicios a través de Internet desde el extranjero. La prestación de servicios comerciales a través de Internet que proceda de una empresa establecida en cualquier otro Estado, se realizará en régimen de libre prestación de servicios y con base en criterios establecidos en acuerdos internacionales reconocidos en la legislación vigente. Sin embargo, las empresas que promuevan sus servicios y realicen transacciones comerciales en Panamá, a través de Internet, deberán cumplir con los requerimientos técnicos y demás obligaciones previstas en la legislación y la reglamentación vigente en la República de Panamá.

No se aprecia entonces oposición o contradicción entre el Código de Derecho Internacional Privado y la Ley de Comercio Electrónico de la República de Panamá en referencia al criterio domiciliar, lo que permite una interesante zona de tangencia entre el Derecho Informático o de la Informática y el Derecho Internacional Privado, regulándose los contratos informáticos o electrónicos celebrados dentro de Panamá como informáticos o electrónicos nacionales mientras que aquellos internacionales se regirán por la Ley 61 de 2015 en cuanto a su proyección internacional para la determinación del derecho aplicable al contrato y demás aspectos de la disciplina internacional privatística.

Dentro de los diferentes sistemas para determinar el lugar de perfeccionamiento del contrato el Artículo 76 de la Ley 61 de 2015 acoge el segundo que la doctrina recomienda en la materia, cual es de la recepción (de la aceptación de la oferta), opción que a nuestro criterio es perfectamente concordante en lo sustancial tanto con el Artículo 15 de la Ley Modelo de Comercio Electrónico de *UNCITRAL* de 1996 revisada en 1998 como con el Artículo 24 de la Convención de Viena de 1980 sobre Compraventa Internacional de Mercaderías así como otras legislaciones en clave de Derecho Comparado (por ejemplo, el Artículo 1.262 numeral 2° del Código Civil de España).

REFERENCIAS BIBLIOGRÁFICAS

BANGEMANN. (1994). *Europa y la sociedad global de la información Recomendaciones al Consejo Europeo.* Bruselas : Unión Europea .

BECERRA, M. (Janeiro-Junho de 1999). La vía europea hacia la Sociedad de la Información. *Revista Brasileira de Ciencias da Comunicaçao*, 35-56.

BERNAL-MEZA, R., & MASERA, G. A. (1/15 de Abril/Mayo de 2007). Sociedad de la información: etapa posterior de la globalización/mundialización Desafíos y riesgos para América latina. *Realidad económica*, 90-116.

BOUTIN, G. (2002). *Derecho Internacional Privado* (Primera ed.). Panamá : Mizrachi & Pujol .

CADENAAFANADOR, W. (Octubre de 2001). La Nueva Lex Mercatoria: un caso pionero en la globalización del Derecho. *Papel Político*(13), 101-114.

CHOMSKY, Noam , & DIETERICH, H. (2004). *La Aldea Global* (Octava ed.). Tafalla (Navarra): Txalaparta.

CIBERESPACIO. (30 de Mayo de 2013). *Wikipedia la enciclopedia libre.* Obtenido de http://es.wikipedia.org/wiki/Ciberespacio

COMERCIOELECTRÓNICO. (14 de Julio de 2018). *Wikipedia la enciclopedia libre.* Obtenido de https://es.wikipedia.org/wiki/Comercio_electrónico

COMPUTADORA. (13 de Septiembre de 2013). *Wikipedia la enciclopedia libre* . Obtenido de http://es.wikipedia.org/wiki/Computadora

CONTRATOINFORMÁTICO. (17 de Julio de 2018). *Wikipedia la enciclopedia libre* . Obtenido de https://es.wikipedia.org/wiki/Contrato_informático

CULLELL MARCH, C. (2010). El principio de neutralidad tecnológica y de servicios en la UE: la liberalización del espectro radioeléctrico. (U. A. Cataluña, Ed.) *Revista de Internet, Derecho y Política*.

DE MIGUEL ASENSIO, P. A. (2000). *Derecho Privado de Internet.* Madrid: Civitas Ediciones.

DRAETTA, U. (2001). *Internet e Commercio Elettronico del Diritto Internazionale dei Privati* . Milano : Giuffré Editore S.p.A.

FERNÁNDEZ ROZAS, J., & SÁNCHEZ LORENZO, S. (2009). *Derecho internacional privado* (Quinta ed.). (T. R. Limited, Ed.) Pamplona : Aranzadi.

FERRER, A. (1997). *Hechos y ficciones de la globalización.* Buenos Aires : Fondo de Cultura Económica.

GLOBALIZACIÓN. (9 de Agosto de 2017). *Wikipedia la enciclopedia libre* . Obtenido de https://es.wikipedia.org/wiki/Globalizaci%C3%B3n

HISTORIADEINTERNET. (13 de Septiembre de 2013). *Wikipedia la enciclopedia libre.* Obtenido de http://es.wikipedia.org/wiki/Historia_de_Internet

ILLESCAS ORTIZ, R. (2001). *Derecho de la Contratación Electrónica.* Madrid: Civitas.

INTERCAMBIOELECTRÓNICODEDATOS. (17 de Julio de 2018). *Wikipedia la enciclopedia libre.* Obtenido de https://es.wikipedia.org/wiki/Intercambio_electrónico_de_datos

INTERNET. (30 de Mayo de 2013). *Wikipedia la enciclopedia libre.* Obtenido de http://es.wikipedia.org/wiki/Internet

LANDÁEZ OTAZO, L., & LANDÁEZ ARCAYA, N. (2007). La Equivalencia Funcional, la Neutralidad Tecnológica y la Libertad Informática. (U. d. Carabobo, Ed.) *Revista de la Facultad de Ciencias Jurídicas y Políticas*, 11-49.

MCLUHAN, M. (1972). *A galáxia de Gutenberg a formaçao do homem tipográfico.* (L. GONTIJO DE CARVALHO, & A. TEIXEIRA, Trads.) Sao Paulo: Editora Nacional Editora da USP.

MCLUHAN, M. (1985). *La galaxia de Gutenberg.* México : Origen Planeta .

MCLUHAN, M. (1996). *Comprender los medios de comunicación: Las extensiones del ser humano.* (P. Ducher, Trad.) Barcelona : Paidós Ibérica .

PÉREZ LUÑO, A.-E. (2004). *¿Ciberciudadanía o ciudadanía.com?* Barcelona: Gedisa.

ROBERTKAHN. (13 de Septiembre de 2013). *Wikipedia la enciclopedia libre.* Obtenido de http://pt.wikipedia.org/wiki/Robert_Kahn

ROJO VILLADA, P. A. (Enero-Febrero de 2003). Europa y la sociedad de la información: análisis del impacto del "Informe Bangemann" sobre la política, la economía y la sociedad europea de la década de los noventa. (U. d. (Tenerife), Ed.) *Revista Latina de Comunicación Social , VI*(53).

SOCIEDADDELAINFORMACIÓN. (20 de Noviembre de 2015). *Wikipedia la enciclopedia libre.* Obtenido de https://es.wikipedia.org/wiki/Sociedad_de_la_información

TELECOMUNICACIÓN. (20 de Septiembre de 2013). *Wikipedia la enciclopedia libre.* Obtenido de http://es.wikipedia.org/wiki/Telecomunicaci%C3%B3n

TORRES TORRES, H. W. (2002). *Derecho Informático.* Medellín : Ediciones Jurídicas Gustavo Ibáñez.

VALENCIA MORENO, A. (2012). *Los principales contratos civiles.* Panamá: Novo Art S.A.

VINTCERF. (13 de Septiembre de 2013). *Wikipedia la enciclopedia libre.* Obtenido de http://pt.wikipedia.org/wiki/Vint_Cerf

FAKE NEWS Y NEUROMARKETING EN LAS TIC'S… SU INCIDENCIA EN LOS DERECHOS HUMANOS, CONCRETAMENTE, EN LA DEMOCRACIA

Por: ***Luis Fernando Contreras Cortés***
Panamá

1. INTRODUCCIÓN

La finalidad del presente trabajo consiste en acercar al lector al conocimiento e importancia de las denominadas fake news (noticias falsas), del neuromarketing y de las Tecnologías de la Información y de la Comunicación, así como su incidencia en un derecho humano tan importante como lo es la democracia, vista desde el punto de vista formal o procedimental. Lo anterior, en virtud de que una gran cantidad de políticos, han utilizado y siguen utilizando técnicas neurológicas para persuadir a las personas de forma emocional a través de noticias falsas y de esta manera inclinar la balanza electoral a su favor; aunado a ello, dichos personajes se valen de las TIC´s, puesto que hoy en día, resultan ser algo asequible casi para cualquier persona, ya que la mayoría de la población puede acceder a ellas, de modo tal que se amplifica la desinformación y, consecuentemente, la ignorancia y el descontento social, y más en esta época en la que las personas privilegian la información de primera mano antes que los medios informativos confiables.

Para el logro de nuestro objetivo, comenzaremos por señalar qué son las TIC´s y de qué forma impactan en la sociedad y consecuentemente en la democracia; posteriormente, haremos alusión a la incidencia de las fake news en la democracia, como ya se ha hecho referencia, formal o procedimental, para lo cual señalaremos, en primer lugar, qué son las noticias falsas, en segundo lugar, tanto el concepto como los elementos de la democracia, para posteriormente relacionar ambas figuras y así dilucidar la afectación que producen las fake news en la democracia a través de las TIC's; después, ahondaremos en el neuromarketing político, una figura que creemos no ha sido tratada desde la perspectiva que presentamos y la cual consideramos también perturba a la democracia, en conjunto con las figuras antes mencionadas, esto es, a las TIC´s y a las noticias falsas, y por último, emitiremos nuestras reflexiones finales, no sin antes señalar dentro de cada apartado algunas propuestas que ayudarán a evitar la transgresión de tan prestigiado derecho humano.

Para concluir este apartado, debemos señalar que la razón que nos ha llevado a estudiar este tema es el interés personal de construir de manera positiva el nuevo paradigma del derecho y las TIC´s, desde un nuevo enfoque y de esta forma, aportar a los sectores académico y jurisdiccional, los elementos necesarios para la comprensión y aplicación de los mismos.

2. LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LA COMUNICACIÓN

Ustedes se preguntarán: ¿Qué relación tienen la democracia con las fake news, con el neuromarketing y con las TIC's? o ¿De qué forma las fake news, el neuromarketing y las TIC's afectan al derecho humano antes citado? Dichos cuestionamientos los responderemos dentro del cuerpo del presente manuscrito, para lo cual seguiremos una metodología que nos permitirá analizar y posteriormente concatenar las figuras antes referidas.

Para efectos metodológicos, consideramos pertinente señalar, en primer término, qué son las Tecnologías de la Información y de la Comunicación (TIC´s), por lo cual haremos alusión a lo

externado por DÍAZ REVORIO, en el sentido de que las TIC´s son el conjunto de instrumentos desarrollados en las últimas décadas para la comunicación y la transmisión de la información.[1]
En ese tenor, encontramos que las TIC´s son el conjunto de herramientas informáticas y computacionales que procesan, almacenan, resumen, recuperan, difunden y muestran información representada en diversas formas. Algunos ejemplos de estas tecnologías son la pizarra digital, los blogs, el podcast y por supuesto la web.[2]

Otra acepción que podemos añadir, es la relativa a que las Tecnologías de la Información y de la Comunicación se identifican con el desarrollo de máquinas y dispositivos diseñados para tratar, transmitir y manejar de manera flexible grandes cantidades de información y conocimiento.[3]

Derivado de los conceptos referidos, podemos advertir que la tendencia de las TIC´s es y será la de establecer las bases para lograr el normal funcionamiento de la red digital de servicios integrados en el que confluirán todas las Tecnologías de la Información y de la Comunicación, como lo son: los ordenadores, teléfonos celulares, cámaras digitales, bancos de datos, consolas de videojuegos, canales de televisión, correo electrónico, video teléfonos, teletextos y videotextos, los cuales están y estarán interconectados, haciendo posible una comunicación instantánea y sin fronteras.

Por otra parte, consideramos oportuno hacer alusión a un concepto normativo que nos ofrece el Estado mexicano dentro del párrafo tercero del artículo sexto de la Constitución Política de los Estados Unidos Mexicano, el cual nos ayuda a la comprensión del concepto que tratamos en este apartado, mismo que establece que "El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet…"; asimismo, dentro del apartado B, fracción I del numeral en cita, se hace referencia al derecho de acceso a las TIC´s con la obligación que tiene el Estado de garantizar "a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales." Dicho reconocimiento constitucional, se realizó mediante la reforma publicada el once de junio de dos mil trece en el Diario Oficial de la Federación.

El referido marco legal, no señala otra cosa que el derecho al acceso y uso de las TIC´s, lo cual comprende la libertad de las personas de acceder y usar eficazmente las tecnologías, navegar por la banda ancha y adquirir información de calidades por los diversos medios digitales, radiofónicos y televisivos. De igual manera, difundir cualquier contenido por los medios mencionados, interactuar y formar parte integral de la Sociedad de la Información, sin importar condiciones sociales o económicas.[4]

Entonces, las TIC´s son un conjunto de innovaciones tecnológicas, pero también son las herramientas que permiten una redefinición radical del funcionamiento de la sociedad, toda vez que, se ha convertido en un acelerador social, puesto que hace que las personas accedan fácilmente a diferentes

[1] DÍAZ REVORIO, Francisco Javier. Los derechos humanos ante los nuevos avances científicos y tecnológicos, editorial Tirant lo Blanch, España, 2009, pág. 166.
[2] Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATIC´s). "Las TIC´s en el Gobierno", consultado en línea en: https://prezi.com/5oscnazc_s0e/las-tics-en-el-gobierno/, el 4 de agosto de 2017.
[3] BUSTILLO PORRO, Vicenta. "Nuevas tecnologías de la información: Herramientas para la educación", consultado en línea en: http://campus.usal.es/~teoriaeducacion/rev_numero_06/n6_art_bustillo.htm, el 22 de agosto de 2017.
[4] Derecho al acceso y uso de las tecnologías de la información y de la comunicación, en el Centenario de la Constitución Política de los Estados Unidos Mexicanos, editorial CNDH-SEP-INEHRM, México, 2015, pág. 11.

tipos de información, por lo que se genera, consecuentemente, nuevas formas de percibir el mundo, así como nuevas variables para realizar diferentes actividades, ya que se modifican constantemente los métodos y técnicas al momento de realizar casi cualquier cosa.

Lo antes señalado, como podemos observar, redunda en algo benéfico para la sociedad más ahora que los gobiernos tratan de incursionar en una democracia basada en la transparencia, rendición de cuentas y participación, lo cual realizan a través de las TIC´s, toda vez que estas permiten el acceso a la esfera pública con facilidad, la publicación de textos e imágenes sin mayores medios de producción, así como la circulación y la manipulación de contenidos. Sin embargo, es aquí en donde se debe tener mucho cuidado, toda vez que, existen personas u organizaciones que buscan, a través de noticias falsas, interferir con dichas facultades otorgadas por el Estado, haciendo un uso inadecuado de las tecnologías, con el objeto de intervenir en el ejercicio del derecho humano denominado democracia, visto desde el punto de vista formal o procedimental, hasta llegar al grado de confundir a la ciudadanía, demeritar a alguna persona o institución o generar un descontento social, entre otras cosas, para de esa forma, alcanzar, de manera general, el poder, tal como lo haremos notar en los subsecuentes parágrafos.

3. LA INCIDENCIA DE LAS FAKE NEWS EN LA DEMOCRACIA

En este apartado, aremos alusión, en primer lugar, a las fake news o noticias falsas, las cuales no son algo realmente nuevo, ya que con el tiempo se ha convertido en una práctica común, el que las personas abusen de las audiencias engañándolas con noticias falsas, sin embargo, se hace más latente, en virtud de los medios a través de los cuales se dan a conocer, en el presente, podemos hablar, a manera de ejemplo, de las redes sociales.

Concretamente, las fake news o noticias falsas son datos que puede utilizar, casi cualquier persona, para demeritar o fortalecer a cierta persona, grupo u organización con el objeto de golpearla mediáticamente.[5]

Por otra parte, podemos señalar que fake news es propaganda, amarillismo o aquella información falsa diseminada bajo la apariencia de un reportaje cuyo contenido es frecuentemente sensacionalista. [6]

Ahora bien, una vez que mencionamos lo que son las noticias falsas, consideramos oportuno, para los efectos de lo que se pretende hacer notar en este ensayo, hacer alusión a la figura jurídica de la democracia, pues es una expresión que representa un grado de complejidad considerable, ya que, como otros vocablos de la ciencia del derecho, tiene múltiples significados, tan es así que podemos advertir que los doctrinistas no llegan a un acuerdo sobre una definición de democracia, y aún más, algunos la consideran como una forma de gobierno, otros, como un régimen político o bien como un procedimiento para elegir a los gobernantes.

Dicho lo anterior y por cuestiones metodológicas, consideramos adecuado señalar que nos constreñiremos a los significados formales o procedimentales, así como uno de los elementos fundamentales que se desprende de la misma.

---

[5] FONTEVECCHIA, Agustino. “Fake News: El cáncer de la web gestado por Google y Facebook”, consultado en línea en: http://www.perfil.com/tecnologia/fake-news-el-cancer-de-la-web-gestado-por-google-y-facebook.phtml, el 7 de mayo de 2018.

[6] HERRERO, Inma. “Fake news, posverdad y redes sociales”, consultado en línea en: https://www.biblogtecarios.es/inmaherrero/fake-news-posverdad-y-redes-sociales/, el 12 de mayo de 2018.

Así pues, etimológicamente, democracia se compone de dos palabras que provienen del griego, *demos* cuyo significado es pueblo y *kratos* que significa autoridad, o también *kratein* que significa gobernar[7].

En ese sentido, Luigi FERRAJOLI[8] señala que la democracia, se concibe como el poder del pueblo de asumir las decisiones públicas, directamente o a través de representantes. Esta noción identifica a la democracia atendiendo exclusivamente a las formas y procedimientos idóneos para legitimar las decisiones como expresión, directa o indirecta, de la voluntad popular, esto es, porque la identifica al tenor del quién (el pueblo o sus representantes) y el cómo de las decisiones (el sufragio universal y la regla de la mayoría), con independencia de sus contenidos, es decir, del qué se decide.

Por su parte, Giovanni SARTORI[9] aduce que la democracia es un procedimiento y mecanismo que genera una oligarquía abierta cuya concurrencia en el mercado laboral atribuye el poder al pueblo y hace valer la responsabilidad de los líderes para con los liderados.
Ahora bien, en cuanto a los elementos de la democracia Norberto BOBBIO[10] hace referencia a seis y manifiesta que éstos podrían ser las raíces sólidas para el desarrollo de la misma, aun en las democracias consideradas como "avanzadas" o "consolidadas":

1. Todos los ciudadanos que hayan alcanzado la mayoría de edad, sin distinción de raza, religión, condición económica y sexo, deben disfrutar de los derechos políticos, es decir, cada uno debe disfrutar del derecho de expresar la propia opinión y de elegir a quién la exprese por él;

2. El voto de todos los ciudadanos debe tener el mismo peso;

3. **Todos los que disfrutan de los derechos políticos deben ser libres para poder votar según la propia opinión, formada lo más libremente posible[11]**, en una competición libre entre grupos políticos organizados, en concurrencia entre ellos;

4. Deben ser libres también en el sentido de que deben ser puestos en la condición de elegir entre soluciones diversas, es decir, entre partidos que tengan programas diversos y alternativos;

5. Tanto para las elecciones como para las decisiones colectivas, debe valer la regla de la mayoría numérica, en el sentido de que se considere electo o válida la decisión que obtenga el mayor número de votos;

6. Ninguna decisión tomada por mayoría debe limitar los derechos de la minoría, particularmente el derecho de convertirse a su vez en mayoría en igualdad de condiciones.

En ese mismo orden de ideas, Kart SHELL[12] determina que los elementos comunes del concepto de democracia son los siguientes:

a. El principio de la soberanía popular. No debe existir ninguna instancia política (aparte de la legitimada por el pueblo) que detente la decisión última sobre las leyes bajo las que el pueblo ha de vivir.

---

[7] Enciclopedia Jurídica Mexicana, editorial Instituto de Investigaciones Jurídicas de la UNAM/Porrúa, T. III, México, 2002, pág. 132.
[8] FERRAJOLI, Luigi. Poderes salvajes. La crisis de la democracia constitucional, editorial Trotta, Madrid, 2011, pág. 27.
[9] SARTORI, Giovanni. Teoría de la democracia, editorial Alianza Universidad, Madrid, 1988, págs. 259 y 260.
[10] BOBBIO, Norberto. Teoría general del derecho y del Estado, editorial UNAM, México, 1958, págs. 333 y 334.
[11] Las negritas fueron puestas por quien realiza el presente ensayo.
[12] Ver ARTEAGA NAVA, Elisur. Tratado de derecho constitucional (segunda edición), Vol. 1, editorial Oxford, México, 2002, págs. 104 y 105.

b. El concepto pueblo comprende a todos los ciudadanos que residen permanentemente en un territorio y que disfrutan de la mayoría de edad legal.

c. En el seno del pueblo reina el principio de igualdad en lo que atañe a la participación en el proceso de formación de la voluntad política.

d. La democracia exige que existan instituciones que permitan al pueblo soberano expresar su voluntad y participar de esta manera en el proceso de formación de la voluntad política. Estas instituciones pueden tener un carácter directo, plebiscitario o representativo.

e. La democracia reclama, la protección de al menos aquellas libertades que el pueblo necesita para la libre formación de su voluntad, esto es de aquellos derechos fundamentales que articulan el proceso de la libre formación de la opinión en lo que concierne a las decisiones políticas.

f. Ha de existir igualdad social por lo menos hasta el extremo de que ninguna parte de la población, a causa de deficiente preparación se vea excluida de la posibilidad de percatarse de sus propios intereses.

Como podemos advertir, tanto Norberto BOBBIO como Karl SHELL coinciden en que uno de los elementos fundamentales de la democracia es la libre formación de la opinión en lo que concierne a las decisiones políticas, opinión la cual debe ser formada lo más libremente posible, pues la democracia no sólo constituye valores, actitudes y conductas, además de un verdadero estado de derecho, sino que también es el reconocimiento implícito de los derechos de las personas, en virtud de que éstas son libres y conscientes de su libertad y, por lo tanto, tienen la facultad de decidir y elegir,[13] todo lo cual se encuentra a su vez regulado en las propias Constituciones, que es en donde deben estar sentadas sus bases, se reconoce y garantiza la protección de los derechos fundamentales, y en donde se establece la organización y atribuciones del poder público.

Sin embargo, creemos que la democracia, al menos en ese aspecto, se encuentra constantemente afectada por las noticias falas a través del uso de las TIC´s, basta con observar lo que sucedió en las elecciones pasadas en los Estados Unidos, ya que según PolitiFact, una agencia independiente que comprueba las declaraciones de políticos estadounidenses, el setenta por ciento de las declaraciones del actual presidente pueden ser clasificadas como "medianamente falsas", "falsas" o "mentiras descaradas".[14]

Para ser más precisos, recordemos que, durante su campaña, Trump dijo explícitamente que Barack Obama era el fundador del Estado Islámico y Hillary Clinton la cofundadora de dicho grupo terrorista; de igual forma, aseveró que el número de inmigrantes ilegales en Estados Unidos era de 34 millones, cuando los estudios académicos y oficiales indican que la cifra apenas ronda los 10 millones; sin embargo, la noticia falsa más difundida ha sido la negación del cambio climático. Los informes científicos prueban que la contaminación es la responsable de un aumento excesivo en la temperatura del planeta, pero algunas voces insisten en que es un mito.[15]

---

[13] PÉREZ CUEVAS, Carlos Alberto. "Los retos de la democracia" en Las aportaciones de las entidades federativas a la reforma del Estado, edición al cuidado de Máximo N. GÁMIZ PARRAL y José Enrique RIVERA RODRÍGUEZ. Editorial UNAM, México, 2005, pág. 395.

[14] El Tiempo. "Carta abierta a los posverdaderos", consultado en línea en: http://www.eltiempo.com/bocas/carta-abierta-de-la-revista-bocas-a-los-posverdaderos-agosto-2017-121170, el 12 de mayo de 2018.

[15] *Ídem*.

Así, varios analistas coinciden en que ese tipo de declaraciones, que, aunque destilaban falsedad despertaban el fanatismo, lo que logró posicionarlo en la Casa Blanca.

En el sentido de lo antes señalado, encontramos a Ovidiu Drobota un joven rumano de veinticuatro años, quien es el fundador de Ending the Fed, una comunidad de Facebook que cuenta con más de trescientos cincuenta mil seguidores, y el cual generó cuatro de las diez noticias falsas de mayor audiencia durante las elecciones presidenciales que consagraron a Donald Trump. Drobota factura aproximadamente diez mil dólares por mes usando Google AdSense, la plataforma de venta de publicidad del gigante de Silicon Valley.[16]

Lo complicado es que pareciera que, como señaló Craig Silverman, editor de BuzzFeed News, [17] "Mientras más falsa es una noticia, más interacciones crea en la audiencia que sigue el medio".

Y es hasta gracioso, ya que en muchos casos ni siquiera se lee el contenido total de las notas, y así lo demuestra el experimento relativo a una nota falsa titulada: "La NASA confirma que la mariguana contiene ADN alienígena de otro sistema solar", pues generó más de ciento cuarenta mil compartidos, mientras que el portal NPR publicó "¿Por qué no leen los norteamericanos?" como chiste, ya que el contenido de la nota explicaba que era una nota falsa, generando cientos de comentarios de lectores enojados con sus conciudadanos por no leer más[18].

Es por ello que, consideramos que las noticias falsas son una amenaza para las instituciones democráticas, tal como lo sostuvo el expresidente Barack Obama quien reconoció el peligro para las libertades democráticas al hablar con la prensa en Alemania poco antes de las elecciones estadounidenses.
Está claro que este tipo de noticias podría hacer que un candidato pierda las elecciones y afectar las relaciones internacionales, toda vez que, al parecer atizar el nacionalismo y la guerra de clases o de ideologías, es un golpe seguro. Más cuando se hace desde el insulto y la calumnia. Tachar al contrincante de ladrón, corrupto, violador o asesino, sin tener las pruebas verificables en la mano, es muy valioso cuando hay un ejército de seguidores que no cuestionan la declaración, sino que la reproducen y la defienden con entusiasmo.[19]

Hoy cuesta tener confianza en el poder de un razonamiento libre y sin temor, especialmente si se ha de aplicar mediante los procesos de gobierno popular, pues parece ser que la creencia de que más expresión y no un silencio obligado como remedio para la falsedad y las falacias, resulta ingenuo, especialmente si se aplica en una campaña electoral.

Debe haber un freno a las noticias falsas, ya que son contrarias a uno de los pilares fundamentales de la democracia: que los votantes puedan decidir de manera libre e informada entre los candidatos en competencia, lo cual no sucede.

Aunado a que, consideramos que acusar durante una campaña electoral a cierto candidato de haber cometido algún ilícito, no es algo menor, y pareciera que la normatividad no brinda un remedio adecuado.

---

[16] *Op. Cit*., FONTEVECCHIA, Agustino.
[17] CORTÉS FIERRO, Ernesto. "Del populismo a la posverdad / Voy y vuelvo", consultado en línea en: http://www.eltiempo.com/bogota/voy-y-vuelvo-sobre-populismo-y-posverdad-97644, el 2 de junio de 2018.
[18] *Op. Cit*., FONTEVECCHIA, Agustino.
[19] *Op. Cit*., El Tiempo, Carta abierta a los posverdaderos.

Entonces, en la era de internet, ¿es tiempo de que el péndulo legal vuelva a inclinarse hacia los delitos de calumnia o difamación? [20], ¿Podría ser el remedio? Y más tomando en consideración que los procesos son largos y costosos y probablemente no resolverían en el momento oportuno los conflictos que se presenten, es decir, no para los efectos pertinentes en los procesos electorales de los que se trate.

Creemos que el verdadero problema es que ni Google ni Facebook, y mucho menos los autores de estos blogs y sitios espurios, se hacen cargo de lo que consume la audiencia y menos cuando sabemos que en el web vale todo porque el anonimato es el rey.

Lo que podríamos hacer antes de difundir algo es convalidar la información o bien verificar la legitimidad de la información que consumimos y compartimos, lo cual se puede realizar consultando, a manera de ejemplo, Snopes (también conocida como Urban Legends Reference Pages), que es una página web conocida como fuente para la validación de leyendas urbanas, rumores, hoax o bulos, cadenas de mensajes y demás historias de procedencia incierta (principalmente estadounidense) o FactCheck.org. En Argentina existe Chequeado y para la comunidad hispanohablante Cazahoax; en Twitter tenemos Maldito bulo o La Buloteca y en Facebook, Caza bulos[21], sitios que, debemos ser honestos, tampoco nos brindan la certeza de lo que sometemos a consulta, pero por algo se debe iniciar.

En México, para tratar de frenar las fake news, en el proceso electoral 2018, nace Verificado 2018, un proyecto realizado por diversos medios, organizaciones de la sociedad civil y universidades, mismo que retoma el nombre que la sociedad utilizó para informar y ayudar a las personas que sufrieron la catástrofe del diecinueve de septiembre (verificado 19S), sin embargo, tampoco sería suficiente, toda vez que, sólo cuenta con la característica de ser netamente informativo, más no vinculante, pero, ha sido una herramienta sumamente útil.

De la misma forma, la sociedad tiene que aprender a diferenciar el contenido profesional del trabajo de un bloguero o un influencer; se requiere regular los derechos digitales y exigirles reparaciones por los daños que pudieran generar, mientras se mejora el ecosistema digital para erradicar estos conflictos.

Finalmente, debemos tomar en cuenta, para estar preparados, que no sólo existen las denominadas fake news, pues ahora podemos observar diferentes formas de engañar a las personas, tal es el caso de las deep fakes las cuales consisten en video montajes ultra realistas hechos con inteligencia artificial, los cuales se crean utilizando un programa denominado FakeApp. Dichos video montajes son una de las formas más nuevas de manipulación digital, y una de las más susceptibles a utilizarse para difamar a políticos, crear pornografía vengativa o tender trampas a las personas para culparlas de crímenes. Los cual debería comenzara preocuparnos por la manera en que esos videos podrían usarse como sabotaje político y propaganda.[22]

---

[20] Project Syndicate. "La libertad de expresión y las noticias falsas", trad., MELÉNDEZ TORMEN, David. Consultado en línea en: http://nuso.org/articulo/la-libertad-de-expresion-y-las-noticias-falsas/, el 2 de junio de 2018.

[21] *Op. Cit*., HERRERO, Inma.

[22]ROOSE, Kevin. "Olvídate de las noticias falsas, los video montajes ya están aquí" en The New York Times, consultado en línea en: https://www.nytimes.com/es/2018/03/07/noticias-falsas-videomontajes-deepfake-fakeapp/?rref=collection%2Fsectioncollection%2Fnyt-es&action=click&contentCollection=fake-news&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection, el 25 de junio de 2018.

4. NEUROMARKETING UNA FORMA DISTINTA DE INCIDIR EN LA DEMOCRACIA

Otra situación que nos ha causado inquietud es el tema de la neurociencia de la cual deriva el neuromarketing y por consecuencia, el neuromarketing político.

Esta subciencia se utiliza cada vez más de hecho las agencias en el mundo que se dedican a ello se han multiplicado de forma muy rápida, tan es así que en últimos días hemos escuchado sobre los conflictos en los que se encuentra el fundador de Facebook así como la declaración que rindió ante el Senado de los Estrados Unidos, hace un par de días, conflictos los cuales derivaron de la utilización de algunas apps en Facebook por parte de la empresa denominada Cambridge Analitica, con la cual recolectaban datos de los usuarios, para posteriormente conocer de forma específica características explotables, con dicha información micro segmentan pautas para dirigir mensajes políticos a la medida de los usuarios según los rasgos sociales y psicológicos de cada persona y aumentar así su efectividad para persuadir o disuadir votantes a través de noticia falsas.

Algunos casos muy notorios y de los cuales se ha hablado bastante en los medios de comunicación, en relación con las noticias falsas y el neuromarketing político son los de Trump, en Estados Unidos; el Brexit, en el Reino Unido y el Acuerdo de Paz, en Colombia.

Pero Ustedes se preguntarán qué es el neuromarketing político, lo cual contestaremos después de externar lo que es el neuromarketing, para tener una mayor claridad en los conceptos, así pues, debemos señalar que neuromarketing es la ventana para observar en el interior de la mente humana, es aquello que LINDSTROM ha denominado nuestra lógica para la compra, los pensamientos, sentimientos y deseos subconscientes que mueven las decisiones de compra que tomamos todos los días de nuestra vida.[23]

El neuromarketing funciona de la siguiente manera:
El decir sí o no, a un determinado producto depende del hipocampo (zona del cerebro relacionada con la memoria) y de su interacción con el lóbulo prefrontal. "Su marca hasta en la amígdala: hoy, gracias a la neurociencia, se sabe que es dónde se guardan las memorias más emocionales del ser humano, este lugar se llama amígdala y es justo ahí donde debe esforzarse para que su marca viva siempre"[24]. Todo lo que una persona experimenta durante cada día de su vida pasa por un proceso de almacenamiento en la memoria reciente y por un periodo muy corto forma parte del presente, pero inmediatamente después, se envía al hipocampo donde se toma la decisión de enviar la información al córtex o a la amígdala. El primero recibe la información cotidiana sin gran importancia, pero la más importante, aquella muy emocional que el hipocampo considera valiosa para formar parte de los constructos personales (teoría que postula que el significado que atribuimos a la experiencia es resultado de una construcción personal) o sistemas de referencia (generadores de reacciones instintivas), se envía a la amígdala[25]. Por lo que, "para que su marca sea poderosa, debe ser convertida en una gran experiencia y ser situada en la parte del cerebro donde las personas no la olvidarán. Para que esto sea así hay una forma sencilla de hacerlo: ¡sorpréndalos! Existen muchas recomendaciones para lograr que la experiencia de una marca sea tan poderosa que viva en la amígdala, pero una muy sencilla de recordar y no tan difícil de ejecutar es: sorprender a los clientes".[26] La experiencia de

[23] LINDSTROM, Martin. Buyology, Barcelona, editorial Gestión 2000, 2008, pág. 15.
[24] "Neuro marca", consultado en línea en: http://neuromarca.com/categoria/blog/estudios-blog/, el 20 de junio de 2018.
[25] MATILLAS BRACAMONTES, Álvaro. "Implicaciones éticas del neuromarketing", consultado en línea en: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/3602/TFG001078.pdf?sequence=1, el 22 de junio de 2018.
[26] *Ídem*.

comer una comida de su abuela, tener una charla con los mejores amigos, deslizar sus dedos por el iPad, tomar una cerveza en la playa, el primer vuelo o el día de la graduación, entre otras, viven en su amígdala.

Otras cuestiones que se trabaja el neuromarketing es el análisis de la repercusión de los anuncios televisivos de una campaña, ayudando a seleccionar el más efectivo, en qué horarios colocar cada uno, identificar los elementos que generan mayor atención, emoción y memoria, mejorar el uso de la semiótica, los personajes, el ritmo, las palabras y la música.[27]

Así pues, el neuromarketing político tiene como punto de partida la neurociencia y el marketing político, por lo que, como lo señala Néstor BRAIDOT, el neuromarketing político es aquel que "investiga y estudia los procesos cerebrales conscientes y metaconscientes que explican la percepción, la conducta y la toma de decisiones de las personas en los campos de acción de la actividad política"[28], en otras palabras, el neuromarketing político estudia el comportamiento y la conducta política de las personas con el objeto de conocer la toma de decisiones en las áreas de acción de la actividad política.

Dicho esto, nos preguntamos, realmente se cumplen los elementos fundamentales de la democracia, concretamente, la libre formación de la opinión en lo que concierne a las decisiones políticas, opinión la cual, se supone, debe ser formada lo más libremente posible o estamos siendo objeto de estudios para posteriormente tomar decisiones, si se puede llamar así, dirigidas.

Ya que, como hemos observado, las emociones tienen una mayor influencia en las decisiones de las personas que la parte racional del cerebro, puesto que el noventa y cinco por ciento de nuestro tiempo y de nuestras decisiones funcionan con el piloto automático, o como lo señala PRADEEP las decisiones que tomamos se gestan en el subconsciente.[29]

De ser así, empresas como Cambridge Analítica, lo que pretenden es direccionar nuestras acciones políticas, toda vez que buscan la información emocional de los votantes a través de las TIC´s, específicamente, las redes sociales como Facebook, Twitter e Instagram, entre otras, sin que estos sean conscientes, lo que trae como consecuencia que no puedan proteger su intimidad y a través de las denominadas fake news o noticias falsas, comúnmente, consiguen generar dichas emociones en los electores y así influenciarlos a un nivel muy profundo a través de campañas publicitarias, dirigidas a la medida de las personas, para de esta manera impulsar la decisión del voto buscada.

Así pues, esta disciplina tiene un acceso privilegiado al mundo de las emociones de las personas, debido a las mejoras tecnológicas, pues se ha facilitado la forma de obtención de información de casi cualquier sujeto, así como obtención masiva de información, el número de situaciones a estudiar aumenta, se mejoran las técnicas de medición al igual que la calidad de la información.

Y vaya que no queremos decir que la neurociencia o el neuromarketing son perniciosos, ya que ello depende de la forma en la que se utilicen, es decir, cómo obtengan la información (con o sin consentimiento de las personas), el fin último de dicha información y el cómo dirijan los resultados

---

[27] *Ídem*.

[28] BRAIDOT, Néstor. "¿Qué ocurre en el cerebro del electorado, qué ocurre en el cerebro de los candidatos?", consultado en línea en: https://www.cronista.com/columnistas/Neuroelecciones-el-cerebro-de-los-electores-20171012-0006.html, el 22 de junio de 2018.

[29] PRADEP, A. K. "El 95% de las decisiones que tomamos se gestan en el subconsciente", consultado en línea en: http://www.lavanguardia.com/ciencia/20110110/54098614275/doctor-a-k-pradeep-el-95-de-las-decisiones-que-tomamos-se-gestan-en-el-subconsciente.html, el 15 de junio de 2018.

de los estudios hechos con la citada información, más no de las disciplinas en sí mismas. Pues dicha afirmación sería como considerar que el hierro lo es. Uno puede utilizar este metal para revestir bombas que caen sobre ciudades o columnas de hospitales que salvan vidas.[30]

Pero, creemos firmemente, a pesar del debate en cuanto a esta subciencia, relativo a "si las nuevas técnicas de neuromarketing político serán capaces de revelar suficiente información acerca del funcionamiento cerebral de los sujetos como para permitir manipular a los sujetos hasta el punto en el que no son capaces de detectar la salida y que dicha manipulación resulte en el comportamiento buscado en cierto grupo de personas", que debería contar con una regulación específica, para que la información que se obtenga de las personas o las imágenes obtenidas del cerebro no se conviertan en una amenaza a la intimidad y a la libertad mental de las mismas.

5. REFLEXIONES FINALES

Es un hecho que las Tecnologías de la Información y de la Comunicación, concretamente, las redes sociales, han adquirido una gran importancia para el ejercicio de los derechos humanos, como lo es, en el presente caso, la democracia, pero también para su vulneración, por lo que es necesario que los Estados tengan un rol más activo, responsable, ético y proporcionado, claro, sin pretender que ejerzan el monopolio en la detección y represión de las noticias falsas, ya que ello abriría un camino extremadamente peligroso que nos podría llevar a conformar Estados totalitarios.

De igual manera, tanto las personas que crean las noticias falsas como nosotros mismos, somos responsables de vulnerar el elemento fundamental del derecho humanos denominado democracia, al cual hemos hecho referencia en el cuerpo de este ensayo, pues privilegiamos la información de primera mano antes que los medios informativos confiables y bajo la premisa de la liberta de difundir la información sin limitación de fronteras, por cualquier medio de expresión, utilizando comúnmente las TIC´s, puesto que hoy en día, resultan ser algo asequible casi para cualquier persona, ya que la mayoría de la población puede acceder a ellas, logramos amplificar la desinformación y, consecuentemente, la ignorancia y el descontento social, cada vez que publicamos o compartimos dicha información.

En razón de lo anterior, debemos ser cautelosos y conscientes de la actividad que desarrollamos a través de las TIC´s y, en la medida de nuestras posibilidades, pasar por un reforzamiento de la producción de información de calidad a gran escala, obviando los corta y pega y la reproducción automática de contenidos sin verificación alguna, puesto que, la protección del referido derecho humano, así como los diversos derechos que se desprenden y relacionan con el mismo, no sólo dependen del Estado, sino de la sociedad en general, esto es, desde las personas que consumen información y probablemente la difunden, hasta los medios de comunicación, los anunciantes y las plataformas tecnológicas, entre otros.

En lo que concierne al neuromarketing político, así como todo lo que conlleva su realización, consideramos que es necesario poner límites tanto a las personas que se dedican a esta sub ciencia, como a todos los entes que intervienen para su realización, toda vez que, estamos hablando de blogueros, influencer, empresas o personas que se dedican a obtener información concreta para posteriormente generar noticias falsas a la medida, en este caso, de los votantes; pero también estamos hablando de las plataformas a través de las cuales, en muchos casos, se obtiene la información de las personas, como es el caso de Google o Facebook, pues se convierten en un problema de grandes dimensiones, ya que ninguno se hace cargo de lo que consume la audiencia, en virtud de que, "no

[30] "Neuromarketing y ética" en Brain and marketing: un viaje al corazón del neuromarketing, consultado en línea en: http://brainandmarketing.blogspot.mx/2015/05/etica-del-neuromarketing.html, el 18 de junio de 2018.

cuentan con filtros netamente funcionales" los cuales detecten los entes que roban información ni mucho menos los que emiten las fake news, violentando de esta manera, el derecho fundamental, referido en el presente ensayo, así como muchos otros.

Así pues, se requiere regular los derechos digitales, fijar verdaderos límites a la privacidad y diseñar, no sólo protocolos de actuación, sino normatividad vinculante, a través de la cual se les pueda procesar, respetando en todo momento sus derechos humanos, para de esta forma, exigir reparaciones por los daños que pudieran generar, mientras se mejoran los ecosistemas digitales para erradicar conflictos como el que ahora señalamos.

6. REFERENCIAS BIBLIOGRÁFICAS

- ARTEAGA NAVA, Elisur. Tratado de derecho constitucional (segunda edición), Vol. 1, editorial Oxford, México, 2002.

- BOBBIO, Norberto. Teoría general del derecho y del Estado, editorial UNAM, México, 1958.

- BRAIDOT, Néstor. "¿Qué ocurre en el cerebro del electorado, qué ocurre en el cerebro de los candidatos?", en: https://www.cronista.com/columnistas/Neuroelecciones-el-cerebro-de-los-electores-20171012-0006.html.

- BUSTILLO PORRO, Vicenta. "Nuevas tecnologías de la información: Herramientas para la educación", en: http://campus.usal.es/~teoriaeducacion/rev_numero_06/n6_art_bustillo.htm.

- CORTÉS FIERRO, Ernesto. "Del populismo a la posverdad / Voy y vuelvo", en: http://www.eltiempo.com/bogota/voy-y-vuelvo-sobre-populismo-y-posverdad-97644.

- Derecho al acceso y uso de las tecnologías de la información y de la comunicación, en el Centenario de la Constitución Política de los Estados Unidos Mexicanos, editorial CNDH-SEP-INEHRM, México, 2015.

- DÍAZ REVORIO, Francisco Javier. Los derechos humanos ante los nuevos avances científicos y tecnológicos, editorial Tirant lo Blanch, España, 2009.

- El Tiempo. "Carta abierta a los posverdaderos", en: http://www.eltiempo.com/bocas/carta-abierta-de-la-revista-bocas-a-los-posverdaderos-agosto-2017-121170.

- Enciclopedia Jurídica Mexicana, editorial Instituto de Investigaciones Jurídicas de la UNAM/Porrúa, T. III, México, 2002.

- FERRAJOLI, Luigi. Poderes salvajes. La crisis de la democracia constitucional, editorial Trotta, Madrid, 2011.

- FONTEVECCHIA, Agustino. "Fake News: El cáncer de la web gestado por Google y Facebook", en: http://www.perfil.com/tecnologia/fake-news-el-cancer-de-la-web-gestado-por-google-y-facebook.phtml.

- HERRERO, Inma. "Fake news, posverdad y redes sociales", en: https://www.biblogtecarios.es/inmaherrero/fake-news-posverdad-y-redes-sociales/.

- LINDSTROM, Martin. Buyology, Barcelona, editorial Gestión 2000, 2008.

- MATILLAS BRACAMONTES, Álvaro. "Implicaciones éticas del neuromarketing", en: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/3602/TFG001078.pdf?sequence=1.
- "Neuro marca", en: http://neuromarca.com/categoria/blog/estudios-blog/.

- "Neuromarketing y ética" en Brain and marketing: un viaje al corazón del neuromarketing, en: http://brainandmarketing.blogspot.mx/2015/05/etica-del-neuromarketing.html.

- PÉREZ CUEVAS, Carlos Alberto. "Los retos de la democracia" en Las aportaciones de las entidades federativas a la reforma del Estado, edición al cuidado de Máximo N. GÁMIZ PARRAL y José Enrique RIVERA RODRÍGUEZ. Editorial UNAM, México, 2005.

- PRADEP, A. K. "El 95% de las decisiones que tomamos se gestan en el subconsciente", en: http://www.lavanguardia.com/ciencia/20110110/54098614275/doctor-a-k-pradeep-el-95-de-las-decisiones-que-tomamos-se-gestan-en-el-subconsciente.html.

- Project Syndicate. "La libertad de expresión y las noticias falsas", trad., MELÉNDEZ TORMEN, David. En: http://nuso.org/articulo/la-libertad-de-expresion-y-las-noticias-falsas/.

- ROOSE, Kevin. "Olvídate de las noticias falsas, los video montajes ya están aquí" en The New York Times, en: https://www.nytimes.com/es/2018/03/07/noticias-falsas-videomontajes-deepfake-fakeapp/?rref=collection%2Fsectioncollection%2Fnyt-es&action=click&contentCollection=fake-news&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=collection.

- SARTORI, Giovanni. Teoría de la democracia, editorial Alianza Universidad, Madrid, 1988.

- Secretaría Nacional de Tecnologías de la Información y Comunicación (SENATIC's). "Las TIC's en el Gobierno", en: https://prezi.com/5oscnazc_s0e/las-tics-en-el-gobierno/.

SOBRE LA NATURALEZA JURÍDICA DEL DERECHO INFORMÁTICO. EL CASO DE MÉXICO

Por: ***Arturo Labastida Contreras***
México

A) ONTOPRAXIOLOGÍA DEL DERECHO INFORMÁTICO.

Ubi societas, ibi jus. Donde hay sociedad hay Derecho, en función de ello el Derecho más que originador de sociedades es producto social según la sociología contemporánea; en el caso del derecho informático esta verdad no puede ser más cierta, máxime cuando la sociología jurídica y las tendencias de interpretación jurídica reconocen el impacto que las revoluciones científicas y tecnológicas han producido en el orden jurídico, pues el desarrollo acelerado de la revolución científica, a lo largo de sus períodos, compone uno de los agentes, rasgos y componentes centrales de la época contemporánea. La intensidad, la velocidad y la profundidad de sus tendencias y efectos se hacen sentir en mayor o menor grado sobre todos los niveles y aspectos de las sociedades nacionales y sobre el sistema internacional en su conjunto.

El impacto pluridisciplinario de la revolución científica y tecnológica es apreciable concretamente en el plano del Estado y el derecho. La atención que politólogos y juristas han prestado a éste fenómeno decisivo para las disciplinas y prácticas profesionales, se ha incrementado paulatinamente, al grado que se requiere una especialización con la que cada rama del conocimiento, aborde este fenómeno. La necesidad de avanzar en la construcción de tal materia, correspondiente a la revolución científica y tecnológica contemporánea, proyecta ante todo dificultades del enfoque a elegir y usar, y de las condiciones y niveles de análisis jurídico y jurídico social para entender al derecho informático, a modo de producto jurídico insito a esta evolución científico-tecnológica en el contexto de la globalización dela economía de mercado; efectivamente este fenómeno, por lo menos a nivel muy elemental debiera de atenderse para su conocimiento, tanto por la sociología jurídica, como por el propio derecho informático en calidad de disciplina jurídica, con sus propios principios y como sistema de conocimientos en plena construcción; prueba de ello es que en este último aspecto, es por demás conocido el principio de equivalencia funcional, como inherente y determinante por excelencia, del derecho informático, máxime que dicho principio subyace vigente en diversas normas del derecho mexicano y extranjero.

Por otra parte, en lo relativo a la sociología jurídica y otras ciencias que estudian este fenómeno del derecho, el universo de investigación se torna bastante amplio, sin embargo a este nivel de abstracción, se puede concluir que serán tres los aspectos que definirán en el conglomerado socio jurídico, al propio derecho informático, es decir y a forma de triángulo equilátero, la economía, la tecnología y el orden Jurídico; entidades estas últimas que no están aisladas, sino interconectadas, en un desarrollo histórico, material, dinámico y dialéctico; en donde el conocer la relaciones del todo con la parte y viceversa, permitirá desentrañar la esencia del derecho informático en sí y para sí.

Cabe agregar que desde los siglos IXX y XX, y con motivo del ascenso de la economía capitalista en occidente, se han plateado diversas teorías, que buscan entender los nexos entre tales entidades; por lo que dichas teorías deben de servir de punto de partida, para conocer este objeto de conocimiento denominado " derecho informático ", fenómeno jurídico, que revitaliza la investigación, en una época en la que se considera que el análisis de esta naturaleza se encontraba estancado y en franca decadencia. Un sistema de usos y costumbres mercantiles en el comercio internacional, han conformado de manera sustantiva la existencia del derecho informático con normas y principios que

le son característicos, como es el de equivalencia funcional entre otras; al tenor de ello, podemos afirmar que este sistema de normas, tiene su razón de ser histórico-jurídica así como su justificación ontológica, en función de las siguientes premisas:

En primer término cual costumbre inveterada en el ámbito del comercio internacional, los comerciantes tuvieron y crearon un derecho propio, reimplantado en Europa con el renacimiento del comercio. El "derecho mercantil" era una forma de ley internacional cuyos elementos fundamentales era la facilidad con que permitía la celebración de contratos obligatorios, el acento puesto en la seguridad de los contratos, y la diversidad de mecanismos que preveía para la concesión, transmisión y recepción del crédito. A lo largo de la edad media, la aplicación del derecho mercantil a los litigios referentes al comercio se difundió a los tribunales reales, a las cortes eclesiásticas, y hasta las cortes señoriales feudales .Para el comerciante internacional, la ley mercantil era imprescindible. La Ley Mercantil al menos en teoría, se aplicaba uniformemente a los negocios entre mercaderes de todos los países. La transformación de ese derecho internacional en legislación nacional llego a evolucionar y constituir la base jurídica del comercio internacional contemporáneo a nivel mundial, hasta nuestros días, en las que esas prácticas jurídicas, se observan como requisito indispensable en el marco de la economía capitalista mundial.

Cabe agregar que diversos autores, entre ellos Henry Maine afirman que el transito del feudalismo al capitalismo se logró por medio de la institución jurídica del contrato, como practica del comercio internacional. En segundo término, una de las características más destacadas de la economía de mercado, es la permanente revolución científico-tecnológica en el ámbito de la producción, lo cual ha devenido entre otras cosas, en el desarrollo de las tecnologías de la información, que como lo señala Alvin Tofler, esas tecnologías ponen a disposición del cualquier persona una cantidad de información incontable e inimaginable; como acontece con el internet, que permite la comunicación y el intercambio de información entre usuarios en lugares distintos.

Sin embargo sin negar lo vertido por ese autor, ello no puede entenderse escindido de la necesidad del mercado de incorporar nuevas mercancías para el público, así como la existencia de la sociedad de consumo, intrínseca a un sistema económico fincado en la libre empresa, de ahí que la información en si misma se inserta en la dinámica de la producción capitalista, convirtiéndose así en un producto susceptible de adquirirse en el mercado, que en el marco de la civilización del consumo ha configurado, lo que autores como Javier Cremades denominan Sociedades de la Información, que dicho autor, y que se caracterizan según los creadores de este concepto, por la capacidad de sus integrantes para obtener y compartir cualquier información de modo inmediato y en cualquier lugar; dicha aseveración permite inferir que ello no es sino, reflejo de la producción industrial y de un aumento en la producción de bienes y servicios que modifico profundamente la estructura del mercado, que en el afán de expandirse allende sus fronteras, y conforme a su naturaleza se auxilia de la tecnología ahora como informática, para promover la abundancia y diversidad de productos existentes en su seno, e inducir al público consumidor a adquirir bienes y servicios, bajo el principio de que consumir implica utilizar mercancías y servicios en razón directa de las necesidades humanas, una de las cuales es entre otras la información; ello bajo la práctica de los denominados contratos telemáticos, que agilizan como no sucedió en ninguna otra época, estas grandes transacciones del comercio nacional internacional hasta crear una nueva práctica jurídica denominada comercio Iuscibernético; de ahí la importancia de la información por medios electrónicos, como medio para lograr que dichos actos de comercio sustentados en la figura del contrato telemático, tengan mayor celeridad y contribuyan a mejorar la mecánica del andamiaje de la economía de mercado a nivel nacional e internacional .

En este contexto el derecho informático , ha incidido en el orden jurídico, puesto que todas las áreas del derecho se han visto afectadas por la aparición de la denominada Sociedad de la Información,

alterando procesos sociales, políticos y jurídicos, ya que hoy se puede observar que las practicas del derecho informático, han trascendido del ámbito de los negocios privados al de la Administración Publica y las garantías individuales, a partir del uso de los medios electrónicos, para ejercer entre otros, el Derecho de Acceso a la Información Pública, en el derecho electoral, asimismo la protección a los datos personales; también en los registros públicos donde la expedición de documentos certificados, denota en todos esos casos el principio de equivalencia funcional, punto toral del derecho informático, lo cual acontece en el Registro civil y el Registro Público de la Propiedad; en el ámbito de las relaciones entre trabajadores y patrones, con motivo de la prestación del trabajo personal subordinado, y desde luego en todas las áreas del orden jurídico que al regular conductas humanas, requieren ser más eficientes y más eficaces. En conclusión, el derecho informático es un producto jurídico de esta globalización de la economía de mercado; como práctica jurídica ha justificado su condición ontopraxiológica, fincando sus propios principios, en el seno de la sociedad de la información; es así una rama del derecho especializada en el tema de la informática, sus usos y aplicaciones en el ámbito jurídico, es decir un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la aplicación de la informática en ese ámbito de derecho. Cabe citar como sinopsis, lo señalado por el Maestro Alejandro Loredo Álvarez "LEX MERCATORIA" "LEX INFORMATICA".

B) RESPECTO DE LAS GRANDES DIVISONES DEL ORDENAMIENTO JURÍDICO.

Antes de abordar el tema de la naturaleza jurídica del derecho informático, es necesario tener como precedente las bases teórico jurídicas de la clasificación del orden jurídico; al efecto debe señalarse, que una de las clasificaciones más discutidas y difíciles de fundamentar jurídicamente, es la que distingue dos parte principales en el derecho objetivo: derecho público y derecho privado. Esta distinción es tradicional y nos viene del derecho romano, sin embargo, el criterio de diferenciación no se ha considerado suficientemente fundado. Por esto los juristas han ensayado constantemente nuevos criterios para formular esta división de las normas jurídicas. Independientemente de los distintos criterios que se han adoptado y puedan acogerse para clasificar al derecho desde el punto de vista público o privado, una primera reflexión se impone en cuanto a la naturaleza misma del derecho en general, que por definición y por esencia siempre ha sido y será un conjunto de normas de indiscutible interés público.

Se nota por consiguiente la tendencia en el derecho moderno, en el sentido de negar valor a la distinción tradicional romana de derecho público y derecho privado. Sin embargo aun cuando es difícil fundar un criterio de distinción, no obstante, en la clasificación de las diversas ramas de esos grandes sectores del derecho, la uniformidad de los autores está de acuerdo en que las normas jurídicas relacionadas con la organización del Estado de manera directa (derecho constitucional, derecho administrativo, penal e internacional público) o indirecta (derecho procesal) son indiscutiblemente derecho público, en tanto que las reglas relacionadas con la organización de la familia y el patrimonio (derecho civil y mercantil) son también consideradas unánimemente como derecho privado. Al lado de estas ramas, existen en algunos Estados, derechos de reciente creación, el agrario, el laboral , el autoral, de protección al consumidor etc. como expresiones del denominado derecho social que según el maestro Alberto Trueba Urbina, en su obra intitulada " La Primera Constitución Político Social del Mundo", lo define como ".....el conjunto de principios, instituciones y normas que protegen, tutelan y reivindican los derechos de los que viven de su trabajo y a los económicamente débiles...."

Sin embargo se puede concluir que las normas jurídicas por sus características sancionadoras de la conducta humana, por su destino que es regular comportamientos humanos y por el órgano que los crea, que es el Estado, son de naturaleza pública. Los juristas están de acuerdo en que en la época contemporánea, no obstante el auge de la privatización de sectores de la administración pública, aún

prevalece, el fenómeno jurídico denominado publificación del derecho privado, pues de acuerdo con las circunstancias imperantes, aquellas normas que en un momento dado estaban incluidas en algún cuerpo legal considerado de derecho privado, han pasado a ocupar un lugar dentro de las del derecho público, conforme se iba acentuando la intervención estatal en determinados aspectos de la vida socioeconómica. Esta irrupción del estado ha sido origen de múltiples discusiones acerca de la naturaleza jurídica de dichas normas que de forma poco usual y por disposición de la ley, pasan a ser tuteladas por el estado de manera directa.

En nuestro país, existen modelos notables de este fenómeno, como sucede con la legislación mercantil, en virtud del interés del estado por la actividad financiera, las inversiones extranjeras, la protección al consumidor y la minería, como acontece con las regulaciones que norman lo relativo a la ecología. Por lo que al derecho mercantil se refiere, es única la vinculación que el derecho público, tiene con esta segunda mitad del derecho privado. Aparte de haberle expropiado significativos campos, como el derecho marítimo, que ha vuelto público, funda con él regímenes jurídicos de combinación de gran empalma.

Esto último ocurre en el derecho de los bancos, en el monetario, en el derecho del comercio exterior, en el de las sociedades anónimas y cooperativas, en el fomento industrial y otros análogos, aquí se fusionan normas de derecho administrativo y normas de derecho mercantil. Es de colegirse que bajo la anterior óptica, el comercio internacional en nuestro país se regula por normas de derecho público, como parte de un régimen híbrido administrativo mercantil. Independientemente de lo expresado debe considerarse sobre el particular, lo señalado por el Jurista Austriaco Hans Kelsen, en su obra "Teoría Pura del Derecho" respecto de las relaciones jurídicas en el derecho público y privado: "....Típico ejemplo de una relación de derecho público es la orden administrativa, una norma individual implantada por el órgano administrativo, mediante la cual el sujeto al cual la norma se dirige queda jurídicamente obligado a comportarse conforme a lo ordenado.

En cambio, como relación típicamente de derecho privado tenemos el negocio jurídico, especialmente: el contrato, es decir, la norma individual producida por contrato, mediante la cual las partes contratantes quedan obligadas jurídicamente a un comportamiento reciproco. Mientras, que en este último ejemplo los sujetos obligados participan en la producción de la norma que los obliga- y en ello reside la esencia de la producción contractual del derecho-, en la orden administrativa de derecho público, el sujeto obligado no tiene participación alguna en la producción de la norma que lo obliga. Se trata del caso típico de una producción autocrática de normas, mientras que el contrato privado significa un notorio método democrático de producción de derecho.

De ahí que ya la teoría más antigua designara la esfera de los negocios privados, como el dominio de la autonomía privada." "....Solo aquello que se denomina derecho privado, el complejo de normas en cuyo centro se encuentra la institución jurídica del así llamado derecho de propiedad individual privado, es desde el punto de vista de la función que esa parte del orden jurídico, tiene con el contexto de la totalidad del derecho, una forma adecuada de producción de normas jurídicas individuales para el sistema económico-capitalista...." En un sistema nacional e internacional de relaciones jurídicas diversas, complejas y dinámicas, es que el derecho informático con los principios que le son inherentes, otorga en paralelo, celeridad con legalidad en la prosecución de tales actos jurídicos, en especial para con los efectos de derecho que en forma de obligación jurídica en su sentido más lato, producen en los sujetos que los celebran y que ahora demandan tengan verificativo a la velocidad que solo se logra en el ciberespacio; de ahí que determinar la naturaleza jurídica de este sistema de normas de derecho, solo podrá lograrse en función del bien jurídico tutelado por dicha institución jurídica del mundo contemporáneo.

C) DETERMINACIÓN DE LA NATURALEZA JURÍDICA DEL DERECHO INFORMATICO EN FUNCION DEL BIEN JURIICO TUTELADO.

En términos generales, bien jurídico se puede entender como el objeto de protección de las normas de derecho. El bien jurídico en el iusnaturalismo tomista y humanista, se encuentra implícito dentro del derecho natural, pues deriva respectivamente de la voluntad emanada de Dios o de la racionalidad humana. Por su parte el iuspositivismo, en el sentido de no tomar en cuenta el derecho natural, el bien jurídico es arbitrariamente fijado por el legislador, de acuerdo a su propio criterio. En la teoría Kelseniana, determinar el bien jurídico es labor del legislador, más no del científico del derecho. Convencionalmente puede entenderse como una acción de buena fe para la protección jurídica de una sociedad; por ejemplo cuando el poder legislativo da leyes para el bien de la sociedad, como el derecho a la vivienda etc.

Es de tomarse en cuenta, que en el caso predominante del derecho público, se verifica el hecho notorio de que se relaciona con otras ciencias, ello manifestado en leyes administrativas que regulan actividades de la administración pública y de los particulares, por ello hay leyes administrativas muy técnicas llenas de conocimientos no jurídicos. Por ejemplo la Ley General de Salud, se apoya en la ciencia sanitaria, dicha ley es un típico caso de ayuda del derecho por parte de un área del conocimiento no jurídico. Hoy existen normas técnicas, expedidas por el secretario facultado por las leyes que enumeran y se publican en el Diario Oficial de la Federación con obligatoriedad. La legislación ecológica también se caracteriza por normas técnicas que elaboran los legisladores con asistencia de los ecologistas.

El derecho administrativo se relaciona con todas aquellas ciencias que proporcionan a la administración los elementos necesarios para organizar y encaminar su actividad en las diversas tareas que al Estado se encuentran encomendadas. La ciencia del derecho administrativo y este como tal, en el desarrollo de su sistema o aplicación, tiene relación con otras ciencias y con otras ramas del derecho, ya que no son fenómenos aislados e independientes. Al tenor del anterior razonamiento jurídico, en el caso que nos ocupa, y dado que el derecho informático, es insito a la utilización de los medios electrónicos para entender su calidad ontológica y su teleología, será por conducto de la ciencia de la informática, lo que nos permitirá dilucidar ese bien jurídico tutelado; en ese orden de ideas podemos decir resumidamente que la informática es el sistema de técnicas que suministra el manejo vertiginoso sino automático de la información.

En su sentido más genérico la información es la acción y efecto de informar o informarse; asimismo informar es enterar o dar noticia de una cosa. En el caso que nos ocupa, nuestro objeto de conocimiento y bien jurídico a determinar, es una información específica que por su naturaleza contiene a su vez actos jurídicos, ya que pone en conocimiento situaciones de derecho de distinta índole, constituyendo así una manera de realizar esos actos con sus respectivas consecuencias en el ámbito del derecho, principalmente porque expresa la voluntad por vía telemática de aquellos quienes los celebran, como es el caso de la firma electrónica ,los contratos telemáticos etc.; además de que sus destinatarios por esa vía electrónica, están en conocimiento de que al recibir tal información, se verá impactada su esfera de derechos, pues una vez realizada su recepción, surte sus efectos el correspondiente acto jurídico.

Bajo este antecedente y cual binomio indisoluble, concurrirá esta información en la categoría de corpus mistycum, en medios electrónicos en calidad de corpus mechanicum, como el bien jurídico que para el derecho informático es materia de protección de parte de las normas de derecho, todo ello partiendo del hecho conspicuo de que la información contenida en esos medios telemáticos cual continente material, es a su vez portadora de esos actos jurídicos, información con efectos de derecho

que inserta en un soporte electrónico configuran lo que algunos autores denominan como Iuscibernetica.

Así el parámetro a partir del cual se determinara su naturaleza jurídica, será en función de aquellas normas de derecho que tutelan ese bien jurídico; a guisa de aproximación, no se puede soslayar que existe una expresa regulación del derecho a la información. Sobre el particular el artículo 6º. Constitucional establece en su parte final que:

"...PARA EL EJERCICIO DEL DERECHO DE ACCESO A LA INFORMACION, LA FEDERACION, LOS ESTADOS Y EL DISTRITO FEDERAL, EN EL AMBITO DE SUS RESPECTIVAS COMPETENCIAS, SE REGIRAN POR LOS SIGUIENTES PRINCIPIOS Y BASES: (ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 20 DE JULIO DE 2007.) I. TODA LA INFORMACION EN POSESION DE CUALQUIER AUTORIDAD, ENTIDAD, ORGANO Y ORGANISMO FEDERAL, ESTATAL Y MUNICIPAL, ES PUBLICA Y SOLO PODRA SER RESERVADA TEMPORALMENTE POR RAZONES DE INTERES PUBLICO EN LOS TERMINOS QUE FIJEN LAS LEYES. EN LA INTERPRETACION DE ESTE DERECHO DEBERA PREVALECER EL PRINCIPIO DE MAXIMA PUBLICIDAD. (ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 20 DE JULIO DE 2007.) II. LA INFORMACION QUE SE REFIERE A LA VIDA PRIVADA Y LOS DATOS PERSONALES SERA PROTEGIDA EN LOS TERMINOS Y CON LAS EXCEPCIONES QUE FIJEN LAS LEYES. (ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 20 DE JULIO DE 2007.) III. TODA PERSONA, SIN NECESIDAD DE ACREDITAR INTERES ALGUNO O JUSTIFICAR SU UTILIZACION, TENDRA ACCESO GRATUITO A LA INFORMACION PUBLICA, A SUS DATOS PERSONALES O A LA RECTIFICACION DE ESTOS. (ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 20 DE JULIO DE 2007.) IV. SE ESTABLECERAN MECANISMOS DE ACCESO A LA INFORMACION Y PROCEDIMIENTOS DE REVISION EXPEDITOS. ESTOS PROCEDIMIENTOS SE SUSTANCIARAN ANTE ORGANOS U ORGANISMOS ESPECIALIZADOS E IMPARCIALES, Y CON AUTONOMIA OPERATIVA, DE GESTION Y DE DECISION.

(ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 20 DE JULIO DE 2007.) V. LOS SUJETOS OBLIGADOS DEBERAN PRESERVAR SUS DOCUMENTOS EN ARCHIVOS ADMINISTRATIVOS ACTUALIZADOS Y PUBLICARAN A TRAVES DE LOS MEDIOS ELECTRONICOS DISPONIBLES, LA INFORMACION COMPLETA Y ACTUALIZADA SOBRE SUS INDICADORES DE GESTION Y EL EJERCICIO DE LOS RECURSOS PUBLICOS. (ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 20 DE JULIO DE 2007.) VI. LAS LEYES DETERMINARAN LA MANERA EN QUE LOS SUJETOS OBLIGADOS DEBERAN HACER PUBLICA LA INFORMACION RELATIVA A LOS RECURSOS PUBLICOS QUE ENTREGUEN A PERSONAS FISICAS O MORALES. (ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 20 DE JULIO DE 2007.) VII. LA INOBSERVANCIA A LAS DISPOSICIONES EN MATERIA DE ACCESO A LA INFORMACION PUBLICA SERA SANCIONADA EN LOS TERMINOS QUE DISPONGAN LAS LEYES. (ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 20 DE JULIO DE 2007.) ..."

Debe destacarse la relación, que este dispositivo tiene con el artículo 16 del texto constitucional, que expresa sobre el particular que: TODA PERSONA TIENE DERECHO A LA PROTECCION DE SUS DATOS PERSONALES, AL ACCESO, RECTIFICACION Y CANCELACION DE LOS

MISMOS, ASI COMO A MANIFESTAR SU OPOSICION, EN LOS TERMINOS QUE FIJE LA LEY, LA CUAL ESTABLECERA LOS SUPUESTOS DE EXCEPCION A LOS PRINCIPIOS QUE RIJAN EL TRATAMIENTO DE DATOS, POR RAZONES DE SEGURIDAD NACIONAL, DISPOSICIONES DE ORDEN PUBLICO, SEGURIDAD Y SALUD PUBLICAS O PARA PROTEGER LOS DERECHOS DE TERCEROS. (ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 1 DE JUNIO DE 2009)

La parte final del artículo 6º constitucional fue el resultado de la reforma política de 1977. La interpretación de la Corte del derecho a la información ha variado con el paso del tiempo; inicialmente consideró que se trataba de una garantía electoral a favor de los partidos, pero después amplio su criterio hasta equiparar este derecho con una garantía individual .El derecho a la información no es sino un complemento a la libertad de expresión, pues no puede opinar correctamente quien no se encuentra bien informado. En este sentido, el 11 de junio de 2002 se publicó en el Diario Oficial de la Federación la Ley de Transparencia y Acceso a la Información Pública Gubernamental, que es de orden público y, aun cuando no reglamente el artículo 6º constitucional ,tiene-según su artículo 1º- la finalidad de "proveer lo necesario para garantizar el acceso de toda persona a la información en posesión de los Poderes de la Unión, los órganos constitucionales autónomos o con autonomía legal, ya cualquier otra entidad federal".

Al tenor de lo anterior, el artículo 9º. De dicha ley establece que las autoridades pondrán información a disposición del público "a través de medios remotos o locales de comunicación electrónica". Esa es, pues, la forma en que las autoridades deben garantizar que los particulares accedan a ciertos datos que la ley no considera información reservada o confidencial. Es de subrayarse que la referida Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, expresa en su capítulo primero, ordinal tercero, fracción quinta, que "Información es la contenida en los documentos que los sujetos obligados generen, obtengan, adquieran, trasformen o conserven por cualquier título". Con mayor perspicuidad se expresa en relación a la información como bien jurídico, la Ley de Transparencia y Acceso a la información pública del Distrito Federal, al señalar en su artículo tercero que "Toda la información Generada, administrada o en posesión de los Entes Públicos, se considera un bien del dominio público, accesible a cualquier persona en los términos y condiciones que establece esta Ley y demás normatividad aplicable".

Esa Ley además establece en su numeral cuarto, fracción novena que " Información Pública es todo archivo, registro o dato contenido en cualquier medio, documento o registro impreso, óptico, electrónico, magnético, químico ,físico o biológico que se encuentre en poder de los entes públicos y que no haya sido previamente clasificada como de acceso restringido". Citando el concepto del jurista Rafael I. Martínez Morales, dominio público es "....El sector de los bienes del estado sobre los cuales este ejerce una potestad soberana, conforme a reglas del derecho público, a efecto de regular su uso y aprovechamiento, y de esa manera asegurar su preservación o explotación racional..." Se puede conjeturar así que los bienes del dominio público son aquellos los cuales se pueden aprovechar en uso y disfrute de los miembros de la comunidad, responden a la satisfacción de una utilidad pública y de los cuales los particulares no pueden apropiarse.

En México los bienes del Dominio Público de la Federación tienen como características que son bienes que forman el patrimonio nacional, son usados por la comunidad y aprovechados eventualmente por esta, por lo cual son de interés general y de utilidad pública, están sujetos al régimen de derecho público, no crean derechos reales sobre los particulares pues solamente pueden usar y disponer de ellos, en los términos y condiciones que señalan las leyes, pero nunca pueden adquirir la propiedad de los mismos, son bienes fuera del comercio, es decir inalienables e imprescriptibles y sus límites son fijados unilateralmente por la Administración Pública Federal. Es sabido dentro de la doctrina administrativa que los bienes de uso común, a que se refiere el artículo

segundo de la Ley General de Bienes nacionales, se trata de aquellos que pueden usarlos todos los miembros de la comunidad con la única limitación que señalan las leyes en los casos correspondientes. También pueden ser aprovechados por los particulares, pero para ello se requiere la autorización legal correspondiente.

Es inconcuso que la información soportada en medios electrónicos, y por tanto como una de sus especies aquella que sirve de portadora de actos jurídicos, es un bien tutelado por el derecho público, es del dominio público y de uso común; esta Iuscibernética es de naturaleza jurídico publica, pues ha transitado de las prácticas comerciales de los particulares, a los demás ámbitos públicos del fenómeno jurídico, máxime cuando el comercio exterior cual actividad mercantil, es regulada por normas administrativas como anteriormente se expresó, de ahí que esos actos jurídicos cual actos de comercio se regulan por normas de derecho público, en consecuencia su concreción informática, es así de naturaleza pública; máxime cuando hasta este momento ninguna institución del derecho privado ha expresado en absoluto concepto alguno, sobre la naturaleza jurídica de la información jurídica soportada en medios telemáticos, pues como ya se ha indicado, esa tutela acontece por intermediación de normas de derecho administrativo.

Es inconcebible un contrato sin leyes ni jueces; cobra así relevancia el Poder Judicial, que es el que cuenta con las atribuciones necearías para administrar justicia de manera cumplida y para mantener el equilibrio de los demás poderes. Una de las funciones más importantes del Poder Judicial de la Federación es proteger el orden constitucional. Para ello, se vale de diversos medios, entre ellos, el juicio de amparo, las controversias constitucionales, las acciones de inconstitucionalidad y la facultad de investigación. Cabe señalar que todos los medios señalados incluyen entre sus fines, de manera relevante, el bienestar de la persona humana.

Es de considerarse lo establecido en los artículo 8,13,14 y 18 de la citada Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, ya que inciden en los actos procésales de los particulares al interior de una litis de derecho privado, efectivamente el Poder judicial De la Federación, deberá hacer públicas las sentencias que hayan causado estado, o ejecutoria y las partes podrán oponerse a la publicación de sus datos personales; por otra parte el reglamento de la Suprema Corte de Justicia de la Nación y del Consejo de la Judicatura Federal , dispone en sus artículo 5º y 6º del citado reglamento ,disponen que la información que tiene bajo su resguardo la Suprema Corte de Justicia de la Nación, el Consejo de la Judicatura Federal y los órganos jurisdiccionales, es publica, con las salvedades establecidas en la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, podrán ser consultados por cualquier persona, en los locales en que se encuentren y en las horas de labores, siempre y cuando se cumpla con los requisitos que garanticen la integridad de la documentación que contienen, los cuales serán fijados por las respectivas comisiones de transparencia; que las constancias que obren expedientes de asuntos concluidos que se encuentren en resguardo de la Suprema Corte de Justicia o de los órganos jurisdiccionales las aportadas por las partes, siempre y cuando les hayan atribuido expresamente tal característica al momento de allegarlas al juicio y que tal clasificación base en lo dispuesto en algún tratado internacional o en ley expedida por el Congreso de la Unión o la Legislatura De los Estados. Por otra parte 5 jul 2010 se expide la Ley Federal de Protección de Datos personales en Posesión de los Particulares, de tal modo que su capítulo primero, relativo a Disposiciones Generales, establece:

Artículo 1.- La presente Ley es de orden público y de observancia general en toda la República y tiene por objeto la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas. Es de medular importancia, considerar lo establecido en el Capítulo Segundo de la ley en comento, intitulado " De los Principios de Protección de Datos Personales", que en los dispositivos que lo forman , ordena: "...CAPÍTULO II

De los Principios de Protección de Datos Personales Artículo 6.- Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en la Ley. Artículo 7.- Los datos personales deberán recabarse y tratarse de manera lícita conforme a las disposiciones establecidas por esta Ley y demás normatividad aplicable. La obtención de datos personales no debe hacerse a través de medios engañosos o fraudulentos. En todo tratamiento de datos personales, se presume que existe la expectativa razonable de privacidad, entendida como la confianza que deposita cualquier persona en otra, respecto de que los datos personales proporcionados entre ellos serán tratados conforme a lo que acordaron las partes en los términos establecidos por esta Ley.

Es interesante el pronunciamiento de la Suprema Corte de Justicia, en materia de privacidad y protección de datos personales: Registro No. 176077 Localización: Novena Época Instancia: Tribunales Colegiados de Circuito Fuente: Semanario Judicial de la Federación y su Gaceta XXIII, Enero de 2006 Página: 2518 Tesis: XIII.3o.12 A Tesis Aislada Materia(s): Administrativa TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL. LA CONFIDENCIALIDAD DE LOS DATOS PERSONALES SÓLO CONSTITUYE UN DERECHO PARA LAS PERSONAS FÍSICAS MAS NO DE LAS MORALES (AUTORIDADES RESPONSABLES).

De la interpretación sistemática de los artículos 1, 3, 4, 8, 18 a 22 y 61 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, en relación con el Acuerdo General 76/2003, del Pleno del Consejo de la Judicatura Federal, que modifica los artículos 19 y tercero transitorio del Acuerdo General 30/2003, que establece los órganos, criterios y procedimientos institucionales para la transparencia y acceso a la información pública para ese órgano del Poder Judicial de la Federación, los Tribunales de Circuito y los Juzgados de Distrito, se advierte que entre los objetivos de la ley citada se encuentra el garantizar la protección de los datos personales en posesión de los sujetos obligados, es decir, la información concerniente a una persona física, identificada o identificable, y para lograrlo otorgó facultades al Pleno del Consejo de la Judicatura Federal, el que dictó los acuerdos correspondientes, estableciendo en relación con los datos personales de las partes, que con el fin de respetar cabalmente tal derecho, al hacerse públicas las sentencias, se omitirán cuando manifiesten su oposición de manera expresa, e impuso a los órganos jurisdiccionales la obligación de que en el primer acuerdo que dicten en los asuntos de su competencia, señalen a las partes el derecho que les asiste para oponerse, en relación con terceros, a esa publicación, en la inteligencia de que la falta de oposición conlleva su consentimiento para que la sentencia respectiva se publique sin supresión de datos; de donde se concluye que la protección de los datos personales de referencia sólo constituye un derecho para las personas físicas, pues así lo señala la fracción II del artículo 3 de la ley mencionada, al indicar que por aquellos debe entenderse la información concerniente a una persona física identificada o identificable, excluyendo así a las personas morales, entre las que se encuentran las autoridades responsables.

TERCER TRIBUNAL COLEGIADO DEL DÉCIMO TERCER CIRCUITO.

Amparo en revisión 550/2004. Tesorería de la Federación y otras. 21 de enero de 2005. Unanimidad de votos. Ponente: Robustiano Ruiz Martínez. Secretaria: Elena Elvia Velasco Ríos. Reclamación 12/2005. Director Regional de Vigilancia de Fondos y Valores de la Tesorería de la Federación. 12 de septiembre de 2005. Unanimidad de votos. Ponente: Robustiano Ruiz Martínez. Secretaria: Elena Elvia Velasco Ríos. Nota: El Acuerdo General 30/2003 citado, aparece publicado en el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XVIII, noviembre de 2003, página 1065. Sin embargo una meditación de este tipo, no puede soslayar el elemento humanista consustancial a cualquier consideración jurídica, en el caso que no ocupa ello nos permite arribar a la relación del

derecho informático con los derechos humanos, como estudiosos del derecho debemos ubicarnos, en el mundo de la axiología jurídica y encontrar su aplicación partiendo del hecho, de que ese sistema normativo es una herramienta de ingeniería social, para tutelar el derecho a la información , el derecho a la privacidad y cualquier otro derecho que inserto cual información pueda ser tutelado por el orden jurídico; situación que acentúa, por lo menos en el contexto mexicano, su naturaleza de derecho público. Solo bajo estas premisas, el derecho informático podrá vincularse como palanca impulsora de los derechos humanos de los mexicanos cual norma de orden público e interés social, habiéndose logrado avances axiomáticos ya transcritos en el texto constitucional y la legislación secundaria; ello adquiere mayor relevancia, si se considera lo que el artículo 1º de la Constitución General de la República que con un sentido humanista expresa:

ARTICULO 1o. EN LOS ESTADOS UNIDOS MEXICANOS TODAS LAS PERSONAS GOZARAN DE LOS DERECHOS HUMANOS RECONOCIDOS EN ESTA CONSTITUCION Y EN LOS TRATADOS INTERNACIONALES DE LOS QUE EL ESTADO MEXICANO SEA PARTE, ASI COMO DE LAS GARANTIAS PARA SU PROTECCION, CUYO EJERCICIO NO PODRA RESTRINGIRSE NI SUSPENDERSE, SALVO EN LOS CASOS Y BAJO LAS CONDICIONES QUE ESTA CONSTITUCION ESTABLECE. (REFORMADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 10 DE JUNIO DEL 2011) LAS NORMAS RELATIVAS A LOS DERECHOS HUMANOS SE INTERPRETARAN DE CONFORMIDAD CON ESTA CONSTITUCION Y CON LOS TRATADOS INTERNACIONALES DE LA MATERIA FAVORECIENDO EN TODO TIEMPO A LAS PERSONAS LA PROTECCION MAS AMPLIA. (ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 10 DE JUNIO DEL 2011) TODAS LAS AUTORIDADES, EN EL AMBITO DE SUS COMPETENCIAS, TIENEN LA OBLIGACION DE PROMOVER, RESPETAR, PROTEGER Y GARANTIZAR LOS DERECHOS HUMANOS DE CONFORMIDAD CON LOS PRINCIPIOS DE UNIVERSALIDAD, INTERDEPENDENCIA, INDIVISIBILIDAD Y PROGRESIVIDAD. EN CONSECUENCIA, EL ESTADO DEBERA PREVENIR, INVESTIGAR, SANCIONAR Y REPARAR LAS VIOLACIONES A LOS DERECHOS HUMANOS, EN LOS TERMINOS QUE ESTABLEZCA LA LEY.

(ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 10 DE JUNIO DEL 2011) ESTA PROHIBIDA LA ESCLAVITUD EN LOS ESTADOS UNIDOS MEXICANOS. LOS ESCLAVOS DEL EXTRANJERO QUE ENTREN AL TERRITORIO NACIONAL ALCANZARAN, POR ESTE SOLO HECHO, SU LIBERTAD Y LA PROTECCION DE LAS LEYES. (ADICIONADO MEDIANTE DECRETO PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 14 DE AGOSTO DEL 2001) QUEDA PROHIBIDA TODA DISCRIMINACION MOTIVADA POR ORIGEN ETNICO O NACIONAL, EL GENERO, LA EDAD, LAS DISCAPACIDADES, LA CONDICION SOCIAL, LAS CONDICIONES DE SALUD, LA RELIGION, LAS OPINIONES, LAS PREFERENCIAS SEXUALES, EL ESTADO CIVIL O CUALQUIER OTRA QUE ATENTE CONTRA LA DIGNIDAD HUMANA Y TENGA POR OBJETO ANULAR O MENOSCABAR LOS DERECHOS Y LIBERTADES DE LAS PERSONAS. (REFORMADO MEDIANTE DECRETO, PUBLICADO EN EL DIARIO OFICIAL DE LA FEDERACION EL 10 DE JUNIO DEL 2011)

D) DERECHO INFORMATICO PARA QUE: Siendo el derecho en su acepción más general, un sistema de normas que regulan la conducta humana, la conducta humana desplegada en usar los medios electrónicos, en el ámbito nacional e internacional, si bien en el contexto mundial aún prevalece una ardua discusión en torno a su naturaleza jurídica, lo cierto es que a nivel nacional cada país ha realizado importantes avances legislativos, tendientes a regular el uso de los medios telemáticos en su contexto jurídico local, lo cual significa un progreso, partiendo del hecho de que en

el año 2004, aun se plateaba por algunos autores el uso de los medios electrónicos, con otras ramas del derecho, pero aún no se contemplaba su regulación. El caso de México denota una regulación parcial, partiendo del hecho de que ahora tiene presencia en el Código Civil Federal y en el Código de Comercio, así como en otras normas, pero aún no existe algún estatuto legal que ex profeso regula esa conducta, lo cierto es que ello se ha ido haciendo necesario. En conclusión la protección constitucional al derecho a la información, así como la regulación administrativa de la información inserta en medios electrónicos emitida y en disposición de los poderes de la unión, por último y hasta ahora, la protección de los datos personales a favor del individuo, permite concluir que al ser la información contenida en medios electrónicos es un bien de uso común y la naturaleza jurídica del derecho informativo se suscribe dentro del derecho público.

MÍNIMA INTERVENCIÓN PENAL Y COMENTARIOS EN LAS REDES SOCIALES

José Romo Santana
Universidad Técnica de Ambato- Ecuador[1]

1. TABLA DE CONTENIDO

2. LOS LÍMITES DEL DERECHO PENAL. -

Es relevante iniciar señalando que el poder punitivo de cualquier Estado democrático debe circunscribirse dentro de demarcaciones político – criminales claramente definidas, respetando principios constitucionales y legales. En consecuencia, toda decisión en materia de política criminal debe guiarse desde la perspectiva de la mínima intervención y de un Derecho Penal subsidiario, fragmentario, residual y de *última ratio.* [2]

Es así como el poder punitivo estatal (entendido como una realidad fáctica), resulta solo legitimo en tanto sea ejercido dentro de los límites jurídicos que el Derecho Penal impone. [3], lo cual implica una aplicación desde todas las esferas del principio de legalidad, el cual en el caso ecuatoriano tiene rango constitucional, y se representa como un eje transversal del sistema jurídico, por medio del cual toda persona que actúe en virtud de una potestad estatal, ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y en la Ley.
Si el Estado de Derecho exige el sometimiento de la potestad punitiva al principio de legalidad y en el estado social dicha potestad solo se legitima si sirve de eficaz y necesaria protección de la sociedad, un estado que además pretenda ser democrático tiene que llenar el Derecho Penal de un contenido respetuoso de una imagen del ciudadano como dotado de una serie de derechos derivados de su dignidad humana, de la igualdad (real) de los hombres y de su facultad de participación en la vida

[1] *Abogado, Especialista en Derecho de la Alta Tecnología, Especialista en Derecho Procesal, Magister en Derecho Penal.*
[2] **Zaffaroni, Eugenio Raúl . 2007.** *Manual de Derecho Penal. Parte General* . Buenos Aires : Ediar, 2007, pag. 14
[3] **García Falconí, Ramiro. 2014.** *Código Orgánico Integral Penal Comentado.* Segunda. Quito : Latitud Cero Editores, 2014, Pág. 40

social [4], en consecuencia el poder punitivo del Estado, se debe activar única y exclusivamente cuando se esté poniendo en riesgo bienes jurídicos innatos a la calidad de ser humano.

El artículo 3 del Código Orgánico Integral Penal, consagra el principio de mínima intervención y señala que "a intervención penal está legitimada siempre y cuando sea estrictamente necesaria para la protección de las personas. Constituye el último recurso, cuando no son suficientes los mecanismos extrapenales.[5] Lo cual evidencia que el sistema penal ecuatoriano se alinea a las posturas dogmáticas y filosóficas respecto al ejercicio de la potestad penal.

Una de las formas de regular el poder punitivo, evitar el castigo arbitrario y las ilegales violaciones a la libertad personal y a los derechos de propiedad es el debido proceso; el mismo que podemos entenderlo como el cumplimiento de las garantías procesales de manera efectiva y certera, [6] tales reglas en el caso ecuatoriano están determinadas en la Ley Suprema y tienen una aplicación directa en toda clase de procesos ya sean administrativos y judiciales.

Resulta siempre importante citar al maestro Luigi Ferrajoli, quien hizo un aporte muy importante al construir un modelo garantista el que a través de axiomas enuncia diez garantías elementales para plantear o definir la responsabilidad penal, las primeras seis son sustancias y las cuatro restantes son adjetivas y son las siguientes:

A1 *Nulla poena sine crimine*. A2 *Nullum crimen sine lege*. A3 *Nulla lex (poenalis) sine necessitate*. A4 *Nulla necessitas sine iniuria*. A5 *Nulla iniuria sine actione*. A6 *Nulla actio sine culpa*. *A7 Nulla culpa sine iudicio*. A8 *Nullum iudicium sine accusatione*. A9 *Nulla accusatio sine probatione*. A10 *Nulla probatio sine defensione.*[7] (Ferrajoli, 1995 pág. 93)

Los modelos teóricos del derecho penal resultan de la inclusión de todos o parte de estos principios, siendo el sistema garantista aquel ordenamiento penal concreto que incluya todos los axiomas de esa serie.

Estos axiomas han sido desarrollados en los principios de retributividad, legalidad, necesidad, lesividad, materialidad, culpabilidad, jurisdiccionalidad, acusatorio, carga de la prueba y contradictorio. Todos ellos se encuentran impregnados en el ordenamiento ecuatoriano, tanto de forma Constitucional como legal, por lo tanto, son de cumplimiento obligatorio para jueces y autoridades administrativas, en consecuencia, el sistema legal ecuatoriano es un sistema garantista de derechos y garantías.

Es importante resaltar el hecho de que cada uno de los diez axiomas citados anteriormente corresponde a uno de los tres momentos básicos del derecho penal: la pena, el delito y el proceso, además se constituyen en un escudo de los ciudadanos contra acciones arbitrarias de los administradores de justicia, como el hecho de emitir sentencias condenatorias, respecto de acciones que no son plausibles de sanción penal, ya que podrían haberse discernido y solucionado en otra esfera legal.

Ferrajoli realiza una distinción entre las garantías primarias o derechos fundamentales como límites al poder público; y las garantías secundarias como los recursos necesarios para hacer efectivas las

[4] **Mir Puig, Santiago. 2016.** *Derecho Penal Parte General.* [ed.] Julio César Faira. Barcelona : Bdef, 2016, pag. 133.
[5] **Asamblea Nacional de la República del Ecuador . 2014.** *Código Orgánico Integral Penal.* Quito : Registro Oficial, 2014.
[6] **Gozaini, Osvaldo. 2004.** *Derecho Procesal Constitucional. El debido proceso* . Buenos Aires : Rubinzal-Culzoni, 2004, pag. 25.
[7] **Ferrajoli, Luigi. 1995.** *Derecho y Razón, Teoría del Garantismo Penal.* [trad.] Perfecto Andrés Ibañez, y otros. Madrid : Editorial Trotta, 1995, pag. 93.

garantías primarias, pero la función de todas las garantías tienden a condicionar el ejercicio absoluto de la potestad punitiva del Estado.

3. EL DERECHO AL HONOR. -

El objeto de este trabajo es justamente analizar un derecho cuya definición puede tener aristas subjetivas, de acuerdo a la persona, y la realidad social, el derecho al honor, y que en varias legislaciones de países iberoamericanos tiene rango constitucional, y se procede al análisis en los siguientes términos:

La palabra honor, viene del latín *honor* y *honoris*, que evidentemente ha servido para describir cualidades como rectitud, dignidad, reputación, que una persona pública debía tener. Además, entre sus características de acuerdo al autor ecuatoriano Felipe Rodríguez, el honor era inherente e igualitario. No obstante, hoy en día el derecho al honor tiene sus diversas percepciones adoptada por varios autores. [8]

Desde el origen de la sociedad y el derecho, se tiene la intención de proteger el honor de las personas, por lo menos de aquellas que se consideraban como tal en la sociedad. Así pues, en el derecho mesopotámico antiguo, existía el Código de Shulgi, en el cual mencionaba el derecho al honor y presentaba algunas regulaciones que permitía sancionar pecuniariamente a quienes atentaran con el honor de la persona. De igual manera en la Ley de las XII Tablas Romana, se sancionaba con pena de muerte aquellos que compusieran canciones que produjeran la infamia o deshonra de otro. En la edad media, la moral burguesa mantenía a la honra y la dignidad en el derecho de familia. Sin embargo, cobra importancia luego de la Segunda Guerra Mundial.

Conforme a la concepción griega, ningún ser humano podía llegar a ser completamente feliz si no adquiría honor. Por otro lado, los romanos tenían una alta estima al honor que lo personificaron en un dios, y lo consideraron como el valor supremo que determinaba la actitud ante la vida y el respeto de sus semejantes. Más adelante, en el medioevo, el honor dejo de ser exclusivo para la nobleza, extendiéndose a todas las clases sociales. Así, en el siglo XIX se distinguieron diferentes clases de honor, de acuerdo a la cultura, a la sociedad y a determinados grupos.[9]

Por lo tanto, al honor se lo puede concebir como una parte de la dignidad de la persona, que se encuentra vinculado con el cumplimiento de los deberes éticos. Para lo cual, Lorenzo citado en la obra del autor Ignacio Berdugo[10]considera que el honor está relacionado a la dignidad humana como atributo de la personalidad. Por consiguiente, el honor es la dignidad y la autoestima de la persona, y la fama es el reflejo exterior de esa dignidad. Por lo tanto, el honor junto con el de intimidad y la propia imagen constituye parte de los derechos de la personalidad y por lo tanto, de los derechos fundamentales e influyentes en la dignidad de la persona.

Según el tratadista italiano Adriano De Cupis, el honor es considerado como la dignidad personal, la que se refleja en el respeto de los demás y en el sentimiento de la propia persona.[11] En consecuencia, el objeto de los derechos de la personalidad es interior al sujeto, no exterior a él, como los restantes bienes objeto de derechos subjetivos.

---

[8] **Rodriguez Moreno, Felipe. 2017.** *Manual de delitos contra el Honor y Libertad e Expresión.* Quito : Cevallos, 2017, pag. 68.
[9] **Rodriguez Moreno, Felipe,** *Manual de delitos contra el Honor y Libertad e Expresión, op. Cit., p. 35-39.*
[10] **Berdugo de la Torre, Ignacio. 1985.** *Revisión del Contenido bien jurídico honor, en homenaje a Hilde Kaufmann.* Buenos Aires : De Palma, 1985, pag. 56.
[11] **De Cupis, Adriano. 1982.** *Derecho a la Personalidad.* Milán : Guifré, 1982, pag 124.

En concordancia con lo señalado, se puede afirmar que el honor es el bien jurídico de la dignidad de la persona, pero que esta se exterioriza en la sociedad. Concluyendo, que al honor no se le puede destruir o desaparecer, solamente porque le injuriaron o calumniaron, debido a que al ser parte de la dignidad está siempre, va a permanecer y lo único que puede producir es la disminución que la sociedad tenía sobre esa persona.[12]

Cuando se afecta al honor de un individuo, sus repercusiones son sociales, indudablemente, y más cuando muchas personas han tomado como costumbre el publicar en las redes sociales ciertos acontecimientos, como por ejemplo los nombres de sus supuestos deudores o acosadores.
De esta manera el tratadista Berdugo de la Torre indica que el honor al constituirse por las relaciones y los valores fundados por la sociedad, ésta establece ciertos parámetros en los cuales se puede desarrollar esa dignidad y personalidad permitiéndole su trascendencia. Sin embargo, cuando esta persona rompe los esquemas su dignidad queda en duda. [13]

Para comprender de mejor manera al honor, como lo indica Muñoz Conde se debe distinguir dos concepciones. La objetiva, que se entiende como el juicio que tiene la sociedad por una persona; y la subjetiva, aquella que está conformada por la conciencia y los sentimientos que tiene la persona sobre su propio prestigio. En conclusión, el honor objetivo es la fama y reputación social (exterior) y el honor subjetivo es la estimación (interior)[14]. En *estricto sensu* el primero se relaciona con la buena fama del que goza la persona y ha trascendido en su medio social por los actos, y el segundo, correspondería a la autoestima propia según lo señalado por la tratadista Ana Laura Cabezuelo[15].

Además, desde una perspectiva jurídica el honor, tiene tres posturas, que le dan cierta limitación, y son: la fáctica, la normativa y la mixta. Así, por ejemplo, si regresamos a la época burguesa, una prostituta no podía reclamar el respeto a su honor, porque la sociedad le interrogaría de qué honor habla. Sin embargo, desde una perspectiva normativa la prostituta tiene honor y nadie le podrá señalar como tal.[16] De esta manera, la postura normativa, permite reconocer el honor de las personas de forma igual respetando la libertad que tiene cada sujeto de elegir su forma de vida, y limitando ciertos juicios de valor que puede generar rechazo social.
Por lo expuesto, el honor casi siempre tendrá como refractario a la libertad de expresión. De esta manera, cuando se discute el honor de una persona es porque ha entrado en colisión la libertad de expresión, sin embargo, trae más consecuencias cuando la noticia es difundida por medios de comunicación social y en redes sociales.

De acuerdo a las consideraciones analizadas, se debe tener en cuenta la excepción con las personas que son figuras públicas. Si bien el contexto normativo no hace excepciones sobre el honor según las personas, la doctrina y la jurisprudencia, sí. Por ende, quienes han decidido ser personajes públicos, voluntariamente someten su vida a la sociedad, las cuales deben aceptar las críticas que nunca van a faltar. Sin embargo, esto tiene un límite, el cual no debe sobrepasar la vida privada.[17]
Con ello, el Tribunal Constitucional y Tribunal Supremo de Justicia Españoles citados en la obra del propio Rodríguez Moreno, mediante fallos 8-6-88, N°107/1988 y 3-6-88, RJ1988/4430, respectivamente, manifiestan que cuando el honor se refiere a personas públicas, la libertad de

[12] **Lombana Villalba, Jaime. 2009.** *Injuria, Calumnia y Medios de Comunicación.* Medellín : Biblioteca Jurídica Diké, 2009, pag. 26.
[13] **Berdugo de la Torre, Ignacio,** *Revisión del Contenido bien jurídico honor, en homenaje a Hilde Kaufmann, op.cit,* p 263.
[14] **Muñoz Conde, Francisco. 1999.** *Derecho Penal Parte Especial.* Valencia : Tirant lo Blanch, 1999, pag. 268.
[15] **Cabezuelo Arenas, Ana Laura. 1998.** *Derecho a la Intimidad.* Valencia : Tirant lo Blanch, 1998, pag. 93
[16] **Rodriguez Moreno, Felipe,** *Manual de delitos contra el Honor y Libertad e Expresión, op. cit., p. 64.*
[17] **Rodriguez Moreno, Felipe,** *Manual de delitos contra el Honor y Libertad e Expresión, op. cit., p. 142.*

expresión tiene mayor eficacia. Esto quiere decir, que cuando la libertad de expresión atenta el honor de una persona que ejerce funciones públicas o de relevancia social, la libertad de expresión e información se justifica frente al derecho al honor, debilitándolo proporcionalmente. [18]
En corolario, cuando nos encontramos frente a personas que están ocupando dignidades de elección popular, puestos directivos en instituciones públicas y privadas, entre otras, aumenta considerablemente la tolerancia a críticas a estos cargos, hace algunos años, las mismas en su gran mayoría se las efectuaba en medios de comunicación, ya que eran los medios más idóneos para comunicación masiva, en la actualidad basta con un comentario en una red social, para desatar debates entre simpatizantes y opositores que indudablemente puede generar afectaciones a los intervinientes.

4. REDES SOCIALES. -

En los últimos años indudablemente nuestras vidas han tenido cambios sustanciales, principalmente para los que nacimos desde 1985 hacia atrás, nuestro entorno de infancia y juventud se caracterizó por una interacción física y directa con nuestros amigos, nuestros mayores tesoros eran las historietas y revistas, y nuestro contacto con la tecnología, con el avance de los años, fue con nuestras series favoritas de la televisión. Sin duda las críticas a los personales públicos se las efectuaba en la mayoría en los diarios y en ciertos programas de opinión tanto radiales como televisivos.
Poco a poco se introdujo en nuestra vida la era de la computación que reemplazaba a las máquinas de escribir en las cuales aprendimos mecanografía, y en un momento determinado llego Internet y sus innumerables posibilidades, a nuestros hogares y trabajos y velozmente tuvimos que adaptarnos para no quedarnos desactualizados.

Las herramientas que brindaba Internet eran cada vez más básicas para nuestras actividades académicas y laborales en todos los campos del conocimiento humano y de pronto a inicios de este milenio aparecieron las redes sociales que ampliaban este espectro a las relaciones interpersonales. En la actualidad es casi impensable que alguien no este activo en las redes sociales; incluso las diferentes instituciones públicas o privadas tienen constante actividad ya no solo por medio de sus páginas web; sino en las redes sociales, ya que es el lugar idóneo para contactarse con sus clientes, por los altos índices de conectividad que estas redes han generado en nuestra sociedad.
De acuerdo al portal WebEmpresa20, el top ten de las redes sociales en la actualidad es de la siguiente forma: 1 *Facebook*, 2 *WhatsApp*, 3 *YouTube*, 4 *WeChat*, 5 QQ, *6 Instagram*, 7 *QZone*, 8 *Tumblr*, 9 *LinkedIn*, 10 *Twitter*.[19]

Las redes sociales, según el autor Keller citado por Gallego, son los conjuntos o tejidos de relaciones entre un grupo de personas, que están unidos directa o indirectamente, voluntaria o involuntariamente a comunicaciones y compromisos a través de los cuales buscan dar u obtener algo de los demás. Por consiguiente, esta nueva forma de crear comunidades le dan el carácter de virtual, permitiéndolo compartir fotografías, videos, información, entre otros.[20] Así, el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información, determina que las redes sociales permiten al usuario crear perfiles, lista de contactos, entre otros, convirtiéndose en un servicio para la sociedad[21].
El perfeccionamiento de las actividades en Internet se produjo con la llegaba de la Web 2.0. Con ello, lo primero que se pretende categorizar desde un ámbito jurídico son los servicios que las redes

[18] **Rodriguez Moreno, Felipe,** *Manual de delitos contra el Honor y Libertad e Expresión, op. Cit., p. 145.*
[19] WebEmpresa20.com, https://www.webempresa20.com/blog/las-30-redes-sociales-mas-utilizadas.html, 04 de julio de 2018.
[20] **Gallego Trijueque, Sara. 2011.** Sistema de Información Científica Redalyc. *Redes Sociales y Desarrollo Humano.* [En línea] 15 de Septiembre de 2011. [Citado el: 4 de Julio de 2018.] http://www.redalyc.org/pdf/3221/322127622007.pdf, pag. 117.
[21] **Guilayn, Albert. 2016.** *Aspectos Legales de las Redes Sociales.* Barcelona : Bosh, 2016, pag. 20.

sociales pueden brindar[22]. Considerando que el principal elemento de las redes son los usuarios a través de sus perfiles, pues los datos que en ellas se comparte, es de carácter personal y por lo tanto se considera una información esencial que requiere protección legal.
Efectivamente, el crecimiento exponencial de la Internet, lo ha transformado en un habitual lugar para cometer actos ilícitos. Además, estos actos ilícitos pueden ser civiles y penales, con su respectiva responsabilidad y sanción. [23]Sin embargo, en el ámbito penal es algo difícil reprimir por diversos motivos como la falta de tipificación específica, la transnacionalidad de las conductas, las calumnias difundidas por Internet, entre otras, siendo difícil su control.

Las redes sociales, en un inicio fueron espacios cibernéticos por medio de los cuales se encontraban antiguas amistades y familiares poco contactados; pero en la actualidad son sitios web que basan su funcionamiento en capitalizar estas relaciones sociales, en crear valor aprovechando esas relaciones de amistad, parentesco, afinidad, etc., prestando servicios que son percibidos a modo de extensiones virtuales de las redes sociales a las que uno pertenece en el mundo *off-line*.[24].
Asimismo, en las redes sociales se involucran derechos de terceros, por ello darle un mal uso, equivaldría delitos que acarrearían sanciones penales. Principalmente, porque la normativa penal se ha convertido en un instrumento fundamental para combatir estos abusos malintencionados[25]. En cuanto a los delitos más comunes son: usurpación de identidad, amenazas, coacciones, descubrimiento y revelación de secretos, contra la integridad moral o sexual, contra el honor y enaltecimiento del terrorismo.

Además, como lo determina el autor Máximo Ortega, los medios digitales por medio de la Internet han permitido cometer delitos tanto en un país como en una ciudad, efectuándose las consecuencias en otro lugar de donde se cometió el delito.[26] Este efecto se conoce como la extraterritorialidad de la ley penal, lo que significa que se requiera una normativa internacional que regule las infracciones sobre todo aquellas injurias y calumnias que atenta el honor de la persona.
Sin embargo, para toda esta evolución, la doctrina así como la jurisprudencia, según Alejandro Barbini, aceptaron al principio de ubicuidad, para aplicar cuando surja un problema en la territorialidad de la ley, especialmente en la jurisdicción y competencia. Además, surge la figura de delitos de distancia, que son aquellas infracciones que se cometen en un lugar pero sus efectos se producen en otro. [27]

Por consiguiente en este tipo de delitos cabe la aplicación del principio, porque permite comprender que el lugar en donde se cometió el delito también se produjo los efectos, por ende establece la competencia territorial, no obstante la jurisdicción debe estar enmarcada en la economía procesal.
De acuerdo al autor Ortega Vintimilla, la normativa penal ecuatoriana en materia digital reconoce el lugar de los hechos como territorio digital. Así, lo establece en el Código Orgánico Integral Penal en sus artículos 460.8 y 500, en el que determina que el reconocimiento del lugar de los hechos se lo realizará en territorio digital, servicios digitales, equipos o medios tecnológicos. Además, se requiere

[22] **Guilayn, Albert,***Aspectos Legales de las Redes Sociales, op. cit.* , p 23.
[23] **Fernández Delpech, Horacio. 2001.** *Internet: Su problemática jurídica* . Buenos Aires : Abeledo Perrot, 2001, pag. 150.
[24] **Nieto Martín, Adán y Maroto, Manuel. 2013.** Las redes sociales en Internet como instrumento de control penal: Tendencias y límites. [aut. libro] Artemi Rallo Lombarte y Ricard Martínez. *Derecho y Redes Sociales.* Pamplona : Arazandi S.A., 2013, pag. 441.
[25] **Guilayn, Albert,***Aspectos Legales de las Redes Sociales, op. cit.* , p 81.
[26] **Ortega Vintimilla, Máximo. 2018.** *Las Calumnias y las expresiones en descrédito o deshonra perpetradas por medios digitales: Facebook, Whats App y más.* Quito : Editorial Jurídica del Ecuador, 2018, pag. 79
[27] **Barbini, Alejandro. 2015.** *Correo electrónico, redes sociales y proveedores de Internet en el proceso penal.* Buenos Aires : La Rocca, 2015,pag. 72.

de un perito para que reconozca donde se encuentra la cuenta de la red social, el IP o desde donde se envió el mensaje mas no se requiere determinar desde que equipo de cómputo se envió el mensaje.[28] La legislación española ha conocido casos en los cuales se ha dictado sentencias relacionado con el Cyberbullying, que analizan determinados nombres de dominio para atribuir la autoría de determinadas injurias y calumnias, escritas en esos sitios web y redes sociales.

Por ejemplo, se dio un caso en el cual el acusado reconoció haber usado el seudónimo de "chispas" en la página web para expresarse con palabas como "ladrón", cuestión que le sirvió al juez para declarar que ha lesionado la dignidad de la persona, imputándole el delito de injuria. A su vez, otro caso que se suscitó, fueron los insultos públicos en la web contra un político, en donde no eran meras criticas protegidas por el derecho a la libertad de expresión, sino que eran insultos que estaban atentando el honor de la persona con el fin de desprestigiarlo[29].

5. PRINCIPALES TIPOS PENALES CON LOS CUALES SE ATENTA AL HONOR DE LAS PERSONAS. -

5.1. CALUMNIA. -

A la calumnia, se la puede definir, como la manera de difamar o mentir, acusando falsamente a otra persona de un delito[30]. Por otro lado, cierto lado de la doctrina determina que la calumnia es un tipo de injuria agravada.

Para que la conducta de calumnia se configure como tipo penal, debe cumplir con ciertos requisitos de idoneidad para calificarla como tal. De esta manera, el ataque debe ser directo y público. Por el contrario cuando, una persona acusa falsamente a otra de forma privada, no cabría delito de calumnia, por no ser un acto público. Además la imputación debe ser determinada; esto quiere decir que la calumnia debe estar dirigida a una persona determinada y que la imputación debe ser precisa. Como por ejemplo, no es lo mismo decir de forma general que alguien es ladrón, a decir que Juan Pérez es ladrón. [31]
Consecuentemente, para imputar el delito de calumnia, se lo debe realizar de forma escrita o verbal, sin que se reconozca la acción gestual o corporal. Para que exista delito de calumnia no es preciso que la imputación falsa se realice con la denominación legal técnica. Por el contrario, lo importante es que se ejecute la calumnia y sea fácilmente identificable. [32] Además, el elemento subjetivo de la calumnia, es el conocimiento de la falsedad, por lo tanto, se considera que es un delito doloso y no culposo. Con ello, el sujeto activo conoce la intención que tiene de menoscabar el honor del sujeto pasivo.

En la calumnia la acción va dirigida a la imputación o atribución falsa de un delito en contra de un tercero, es decir se atribuye la responsabilidad de una acción, típica. antijurídica y culpable, a un tercero que no ha tenido ninguna clase de participación.

---

[28] **Ortega Vintimilla, Máximo,** *Las Calumnias y las expresiones en descrédito o deshonra perpetradas por medios digitales: Facebook, Whats App y más, op. cit.,*pag. 109.
[29] **Bueno de Mata, Federico. 2014.** *Prueba Electrónica y Proceso 2.0.* Valencia : Tirant lo Blanch, 2014, pag. 148.
[30] **Huerta, Guerrero Luis Alberto. 2002.** *libertad de expresión y acceso a la información pública.* Lima - Peru : Comisión Andina de Juristas , 2002, pag. 58.
[31] **Rodriguez Moreno, Felipe,** *Manual de delitos contra el Honor y Libertad e Expresión, op. Cit., p. 324.*
[32] **Rodriguez Moreno, Felipe,** *Manual de delitos contra el Honor y Libertad e Expresión, op. Cit., p. 330.*

Para comprender de mejor manera el delito de calumnia, el Tratadista Rodríguez Moreno, realiza un análisis a la normativa determinada en el art. 182 del Código Orgánico Integral Penal del Ecuador COIP. Concibe que el verbo rector, es *realizar* y el verbo auxiliar es *imputar*. Por ende, esta realización puede ser hecha por cualquier medio, de forma activa u omisiva; así el verbo rector final sería *realizar imputación.* Además, el elemento objetivo de la calumnia, es el resultado que se obtenga del verbo *realizar,* que sería como estima la normativa la *falsa imputación de un delito en contra de otro.*[33] En otras palabras, esto quiere decir que la falsedad es subjetiva o personal y que el calumniador es consciente de que su imputación es falsa contra un tercero.

Es necesario referirse al inciso final del Art. 182 ibídem, en el cual hace mención la *retractación*. Esta institución jurídica, nace en Italia en la edad media, la cual es un mecanismo que permite archivar el proceso penal en cualquier momento de la causa, hasta antes de que se dicte sentencia. Sin embargo, esto no quiere decir que al retractarse se esté eliminando la responsabilidad, simplemente se archiva el proceso.
A esta altura es relevante señalar que la retractación puede darse en cualquier momento, sin necesidad de que se dicte sentencia. Puede darse en la contestación a la querella, en la etapa de prueba, en la audiencia de conciliación y juzgamiento, e incluso mediante cualquier escrito que se presente en cualquier momento. [34]

Es necesario señalar que según lo señalado por Jorge Buompadre, en su obra delitos contra el honor, citado por el propio Rodríguez, no es posible que la retracción siempre sea eficaz y placentera, pues por la forma de imputar falsamente el delito, puede resultar imposible retractarse, siendo la única salida que el ofendido acepte una disculpa personal y garantía de no repetición, caso contrario el juez, no puede aceptar la retracción.
Indudablemente, la figura más grave del delito contra el honor determinado en la normativa penal ecuatoriana, es la calumnia. Pues al considerarse el honor legal el bien jurídico protegido por este tipo de delito, lo está considerando como aquel honor que le pertenece a todas las personas como derecho. El bien jurídico honor es algo inmaterial y valorativo, sujeto a los cambios sociales, y la lesión recae sobre un valor con componentes objetivos y subjetivos que de él surgen.

5.2. INJURIA. -

A la injuria se la puede definir en términos generales como un atentado al honor de las personas, utilizando diferentes mecanismos para lograr dañar el bien jurídico tutelado, según el tratadista Buompadre Jorge Eduardo citado por Felipe Rodríguez en su Manual de delitos contra el honor la injuria es la acción de proferir expresiones que menoscaben la honra de una persona o, en palabras más sencillas: la injuria es principalmente la manifestación de un juicio de valor que implica una desaprobación de la posición que la persona ofendida tiene en la sociedad. [35]

En consecuencia la injuria es el acto público, que afecta el honor objetivo, es decir la imagen pública de una persona en la sociedad; por ejemplo, decir públicamente que alguien engaña a su pareja, esposo o esposa con otra persona. Es la expresión que golpea la dignidad de una persona lacerando su reputación o atentando contra su propia estima. Puede estar en la atribución de algunos hechos, formulando juicios de valor sobre el individuo.

La doctrina ha establecido ciertos parámetros para regular el tratamiento penal de esta clase de conductas y se dice que en ningún caso configurarán delito de injurias las expresiones referidas a

[33] **Rodriguez Moreno, Felipe,** *Manual de delitos contra el Honor y Libertad e Expresión, op. Cit., p. 317.*
[34] **Rodriguez Moreno, Felipe,** *Manual de delitos contra el Honor y Libertad e Expresión, op. Cit., p. 334.*
[35] **Rodriguez Moreno, Felipe,** *Manual de delitos contra el Honor y Libertad e Expresión, op. Cit., p. 394.*

asuntos de interés público o las que no sean asertivas. Tampoco configurarán delito de injurias los calificativos lesivos del honor cuando guardasen relación con un asunto de interés público. [36]

Lo señalado anteriormente ahonda más su esfera subjetiva, ya que dependerá del administrador de justicia determinar si el asunto es de interés público, sin dejar de lado el contenido de los comentarios; por cuanto si se utiliza términos agresivos y falsos, que ponen en evidente riesgo el desarrollo de las actividades permanentes de la persona atacada, si causa conmoción en un determinado conglomerado, o pone en riesgo la prestación de un servicio público, se debe activar el poder punitivo del Estado; sin perjuicio del resto de acciones legales a las que hubiere lugar.

En cuanto a la acción típica, diremos en este caso que la misma consiste en que una o más personas publiquen, es decir, den a conocer a personas indeterminadas (que no pudieron conocerlas antes), o reproduzcan, es decir, vuelvan a producir o repitan también con llegada a terceros (aunque sea una sola persona); injurias o calumnias proferidas por otro.

En el caso Ecuatoriano, con la promulgación del Código Orgánico Integral Penal, esto es el 10 de febrero del 2014, el tratamiento de esta temática, tuvo un cambio radical; puesto que en la actualidad únicamente existe la injuria como tal, la cual sigue siendo una infracción penal pero dejó de ser delito y ahora es contravención, conforme se señala a continuación:
Artículo 396.- Contravenciones de cuarta clase.- Será sancionada con pena privativa de libertad de quince a treinta días: 1. La persona que, por cualquier medio, profiera expresiones en descrédito o deshonra en contra de otra. Esta contravención no será punible si las expresiones son recíprocas en el mismo acto (…) [37]

La legislación ecuatoriana es clara en determinar que el bien jurídico tutelado es el honor objetivo, puesto que el proferir expresiones de la forma señalada tiene que encausar procesos en los cuales únicamente haya que probar la clase de honor señalado anteriormente.
Indudablemente, el tener un encuadre más sencillo de las injurias ha sido un avance significativo en la legislación ecuatoriana; puesto que de cierta forma esta clase de procesos se los ventila de forma sumaria y no como delito, sino como contravención y si el juzgador cuenta con elementos de convicción, podrá resolver la causa con una sentencia que no podrá exceder de los 30 días, para muchos quizá no sea lo óptimo, pero de todas formas el campo de acción está delimitado, y la carga punitiva de la sanción tiene un límite definido, lo cual impide las sanciones desproporcionales que antes existían.
Lógicamente, se debe normar de manera más específica, para que muchos de estos casos queden completamente fuera del ámbito penal, y sean tratados en vía civil o administrativa, según la naturaleza de cada proceso, y se queden bajo la protección penal únicamente los casos que por su trascendencia e impacto social, lo ameriten.

6. LIBERTAD DE EXPRESIÓN. -

Uno de los pilares del sistema constitucional de derechos es la libertad de expresión, amparada en el caso ecuatoriano en la Constitución de la República en los artículos 66, numeral 6 y 384 y bajo la protección de las leyes en particular de la Ley Orgánica de Comunicación. La materialización de la

[36] **Aguirre, Eduardo Luis y Osio, Alejandro Javier. 2015.** Código penal comentado de acceso libre - Calumnias e Injurias. [En línea] 2015. http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37678.pdf, pag. 9
[37] **Asamblea Nacional de la República del Ecuador . 2014.** *Código Orgánico Integral Penal.* Quito : Registro Oficial, 2014

libertad de expresión permite a los ciudadanos exponer de forma abierta, sólida y sin miedo, dentro del marco del respeto a los derechos, sus criterios, opiniones e información.

La libertad de expresión, al igual que el resto de los derechos y libertades, no es absoluta encontrando sus límites en el andamiaje jurídico y por la relación para con otros derechos. Es decir que, la libertad de expresión se encuentra limitada por ciertos derechos fundamentales que regulan su accionar, como pueden ser el honor, la intimidad y la dignidad de las personas. Todo ello se traduce en límites prácticos para el ejercicio de la libertad de expresión.

Así mismo, la veracidad juega un rol fundamental para comprender el marco de acción de la libertad de expresión. Por ejemplo, para un supuesto de difusión de contenidos de interés público general, la información difundida debe satisfacer dos elementos: el de relevancia pública y el de interés social. Sin embargo, y aun cuando satisfaga los dos elementos antes mencionados la información debe entenderse como veraz, sin afectar la seguridad, el honor, ni el bienestar general.

En la práctica, y, aun argumentando la veracidad de cierta información y el posible interés público general de la misma, su difusión y comunicación, para encontrarse al amparo de la legalidad, debe estar desprovista de expresiones vulgares, desagradables, injuriosas o vejatorias dado que ellas resultan innecesarias para transmitir una idea o un juicio de valor y por otro lado afectan derechos personalísimos como el honor, prestigio, etc., de quienes estuvieren implicados en el contenido.
No hay menor duda que esta temática refleja complejidad puesto que como dice la autora Concepción Carmona, no tiene fácil ni unánime solución doctrinal ni jurisprudencial, pues nos encontramos frente a un bien jurídico de naturaleza eminentemente subjetiva, tan íntimamente conectado con la personalidad de cada cual, y, al propio tiempo, tan influenciado por los criterios valorativos culturales y sociales imperantes según el momento histórico, que resulta bastante complejo acuñar un concepto del mismo que satisfaga plenamente las diversas expectativas existentes al respecto. [38]

En principio, las conductas puramente expresivas serían el objeto de tutela y protección de los derechos fundamentales de expresión e imprenta. Esto quiere decir que, como regla general, las expresiones que emitamos estarían jurídicamente protegidas, cualquiera que sea su contenido y cualquiera que sea la forma de transmisión de las mismas[39].

Es necesario señalar que esta protección termina cuando se trata de expresiones incitatorias que, siendo expresiones, tienen efectos conductuales más o menos directos y pueden dar lugar ya no a la protección de las mismas, sino a la determinación de responsabilidades jurídicas para quienes las emitan, es decir si se está promoviendo el odio contra cierta persona e incita a la agresión a la misma, esa protección se ve totalmente disminuida.

Para el caso que la información excediese los lineamientos de una mera opinión para pasar a constituir el objeto inicial de, ya sea, una petición, una denuncia, una demanda, etc., el articulado del ordenamiento jurídico ecuatoriano establece con coherencia que es imprescindible realizar su encauce ante las autoridades competentes en la instancia y en la materia, de modo que, no sólo en aras de la economía legal y eficacia procesal, sino también para una mejor satisfacción del reclamo al momento de accionar los resortes institucionales.

---

[38] **Carmona Salgado, Concepción. 2012.** Corte Interamericana de Derechos Humanos . *Calumnias, Injurias y otros atentados al honor.*http://www.corteidh.or.cr/tablas/r31007.pdf, pag.1.
[39] **Carbonell, Miguel. 2011.** El fundamento de la libertad de expresión en la democracia constitucional. [aut. libro] María Paz Ávila Ordoñez, Ramiro Ávila Santamaría y Germano Gómez. [ed.] María Paz Ávila Ordoñez, Ramiro Avila Santamaría y Gustavo Gómez Germano. *Libertad de Expresión: debates, alcances y nueva agenda.* Quito : Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 2011, pag. 95.

El panorama en la actualidad se encuentra aún más difuso por la forma en que se genera y transmite la información principalmente en las redes sociales, ya que su efecto viral puede lograr consecuencias en pocos minutos, que superan a las que se generan por los medios de comunicación tradicionales.

El derecho penal se encuentra transitando por una de sus etapas más difíciles, no sólo por los evidentes problemas que enfrenta para "legitimar" su misión dentro del conglomerado social, como también porque hoy más que nunca se tiene conciencia de que no se le puede confiar al derecho penal la función de resolver problemas sociales, no sólo porque es la peor vía para hacerlo, sino por la multiplicidad de efectos simbólicos que implica.[40]

Es necesario señalar que los diferentes tribunales nacionales e internacionales, han tratado la libertad de expresión en diferentes controversias las cuales pasaremos a describirlas:
El Tribunal Constitucional Español 9/2007, de 15 de enero, mediante sentencia señaló dentro de la acción de amparo, que la libertad de expresión se revela como necesaria para expresar ideas u opiniones de interés púbico, en la medida de que no sean injuriosas, vejatorias ni que contengan insultos [41]. Es decir, alinea su criterio a la doctrina antes señalada, definiendo claramente que el límite principal de la libertad de expresión es el respeto al derecho al honor. [42]

De igual manera la Sentencia 047-15-SIN-CC de la Corte Constitucional del Ecuador, ratifica en su análisis que el único límite para el goce efectivo del derecho a la libertad de expresión es el respeto a los derechos o a la reputación de los demás, con ello afirma que la libertad de expresión tiene su límite en la responsabilidad por las declaraciones o expresión que afecten negativamente la reputación o la honra de las personas. Para resumirlo lo reseñado precedentemente es de destacar que la libertad de expresión no es absoluta, y que debe armonizarse con la exigencia de otros derechos.[43]
En la esfera penal internacional es necesario señalar algunos fallos emitidos por la Corte Interamericana de Derechos Humanos los cuales evidencian que el criterio de este Organismo de Justicia radica en la despenalización de esta clase de conductas, según lo desarrollado por el tratadista Rodríguez. [44]

En el caso Herrera Ulloa vs. Costa Rica, la corte determina el impacto negativo de una sentencia condenatoria sobre la libertad de expresión. La imposición de sanciones penales, como consecuencia de determinadas expresiones, funciona como un método indirecto de restricción a la libertad de expresión. Los Estados deben abstenerse de censurar la información relacionada con actos de interés público, ejecutados por funcionarios públicos o por particulares involucrados voluntariamente en asuntos públicos, quienes deben reflejar mayor tolerancia a las críticas.

Por su parte en el caso Ricardo Canese vs. Paraguay la Corte antes señalada consideró que la sentencia condenatoria en materia penal es una violación de la Convención americana. Y la Comisión informó sobre la inexistencia de una alternativa menos lesiva para la libertad de expresión (como la responsabilidad civil) en el ordenamiento jurídico paraguayo

---

[40] **Chirino Sánchez, Alfredo. 2011.** Libertad de Expresión y Ley Penal. [aut. libro] María Paz Ávila Ordoñez, Ramiro Ávila Santamaría y Gómez Gustavo. *Libertad de Expresión: debates, alcances y nueva agenda.* Quito : Organización de las Naciones Unidas , 2011, 137.

[42] **Tribunal Constitucional de España. 2007.** *Sentencia 9/2007.* [En línea] 15 de enero de 2007. http://hj.tribunalconstitucional.es/pt/Resolucion/Show/5976.
[43] **Corte Constitucional del Ecuador. 2015.** *Sentencia 047-15-SIN-CC.* [En línea] 23 de septiembre de 2015. https://www.corteconstitucional.gob.ec/sentencias/relatoria/relatoria/fichas/047-15-SIN-CC.pdf.
[44] **Rodriguez Moreno, Felipe,** *Manual de delitos contra el Honor y Libertad e Expresión, op. Cit., ps. 177-196*

En efecto, la Comisión asimila en este caso la autocensura a la censura previa, al producir los mismos efectos: no permitir que las expresiones circulen. Como se puede ver, los órganos del sistema interamericano coinciden en reprobar los efectos de una sentencia penal condenatoria causada por la emisión de una opinión, ya que dichos efectos no solo recaen sobre el condenado, sino que menoscaban la posibilidad de que otros miembros de la sociedad tengan acceso a dichas opiniones o informaciones.

En Ecuador, el Derecho penal ha sido y continúa siendo aplicado con demasiada frecuencia y absoluta falta de proporción para sancionar a quienes ejercen su derecho a manifestar[45], a lo largo del gobierno de Rafael Correa, existieron varios procesos legales en contra de ciudadanos que por medio de las redes sociales emitían sus críticas al gobierno; no podemos negar que muchas de ellas, utilizaban frases extremadamente agresivas y que indudablemente ameritaban la acción de la justicia, pero la gran mayoría eran expresiones que no eran plausibles de ninguna clase de sanción.
Lo aseverado evidencia la poca tolerancia que tenía el ex mandatario para sus críticos; incluso en sus muy conocidas sabatinas, daba a conocer los datos personales de su detractores, con la finalidad de que sus simpatizantes arremetieran contra ellos. Estos casos ya fueron detallados en un anterior artículo para el Congreso de la FIADI de Salamanca – España.

7. ENCAUSE SOCIAL DE LAS CALUMNIAS E INJURIAS. -

De acuerdo al maestro Luigi Ferrajoli, en su obra derecho y razón; el fin general del derecho penal es la protección del débil contra el más fuerte: del débil ofendido o amenazado por el delito, así como del débil ofendido o amenazado por la venganza; contra el más fuerte, que en el delito es el delincuente y en la venganza es la parte ofendida.[46]

En efecto, los órganos judiciales deben buscar un equilibrio legal y procesal en búsqueda de la justicia, para lograr una homeostasis social, que permita el cumplimiento del fin del derecho penal, el cual debe estar desprovisto absolutamente de injerencias políticas.
En el caso que nos atañe; el entendimiento del bien jurídico honor es un tanto complicado, puesto que está condicionado a realidades históricas, geográficas y sociales; la sociedad latinoamericana actual no es la misma que la de años noventa, es que el camino que nos marcó las nuevas tecnologías es aún incierto. Resulta difícil saber cómo reaccionar ante ciertos delitos informáticos por todos los matices que presenta su encause.

Realmente, los tipos penales injurias y calumnias, en la actual sociedad de la información resultan muy complicados de aplicarlos, y más aún si se la acción delictiva se la efectúa por medio de redes sociales, puesto que su tipicidad obedece a otra realidad, donde los sistemas de información tenían otro impacto en la ciudadanía, y la mayoría de casos se daban por publicaciones en diarios escritos, radio y televisión y cartas.

Hoy en día el medio más efectivo para efectuar es simplemente una publicación en redes sociales con un perfil verdadero o un anónimo, este entorno digital como ya se señaló anteriormente es el sitio adecuado para causar reacciones, puesto que la gran mayoría de usuarios interactúan inmediatamente y las notificaciones propias de las redes sociales tienen a que estos contenidos se difundan inmediatamente.

---

[45] **Salazar Marín, Daniela. 2012.** *La criminalización de la protesta como restricción de la libertad e expresión en el Ecuador*. [aut. libro] Ramiro Ávila Santamaría. *Protesta Social, libertad de expresión y derecho penal.* Quito : Corporación Editora Nacional, 2012, pag. 77.
[46] ***Ferrajoli, Luigi,*** *Derecho y Razón, Teoría del Garantismo Penal, op. cit., pag. 335.*

Lo señalado evidencia, que los actuales avances tecnológicos y el espacio virtual, que son parte de nuestra vida, nos hayan conducido a una sociedad de riesgo. Esta revolución desarrollada en las últimas décadas, incluso potencian las posibles intromisiones en nuestra vida privada e intimidad.
Sin embargo de lo expuesto, se requiere de mucha prudencia al momento de definir nuevos tipos penales, ya que no toda acción antijurídica requiere del derecho penal, como vía de justicia.
En los códigos penales actuales como en el caso ecuatoriano, se han definido una cantidad de tipos penales nuevos muchos de ellos que no ameritan ser considerados como delitos, puesto que podrían tener un efectivo tratamiento por vía civil o administrativa; y unos tantos que no tienen sentido su tipificación en el ordenamiento jurídico nacional.

De acuerdo a Ferrajoli un programa de derecho penal mínimo debe apuntar a una masiva deflación de los bienes penales y de las prohibiciones legales, como condición de su legitimidad política y jurídica; en consecuencia, la creación de nuevos tipos penales indudablemente atenta directamente al principio de mínima intervención.[47]

En efecto, el bien jurídico honor ameritaría protección penal en casos extremos, es decir cuando el caso en particular sea incontenible por otra vía procesal y su ataque traiga consigo una conmoción en un determinado conglomerado. Lógicamente lo señalado debe ser analizado conjuntamente con la realidad social e histórica dentro de la cual se efectúa la conducta.

8. PROBLEMÁTICA GENERADA RESPECTO AL PRINCIPIO DE MÍNIMA INTERVENCIÓN. -

Realmente, es un problema muy serio el ¿cómo superar la problemática respecto al principio de mínima intervención penal en la libertad de expresión ejercida por medio de las redes sociales?, realmente la única solución posible es la inmediata adopción de medidas alternativas que aseguren un ejercicio adecuado del reproche frente a eventuales abusos de esta libertad.
Efectivamente, se deben ir generando normativa tanto en sede administrativa como en la esfera civil, que nos permitan ejercer acciones efectivas que a este respecto ameriten sanción; puesto que si no existe sanciones adecuadas nos ubicaríamos en el otro extremo de la problemática, esto es la impunidad;

El problema se agudiza aún más cuando el abuso de la libertad de expresión, afecta a un determinado conglomerado social, como por ejemplo, si una persona señala públicamente que una entidad bancaria está quebrada y que cerrará sus puertas, o que enfáticamente asevere que una universidad será intervenida por la mala calidad de la educación y pésima administración de sus autoridades.
En los ejemplos antes señalados si bien estos ataques se podrían dirigir ya sea para el gerente del banco o al rector de la universidad, tienen una repercusión inmediata en los clientes y en los estudiantes, respectivamente, lo que daría como resultado una crisis interna dentro de las instituciones ejemplificadas.

Más aún si los comentarios son continuos y evidenciando información falsa o no relacionada al tema, generando aún más confusión; indudablemente que es necesario activar el poder punitivo del Estado, puesto que estos ataques al honor y al prestigio de ciertos directivos, tienen considerables efectos colectivos que pueden llevar al generan caos social.
Un porcentaje considerable de la sociedad ecuatoriana no tiene una cultura respecto del manejo de las redes sociales, y de las consecuencias en todos los ámbitos que una publicación, fruto de un momento de frustración, ira, odio, celos, pueden generar.

[47] ***Ferrajoli, Luigi,*** *Derecho y Razón, Teoría del Garantismo Penal, op. cit., pag. 477.*

De lo expuesto, se colige que se debe promover un estímulo estatal a una cultura de la autorregulación en Internet que permitiría, con más eficacia y también con más legitimidad, controlar los ejercicios abusivos de la libertad de expresión en las redes sociales. Esto no solo permitiría desarrollar las obligaciones positivas de la Convención americana en la materia, sino que evitaría intromisiones desproporcionadas del Estado en la órbita de las libertades de sus habitantes.[48]

9. PRINCIPALES OBSTACULOS PROCESALES AL MOMENTO DE TRAMITAR CAUSAS. -

Las redes sociales, por el libre acceso y la difusión masiva que supone su ubicación en el medio *on line*, constituyen un entorno idóneo para la comisión de varios delitos, en especial, por la facilidad de perpetración a distancia y frecuente sensación de impunidad ligado a inicial – y a veces permanente- anonimato. A todo ello se añaden, en no pocas ocasiones, serias dificultades para su investigación, por las limitaciones tecnológicas que supone la posibilidad de ocultar o borrar rastros en la red.[49]
En muchos casos en nuestro país hemos visto con mucha preocupación que varias causas han sido admitidas a trámite sin contar con una prueba técnica que pueda dar elementos de convicción al operador de justicia. La prueba debidamente solicitada, practicada e incorporada sin duda alguna producirá certeza al juzgador respecto a que si la conducta analizada es o no plausible de sanción.
Es necesario tener certeza en el hecho de que los testimonios no pueden reemplazar a una prueba pericial, varios casos por calumnias e injurias se han accionado, con una supuesta captura de pantalla del perfil de una red social de un ciudadano y tres testigos que dicen haber visto esa publicación. Realmente un testigo puede relatar hechos que pudo percibir por medio de sus sentidos, pero resulta un poco complicado que recuerde con precisión el contenido exacto de la publicación atacada, ya que inclusive los signos de puntuación revisten importancia en el análisis del sentido de la frase.

A lo señalado, resulta un tanto complejo llevar a plenitud el ejercicio del reconocimiento del lugar de los hechos en territorio digital, servicios digitales, equipos o medios tecnológicos, según lo expresado en el Código Orgánico Integral Penal en sus artículos 460.8 y 500, ya que en el caso de las redes sociales, se puede iniciar sesión desde una gama considerable de dispositivos, y su entorno es dinámico; y casi nunca se podrá contar con el terminal desde el cual se cometió la conducta antijurídica, lo más recomendable en estos casos es descargar mediante una pericia el contenido de la página, con la finalidad de que la prueba se conserve y pueda ser complementada con otros estudios periciales como reconocimientos faciales, de voz, transcripción de los audios y videos y descripción del entorno.
Indudablemente cada persona y grupos sociales han creado conceptos respecto de la libertad de expresión, a tal punto que en ciertos casos el anonimato ha disminuido, por cuanto las personas necesitan ser reconocidas, y plenamente identificables como opositores a determinado régimen universitario, local, provincial o nacional. Cada vez es más común el subir publicaciones a la red Facebook por ejemplo, y después de unas horas borrarla o cambiarle su estado de público a privado, circunstancia que complica el estudio técnico ya que el requerimiento para efectuar un peritaje toma varios días.

Estos grupos de personas tienen el convencimiento que desde sus redes sociales pueden generar cambios sustanciales en la sociedad, que en ciertos casos han llegado a extremos generando confusión y caos en ciertas instituciones. En la ciudad de Ambato por ejemplo una ciudadana empezó a desprestigiar a la Universidad en la que estudia, y atentar gravemente contra el honor no solo de la casa de estudios sino de sus autoridades, con videos frecuentes viralizados en diferentes redes sociales

[48] **Upegui Mejia, Juan Carlos. 2018.** Sistema de Información Científica Redalyc. [En línea] 15 de julio de 2018. http://www.redalyc.org/html/3376/337630235006/, pag. 180.
[49] **Alonso García , Javier. 2015.** *Derecho Penal y Redes Sociales.* Pamplona : Aranzandi, SA, 2015

principalmente Facebook y WhatsApp , que varios estudiantes dudaron de la calidad académica y muchos de ellos busco cambiarse de universidad, otros decididos a defender su casa de estudios, contrastando la información que emitía y emitir comunicados por las mismas redes, otros se dedicaron hacer memes de la situación.

La estudiante luego de un proceso administrativo fue suspendida temporalmente de su actividades académicas, acudió en sede administrativa, vía recurso de apelación al Consejo de Educación Superior CES, y en sede jurisdiccional, aduciendo principalmente violación a la libertad de expresión, cláusula de conciencia, derecho a la educación, en esta última esfera el juez constitucional a quo, determinó mediante sentencia que no existía violación a derecho constitucional alguno, resaltando el hecho de que se contaba con prueba pericial, documental y testimonial que justificaban la actuación del ente administrativo que emitió la sanción, en la actualidad dicho fallo está apelado, y hasta la entrega de este trabajo no existe resolución del CES ni del tribunal de apelación.

10. CONCLUSIONES. -

- Nos encontramos frente a una encrucijada; por un lado, el principio de mínima intervención penal y por otro lado sentimos como ciertos delitos cometidos abiertamente por las redes sociales quedan en la impunidad.

- Se debe promover un estímulo estatal a una cultura de la autorregulación en Internet que permita, con más eficacia y también con más legitimidad, controlar los ejercicios abusivos de la libertad de expresión en las redes sociales. Evitando con esto intromisiones desproporcionadas del Estado en la órbita de las libertades de sus habitantes.

- Se ha evidenciado la necesidad de un derecho penal que evada el populismo punitivo, y que funcione bajo el principio de mínima intervención penal, haciendo uso de las penas privativas de libertad como *ultima ratio*, procurando utilizar mecanismos extrapenales para tratar esta clase de conductas.

- Definitivamente, es de suma importancia que el bien jurídico honor, por su naturaleza, se encuentre bajo protección penal en la legislación ecuatoriana, y se lo procese en casos excepcionales, claramente definidos, mientras no se cuenta con una vía procesal expedita para hacer valer esta clase de derechos de forma eficiente y eficaz.

- La excepción antes señalada, se basa en que se debe activar el poder punitivo del Estado a este respecto, cuando los comentarios y publicaciones contengan expresiones evidentemente vulgares, agresivas, injuriosas o vejatorias, conjunta o separadamente es necesario considerar cuando las agresiones sean continuas en el tiempo, afecten el bien jurídico tutelado y ocasionen conmoción en un determinado conglomerado.

- Cada caso debe ser analizado individualmente, y en base a pruebas técnicas debidamente practicadas, analizar si la conducta es o no plausible de sanción por la vía penal.

- Para que proceda la calumnia es necesario que se tenga plena certeza que concurrió claramente su elemento subjetivo, esto es el conocimiento de la falsedad, ya que es considerada un delito doloso y no culposo, en consecuencia, el calumniador es consciente de que su imputación es falsa contra un tercero.

- En el delito de injurias las expresiones referidas a asuntos de interés público de acuerdo a su contexto, podrían no ser plausibles de sanción penal, para lo cual el administrador de justicia debe valerse de todos los medios probatorios para determinar el particular, teniendo en consideración la posible transgresión de derechos fundamentales.

- Los diferentes delitos perpetrados por redes sociales requieren una revisión adecuada por el legislador, puesto que la mayoría de ellos obedece a una realidad histórica y social diferente, y se debe tipificar claramente conductas y procedimientos para que el juzgador tenga claro los parámetros técnicos y legales que se deben tratar para sustanciar una causa de esta naturaleza.

- Lo señalado anteriormente ahonda más su esfera subjetiva, ya que dependerá del administrador de justicia determinar si el asunto es de interés público, sin dejar de lado el contenido de los comentarios; por cuanto si se utiliza términos agresivos y falsos, que ponen en evidente riesgo el desarrollo de las actividades permanentes de la persona atacada, si causa conmoción en un determinado conglomerado, o pone en riesgo la prestación de un servicio público, se debe activar el poder punitivo del Estado; sin perjuicio del resto de acciones legales a las que hubiere lugar.

- Se deberían proponer políticas de Estado direccionadas a mejorar las relaciones internacionales, puesto que en el caso de transnacionalidad del delito, las políticas exteriores juegan un papel fundamental para que el delito no quede en la impunidad.

- En el Ecuador se debe brindar herramientas técnico- legales que permitan la conservación de publicaciones en redes sociales, de manera efectiva y oportuna, puesto que esta información es altamente volátil y si desaparece resultaría casi imposible la administración de justicia, puesto que no se contaría con elementos suficientes que evidencien un procedimiento que respete las garantías establecidas para el efecto.

11. BIBLIOGRAFÍA. -

Aguirre, Eduardo Luis y Osio, Alejandro Javier. 2015. Código penal comentado de acceso libre - Calumnias e Injurias. [En línea] 2015. http://www.pensamientopenal.com.ar/system/files/cpcomentado/cpc37678.pdf.

Alonso García , Javier. 2015. *Derecho Penal y Redes Sociales.* Pamplona : Aranzandi, SA, 2015.

Asamblea Nacional de la República del Ecuador . 2014. *Código Orgánico Integral Penal.* Quito : Registro Oficial, 2014.

Barbini, Alejandro. 2015. *Correo electrónico, redes sociales y proveedores de Internet en el proceso penal.* Buenos Aires : La Rocca, 2015. 978-987-517-147-3.

Berdugo de la Torre, Ignacio. 1985. *Revisión del Contenido bien jurídico honor, en homenaje a Hilde Kaufmann.* Buenos Aires : De Palma, 1985.

Bueno de Mata, Federico. 2014. *Prueba Electrónica y Proceso 2.0.* Valencia : Tirant lo Blanch, 2014.

Cabezuelo Arenas, Ana Laura. 1998. *Derecho a la Intimidad.* Valencia : Tirant lo Blanch, 1998.
Carbonell, Miguel. 2011. El fundamento de la libertad de expresión en la democracia constitucional. [aut. libro] María Paz Ávila Ordoñez, Ramiro Ávila Santamaría y Germano Gómez. [ed.] María Paz Ávila Ordoñez, Ramiro Avila Santamaría y Gustavo Gómez Germano. *Libertad de Expresión: debates, alcances y nueva agenda.* Quito : Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 2011.
Carmona Salgado, Concepción. 2012. Corte Interamericana de Derechos Humanos . *Calumnias, Injurias y otros atentados al honor.* [En línea] 2012. [Citado el: 2018 de julio de 04 .] http://www.corteidh.or.cr/tablas/r31007.pdf.
Chirino Sánchez, Alfredo. 2011. Libertad de Expresión y Ley Penal. [aut. libro] María Paz Ávila Ordoñez, Ramiro Ávila Santamaría y Gómez Gustavo. *Libertad de Expresión: debates, alcances y nueva agenda.* Quito : Organización de las Naciones Unidas , 2011.
Corte Constitucional del Ecuador. 2015. Corte Constitucional del Ecuador. *Sentencia 047-15-SIN-CC.* [En línea] 23 de septiembre de 2015. [Citado el: 2018 de julio de 04.] https://www.corteconstitucional.gob.ec/sentencias/relatoria/relatoria/fichas/047-15-SIN-CC.pdf.
De Cupis, Adriano. 1982. *Derecho a la Personalidad.* Milán : Guifré, 1982.
Fernández Delpech, Horacio. 2001. *Internet: Su problemática jurídica* . Buenos Aires : Abeledo Perrot, 2001.
Ferrajoli, Luigi. 1995. *Derecho y Razón, Teoría del Garantismo Penal.* [trad.] Perfecto Andres Ibañez, y otros. Madrid : Editorial Trotta, 1995.
Gallego Trijueque, Sara. 2011. Sistema de Información Científica Redalyc. *Redes Sociales y Desarrollo Humano.* [En línea] 15 de Septiembre de 2011. [Citado el: 4 de Julio de 2018.] http://www.redalyc.org/pdf/3221/322127622007.pdf.
García Falconí, Ramiro. 2014. *Código Orgánico Integral Penal Comentado.* Segunda. Quito : Latitud Cero Editores, 2014.
Gozaini, Osvaldo. 2004. *Derecho Procesal Constitucional. El debido proceso* . Buenos Aires : Rubinzal-Culzoni, 2004.
Guilayn, Albert. 2016. *Aspectos Legales de las Redes Sociales.* Barcelona : Bosh, 2016. 978-84-9090-105-2.
Huerta, Guerrero Luis Alberto. 2002. *libertad de expresión y acceso a la información pública.* Lima - Peru : Comisión Andina de Juristas , 2002.
Lombana Villalba, Jaime. 2009. *Injuria, Calumnia y Medios de Comunicación.* Medellín : Biblioteca Jurídica Diké, 2009. 978-958-8075-86.
Mir Puig, Santiago. 2016. *Derecho Penal Parte General.* [ed.] Julio César Faira. Barcelona : Bdef, 2016.
Muñoz Conde, Francisco. 1999. *Derecho Penal Parte Especial.* Valencia : Tirant lo Blanch, 1999.

Nieto Martín, Adán y Maroto, Manuel. 2013. Las redes sociales en Internet como instrumento de control penal: Tendencias y límites. [aut. libro] Artemi Rallo Lombarte y Ricard Martínez. *Derecho y Redes Sociales.* Pamplona : Arazandi S.A., 2013.
Ortega Vintimilla, Máximo. 2018. *Las Calumnias y las expresiones en descrédito o deshonra perpetradas por medios digitales: Facebook, Whats App y más.* Quito : Editorial Jurídica del Ecuador, 2018. 978-9978-17-480-7.
Rodriguez Moreno, Felipe. 2017. *Manual de delitos contra el Honor y Libertad e Expresión.* Quito : Cevallos, 2017.
Salazar Marín, Daniela. 2012. La criminalización de la protesta como restricción de la libertad e expresión en el Ecuador. [aut. libro] Ramiro Ávila Santamaría. *Protesta Social, libertad de expresión y derecho penal.* Quito : Corporación Editora Nacional, 2012.
Tribunal Constitucional de España. 2007. Tribunal Constitucional de España. *Sentencia 9/2007.* [En línea] 15 de enero de 2007. [Citado el: 2018 de julio de 04.] http://hj.tribunalconstitucional.es/pt/Resolucion/Show/5976.
Upegui Mejia, Juan Carlos. 2018. Sistema de Información Científica Redalyc. [En línea] 15 de julio de 2018. http://www.redalyc.org/html/3376/337630235006/.
Zaffaroni, Eugenio Raúl . 2007. *Manual de Derecho Penal. Parte General* . Buenos Aires : Ediar, 2007.

EL CONSENTIMIENTO EN LAS RELACIONES CONTRACTUALES

PERSONA – MÁQUINA

Por: María Camila Rodríguez Lozada

Durante años juristas y doctrinantes han coincidido al definir el contrato como un acuerdo de dos o más personas que conlleva al surgimiento de obligaciones y como consecuencia, efectos jurídicos, el cual, ha sido regulado en Colombia por el Código Civil (Ley 57 de 1887), que expresamente señala en su artículo 1502 unos requisitos necesarios para llegar a obligarse en una relación contractual, como lo son: 1) capacidad legal, 2) ausencia de vicios en el consentimiento, 3) que recaiga sobre un objeto lícito, y finalmente 4) La existencia de una causa lícita.

Dichas exigencias fueron adoptadas por nuestro ordenamiento jurídico de la teoría general de los contratos, sin embargo, debe tenerse en cuenta que el derecho se caracteriza por ser dinámico y cambiante, muchos de los conflictos que en la actualidad son eje de discusión ni siquiera fueron previstos por el legislador, por lo cual resulta necesario contextualizar el desarrollo contractual a los factores económicos y sociales, protagonistas en la nueva era tecnológica.

El avance que ha tenido la tecnología durante los últimos veinte años ha permitido innovadoras técnicas contractuales, las cuales eran inimaginables para el legislador decimonónico, pero que hoy día no son solo tema de discusión y debate, sino también de regulación jurídica, ya que en el nuevo escenario de contratación son necesarios replanteamientos respecto de cuestiones clásicas entre los iusprivatistas.

Un claro ejemplo de ellos fue Pothier, quien desarrolló en su "Tratado de las obligaciones", aquellos elementos que pertenecen a la esencia de las obligaciones, como lo son:

1. "Que hay una causa de la cual nace la obligación.
2. Personas entre las cuales ésta se contrata.
3. Alguna cosa que sea el objeto.

Además, asegura que los contratos son la causa principal de las obligaciones y propone hacer un estudio integral de este teniendo en cuenta los siguientes aspectos:

- Definición del contrato.
- Las diferentes cosas que son necesarias de distinguir en cada contrato.
- Las diferentes divisiones de los contratos.
- Los vicios que podemos encontrar en el contrato.
- La capacidad de las personas que pueden contratar.
- El objeto del contrato.
- Los efectos del contrato.
- Las reglas para la interpretación de los contratos." (González, Ferreyros & Carrascosa (2004) "Los contratos en la sociedad de la información, formularios de contratos informáticos e internet" pág. 27. Granada: Comares)

Esta categorización del derecho de los contratos, como se ve, no es una invención del Código Civil, ella fue establecida antes de la codificación y utilizada después sin mayores

cambios, por lo que podría pensarse que dicha estructura corresponde a un enfoque cognitivo del derecho, que ha sido admitida por la mayoría de los juristas.

Sin embargo, dichos planteamientos se quedan cortos en la actualidad en la cual se desarrolla el mundo de las obligaciones, y es de entenderse, pues fue solo a principios de los años veinte en los Estados Unidos, cuando apareció la venta por catálogo, que se empezaron a vislumbrar pequeñas luces de relaciones contractuales inmersas en la era tecnológica.

De hecho, aún en la actualidad, cuando día a día podemos encontrar multiplicidad de innovadores cambios tecnológicos, resulta muy complejo vislumbrar los aportes conceptuales, dogmáticos, jurisprudenciales, doctrinales y legales que se han realizado de los contratos en la sociedad de la información y la ciencia,

Lo anterior debido a que, considerar la existencia de una relación contractual entre individuos y máquinas o simplemente máquinas, resultaba absurdo hace muy poco tiempo atrás; situación que pone en absoluto riesgo los numerales 1 (uno) y 2 (dos) de la tesis adoptada por el Código Civil en su artículo 1502, es decir aquellos que se refieren a su capacidad legal y al consentimiento libre de vicios

En otro escenario, donde la interacción es entre un individuo y una máquina, o entre dos máquinas resulta aún más ilógico contemplar el concepto de consentimiento adoptado por el código, esto en sentido estricto, sin embargo, existen diferentes autores que se han atrevido a plantear teorías de las cuales vale la pena ahondar, pues como ya se mencionaba, en caso de carecer un contrato de consentimiento por alguna de sus partes este puede perder su objetivo.

Frente a la problemática anteriormente planteada los juristas han optado por iniciar el desarrollo y la solución de esta conceptualizando, caracterizando cada uno de los contratos que pueden llegar a nacer en la vida jurídica en el medio electrónico y de la tecnología; sin embargo, este es un tema muy extenso que no nos atañe, pues el punto vértice del presente artículo es la afectación del consentimiento en las relaciones contractuales emergentes en la nueva era tecnológica.

Es por lo anterior, que ha surgido la siguiente pregunta: ¿Cómo se ha afectado el consentimiento como requisito para obligarse, en las relaciones jurídicas contractuales entre personas y máquinas; en el marco de la era de la tecnología y la sociedad de la información?, cuestionamiento que requiere unos conceptos básicos que permitan desarrollar todo un acápite de aportes al tema en cuestión.

El primero de ellos es la expresión "tecnologías de la información" de la cual se dice en el comunicado del 14 de septiembre de 2001 por parte de la Comisión, el Consejo y el Parlamento Europeo: *"las TIC son un término que se utiliza actualmente para hacer referencia a una gama amplia de servicios, aplicaciones y tecnologías, que utilizan diversos tipos de equipos y de programas informáticos, y que a menudo se transmiten a través de las redes de telecomunicaciones*".

Por otro lado, la definición de "servicios de la sociedad de la información" que está plasmada en la Directiva 98/34/CE del Parlamento Europeo y del Consejo, del 22 de junio de 2008, donde se caracteriza como "todo servicio prestado normalmente a cambio de una

remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios".

Aceptaciones teóricas y legales respecto de las cuales el sistema jurídico colombiano no se ha pronunciado, dejando un vacío enorme en las exigencias formales y la seguridad jurídica en torno a la formación del contrato, lo cual hace que este adolezca de diversas debilidades y riesgos que no se puede permitir el derecho en la nueva era de la tecnología.

La realidad jurídica en la cual está inmerso el ordenamiento colombiano ha evidenciado que la figura clásica del contrato en el derecho comercial es ya bastante obsoleta y lejana de las necesidades del Siglo XXI, donde la sociedad de la información y la era tecnológica son protagonistas y promotores de nuevas relaciones contractuales.

La relevancia de este tema radica en que es el contrato la principal fuente de obligaciones, ya que en su concepto acoge dos ideas fundamentales como lo son la voluntad y la relación jurídica obligatoria, la cual seguidamente provoca unos efectos jurídicos, eso sí, si en su desarrollo se han cumplido con unos requisitos, dentro los cuales está la capacidad y el consentimiento.

Es decir, que teniendo en cuenta la teoría clásica, si una relación jurídica adolece de consentimiento sería absurdo denominarla "contrato", por lo tanto, la obligación y la responsabilidad civil que este vínculo genera permanecería ausente; situación que resulta absolutamente perjudicial para una o ambas partes.

Por lo que resulta evidente que estos planteamientos, aceptados hace ya décadas no pudieron prever lo que en la actualidad ocurre, y es que el contrato no siempre es llevado a cabo por dos personas o individuos, es decir que ahora contratamos sin siquiera darnos cuenta con máquinas o en un medio electrónico del cual desconocemos una de sus partes.

Es decir que el sector tecnológico requiere de un tipo de contratos, con características técnicas y jurídicas específicas, con una regulación legal que permita hacer exigible lo pactado, ya que su demanda ha aumentado considerablemente con el auge de la tecnología donde personas naturales y jurídicas buscan establecer relaciones con otras, que resultan difíciles de entender desconociendo el derecho del comercio electrónico y la sociedad de la información.

Para entender esta problemática de manera integral es necesario desarrollar 4 puntos básicos, como lo son la contextualización del contrato de compraventa, su relación con el consentimiento y la autonomía privada de la voluntad, la contextualización de las máquinas dispensadoras, el marco legal que se ha desarrollado respecto del tema y finalmente las teorías que se han planteado y pueden adaptarse al mismo.

1. CONTEXTUALIZACIÓN DEL CONTRATO

Actualmente el contrato es entendido como un acuerdo de voluntades destinado a crear, regular o extinguir obligaciones, un concepto, que a diferencia de lo que se cree, no fue concebido en el Derecho Romano, más bien podríamos calificarlo como reciente, producto de una evolución del derecho Civil y Mercantil.

Marcelo Urbano, nos refiere que el vocablo aparece por primera vez en un texto de Labeon, jurista proculeyano de la época del emperador Augusto (s. I d.C.). Más tarde en el periodo clásico del Derecho Romano (s. II d. C), surgió la figura con su perfil de convención.

Cristóbal Alzate precisa que en el Derecho Romano clásico la palabra *contractus* designa genéricamente lo contraído. Significó aquella relación que da origen al vínculo jurídico, en sí "la obligación" de una y otra parte, que surgía del acuerdo de voluntades. (Alzate Hernández, 2009, pág. 36)

La cual estaba investida de unos rituales y formalidades indispensables para que dicho nexo generara una obligación real de hacer, contrario sensu ocurría con la *conventio*, sobre la cual Bonfante sostenía que el término contractus no significaba conventio, ya que más que aludir a un acuerdo, se refería al negocio o a la relación causal del vínculo jurídico, la cual se caracterizaba por carecer de fuerza vinculante. (Bonfante, 1929, pág. 300-400)

Pese a estas distinciones el Código Civil Colombiano en su artículo 1495 asimila el término contrato con el de convención, expresando taxativamente que contrato o convención es un acto por el cual una parte se obliga para con otra a dar, hacer o no hacer alguna cosa. Cada parte puede ser de una o de muchas personas.

Una definición que diferentes juristas califican como deficiente, por lo cual es necesario acudir a otras disposiciones del código, como lo son:

- Art. 1494. Las obligaciones nacen, ya del concurso real de las voluntades de dos o más personas, como en los contratos o convenciones.
- Art. 1496. El contrato es unilateral cuando una de las partes se obliga para con otra que no contrae obligación alguna; y bilateral, cuando las partes contratantes se obligan recíprocamente
- Art. 1502. Para que una persona se obligue a otra por un acto o declaración de voluntad es necesario: 1. Que sea legalmente capaz; 2. Que consienta en dicho acto o declaración y su consentimiento no adolezca de vicio; 3. Que recaiga sobre un objeto lícito; 4. Que tenga una causa lícita.

El Código de Comercio colombiano en su artículo 864 plantea que el contrato es un acuerdo de dos o más partes para constituir, regular o extinguir entre ellas una relación jurídica patrimonial, y salvo estipulación en contrario, se entenderá celebrado en el lugar de residencia del proponente y en el momento en que éste reciba la aceptación de la propuesta.

Se presumirá que el oferente ha recibido la aceptación cuando el destinatario pruebe la remisión de ella dentro de los términos fijados por los artículos 850 y 851

Un precepto no muy alejado es el planteado por el código napoleónico, el cual expone en su artículo 1101 "El contrato es una convención por la cual una o más personas se obligan, hacia otra o varias más, a dar, hacer o a no hacer alguna cosa", concepción acogida precisamente por Andrés Bello al redactar el Código Chileno en 1853.

Por otro lado, el Código Italiano en su artículo 1321, redefinió el contrato sobre la base del acuerdo de dos o más partes para construir, regular, o disolver entre ellas una relación jurídica patrimonial, haciendo énfasis en la noción de acuerdo y calificando su contenido patrimonial,

esta disposición normativa superó el concepto de la doctrina clásica francesa, al ampliar el objeto del contrato de mera creación de obligaciones hasta la regulación y extinción de estas.

El contrato en general es definido en forma abstracta por Urbano como una relación en donde intervienen como partes varias personas, quienes coinciden en una declaración de voluntad común sobre un objeto, lo cual da nacimiento a las obligaciones respectivas (Urbano, 2003, Pág. 11)

Es por esto que el contrato se ha convertido en un elemento indispensable para las relaciones personales, pues al tener múltiples funciones económicas y sociales permite el nacimiento de vínculos jurídicos donde las personas pueden intercambiar bienes y servicios bajo unos preceptos legales que invisten sus actos de legitimidad.

Ahora bien, es menester precisar que cualquier intento de conceptualizar la figura del contrato no puede desechar dos ideas fundamentales: el consentimiento y la relación jurídica obligatoria. Por lo que con total certeza podemos afirmar que es el contrato la principal fuente de las obligaciones.

Alberto Blanco indica que "El contrato es un acto jurídico bilateral para cuya existencia se requiere (…) la manifestación de voluntad de dos o más personas; las que, reconociendo distintas causas y tendientes a diferentes fines, han de coincidir necesariamente para formar el consentimiento (…) del que se ha de derivar los efectos obligatorios de la manifestación de voluntad: todo consentimiento en este sentido, resultará obligatorio, aunque no todo contrato reconocerá como base de su eficacia el mero consentimiento" (Blanco, 1948, pág. 174)

Entonces, entendemos el contrato como aquel acuerdo capaz de producir efectos jurídicos consistentes en crear, modificar o extinguir una relación jurídica obligatoria, desarrollada por lo que la definición de contratos acoge como partes, estas son los sujetos que expresan su voluntad y cuya unión de la misma invisten de validez el contrato, Alzate define la voluntad como el querer interno que manifestado bajo el consentimiento produce efectos en derecho. (Alzate, 2009, pág. 136)

Por otro lado, Bercovitz afirma "El primero de los requisitos esenciales del contrato es el consentimiento. El consentimiento es el acuerdo de voluntades de dos o más personas sobre el objeto y la causa del contrato. Para que un contrato exista, no hacen falta varios consentimientos (tantos como partes). Hay un único consentimiento, que es el fruto de la integración de las voluntades de las partes. Cada una de estas voluntades individuales adquiere rango de requisito esencial del contrato en tanto que conforma, junto a las demás voluntades, el consentimiento contractual." (Rodríguez Cano, 2011, pág. 536)

Concepto que está vinculado inevitablemente con la autonomía privada de la voluntad, en cuyo desarrollo conceptual han intervenido ilustres juristas, como Fernández Sessarego, quien la define como "el poder de autodeterminación de una persona para reglamentar y ordenar las relaciones jurídicas en las que es o ha de ser parte, esto justificado en la permisibilidad legal que regula el vínculo contractual". (Fernández Sessarego, 2000, pág. 218)

Para Cristóbal Alzate ésta se desarrolla en todas las actividades humanas relevantes para el derecho, ya sean comerciales, familiares, sucesorias, etc., y su contenido comprende:

CONTENIDO DE LA AUTONOMIA DE LA VOLUNTAD
Decidir si el contrato se celebra o no. Ninguna de las partes puede imponer unilateralmente a la otra el contenido de un contrato, sin que la otra lo acepte.
Elegir a su contraparte, la persona o personas con quien se desea contratar.
Definir la formación del contrato, los términos de la oferta. Quien recibe una oferta puede en su arbitrio aceptarla o rechazarla, o efectuar una contraoferta.
Escoger el contenido del contrato. Puede ser fijado como las partes lo decidan, con excepción de las leyes de carácter imperativo, las cuales no pueden ser derogadas por voluntad de los contratantes
Modificar las normas legales dispositivas o supletorias, que han sido establecidas especialmente para los contratos nominados.
Elegir el tipo contractual, acogiendo uno de los tipos regulados o concluir contratos con finalidades no previstas en la ley (atípicos), siempre que no se opongan al orden jurídico.
Acordar las modalidades de resolución de las controversias emergentes del contrato (amigable componedor, arbitramento, transacción, conciliación).
Modificar de común acuerdo los contratos celebrados o dejarlos sin efecto. La voluntad unilateral de una de las partes no puede alterar ni extinguir lo pactado.
Representación. Una parte puede actuar por sí misma, o por mandatario, mediante representación con poder general o especial.
La forma. Es obligatoria por mandato de la ley en casos taxativamente señalados. Las partes pueden decidir por ellas mismas que una formalidad sea obligatoria.

Alzate Hernández, Cristóbal (2009), "*Fundamentos del contrato, Segunda edición*", Ibáñez: Bogotá, D.C.

A su vez, ésta se ve manifestada por los principios generales de la contratación, como lo son:

- Libertad jurídica de contratar
- Consensualismo
- Fuerza obligatoria del contrato
- Efecto relativo del contrato
- Ejecución de buena fe
- Responsabilidad contractual

Esto quiere decir que, aunque la autonomía privada de la voluntad se trate de un actuar optativo, facultativo y autónomo, los sujetos que la ejecuten no podrán transgredir la ley, pues es esta la que brinda la legalidad necesaria para hacer exigible el contenido de la relación jurídica en cuestión.

La Constitución Política de Colombia en su artículo 333 acoge la autonomía de la voluntad, al consagrar: "La actividad económica y la iniciativa privada son libres, dentro de los límites del bien común. Para su ejercicio, nadie podrá exigir permisos previos ni requisitos, sin autorización de la ley.

La libre competencia económica es un derecho de todos que supone responsabilidades. La empresa, como base del desarrollo, tiene una función social que implica obligaciones. El Estado fortalecerá las organizaciones solidarias y estimulará el desarrollo empresarial.

El Estado, por mandato de la ley, impedirá que se obstruya o se restrinja la libertad económica y evitará o controlará cualquier abuso que personas o empresas hagan de su posición dominante en el mercado nacional. La ley delimitará el alcance de la libertad económica cuando así lo exijan el interés social, el ambiente y el patrimonio cultural de la nación."

Asimismo, la Corte Constitucional en sentencia C/060/2001 expone que la autonomía de la voluntad se configura cuando los propios sujetos deciden el destino de su vínculo, al precisar:

"Si algún significado ha de dársele al principio de autonomía de la voluntad, que estructura todo el régimen de contratación nacional (pública y privada), éste tiene que ver con la posibilidad de que sean los propios sujetos de la relación jurídica, quienes decidan el destino de su vínculo y obviamente, los procedimientos y autoridades que habrán de resolver los eventuales desacuerdos"

Por su parte, para Arrubla Paucar el término de "autonomía de la voluntad" es inexistente en la actualidad, al indicar una relevancia de la voluntad, como raíz, fuente y causa de efectos jurídicos del contrato, prefiere entonces referirse a "autonomía privada" la cual, define como el poder que confiere el sistema jurídico estatal a los particulares para crear normas jurídicas.

Lo anterior, justificando que la manifestación de la voluntad, ha dejado de ser el presupuesto fundamental del negocio jurídico, ya que, aunque esta pone en marcha el negocio, la cual es una fuente creadora de derecho objetivo, es la ley quien otorga y señala los efectos de tal manifestación. (Arrubla Paucar, 2008, pág. 55)

2. CONTEXTUALIZACIÓN DE LAS MÁQUINAS DISPENSADORAS.

El derecho poco acoge lo concerniente al tema de las máquinas, la mecánica y los nuevos dispositivos electrónicos que diariamente ingresan al mercado y son aceptados y usados por la gran mayoría de la población mundial, sin embargo, y aunque parezcan áreas inconexas, dichas expresiones tecnológicas han afectado drásticamente el ámbito legal, a tal punto que el legislador se ha visto en la obligación de crear nuevas normas que brinden una seguridad jurídica al consumidor.

Respecto al tema el Consejo de las Comunidades Europeas expresa en su Directiva 891392/CEE relativa a la aproximación de las legislaciones de los estados miembros sobre maquinas todo un acápite normativo que fija los requisitos esenciales de seguridad, salud y

desarrollo industrial que deben tener este tipo de artefactos al momento de su elaboración y ejecución.

Precisamente el artículo 2 de este Real Decreto cita: "se entenderá como «máquina» un conjunto de piezas u órganos unidos entre sí, de los cuales uno por lo menos habrá de ser móvil y, en su caso, de órganos de accionamiento, circuitos de mando y de potencia, u otros, asociados de forma solidaria para una aplicación determinada, en particular para la transformación, tratamiento, desplazamiento y acondicionamiento de un material.

También se considerará como máquina, un conjunto de máquinas que, para llegar a un mismo resultado estén dispuestas y accionadas para funcionar solidariamente.

Se considerará igualmente como «máquina» un equipo intercambiable que modifique la función de una máquina, que se ponga en el mercado con objeto de que el operador lo acople a una máquina, a una serie de máquinas diferentes o a un tractor, siempre que este equipo no sea una pieza de recambio o una herramienta."

Conceptos que a simple vista podrían tacharse como característicos de la nueva era tecnológica, sin embargo, la elaboración de máquinas es una de las actividades más antiguas realizadas por el hombre en su constante búsqueda de practicidad para día a día, un claro ejemplo de ello, son las máquinas dispensadoras, un dispositivo que se encarga de proporcionar diferentes productos al usuario sin que sea necesaria la interacción entre dos o más personas.

Este tipo de artefactos, aunque se estiman modernos, se remontan al año 215 a.C. cuando el ingeniero y matemático Helenístico Herón de Alejandría materializa una serie de inventos concebidos por él y su compañero y colega Ctesibio, en un libro titulado "Pneumatika", donde se desarrollaba una máquina totalmente automática que operaba a través de dracmas, las cuales permitían que fuera dispensada una cantidad mínima de agua de sacrificio; sin embargo no hay evidencia de una producción de dichos dispositivos a gran escala ni de una verdadera ejecución automatizada.

Alrededor de 1615 toman protagonismo en las tabernas inglesas las máquinas dispensadoras de tabaco, caracterizadas por ser portátiles y elaboradas en latón, más tarde, durante el siglo XIX, este tipo de instrumentos comenzaron a tener mucho mayor alcance gracias a Richard Carlie, un vendedor de libros que en su intento por evitar el arresto por tráfico de obras prohibidas crea una máquina dispensadora de periódicos.

En 1967 Simeón Denham obtuvo la patente para la primera máquina dispensadora de sellos totalmente automática, posteriormente en 1833 el inglés Percival Everitt crea dispositivos dispensadores de sobres, tarjetas postales y papeles para cartas, los cuales fueron instalados en estaciones de ferrocarril y oficinas de correos y dispensadores de sobres.

La primera compañía que se formó para la venta de este tipo de máquinas fue la Sweetmeat Automatic Delivery Company en 1887 en Inglaterra; seguidamente en 1888 nace en América la industria de máquinas expendedoras, cuando Thomas Adams Gum Company comenzó a vender sus chicles de Tutti Frutti, un éxito inmediato para la industria mercantil.

Ulteriormente la fabricación e implementación de máquinas expendedoras creció a tal punto que el Departamento de Comercio de EE.UU. informó que en 1995 alrededor de 45 empresas

se dedicaban a la producción de los artefactos en mención cuya operatividad era a través de dinero, dentro de las cuales se encontraba el expendio de bebidas, alimentos, confitería, cigarrillos, agua y sellos, entre otras.

En la actualidad el mercado de las máquinas dispensadoras es mucho más amplio en invasivo, a tal punto que acoge productos orgánicos, naturales, procesados y artificiales con el objetivo de llegar a todo tipo de público, es por esto que se ha vuelto parte de nuestra cotidianidad encontrar estos artefactos en prácticamente todos los lugares que concurrimos.

3. MARCO LEGAL DESARROLLADO AL RESPECTO

Aunque en el día a día se materializan este tipo de contratos, la legislación colombiana no se ha pronunciado de manera alguna, sin embargo, si lo ha hecho un país, cuyo desarrollo legislativo ha sido un modelo histórico para el nuestro, como lo es España.

La doctrina jurídico-mercantil española ha reconocido la existencia de contratos de compraventa con características singulares, denominados "especiales", ya que por su contenido no corresponden a los referidos y contemplados en la legislación vigente; un tema bastante controversial para los autores que se involucran en el mismo, pues referirse a una "compraventa especial" puede llegar a tener un sin número de interpretaciones.

Los criterios para diferenciar entre un contrato de compraventa "común" de uno "especial" no son unánimes para los doctrinantes, pues dicha especialidad puede recaer en su preparación, su perfección, su ejecución, las condiciones que formula el vendedor, el lugar en que se celebra, la presencia actuante o en la ausencia física de los que contratan, la modificación de las obligaciones de las partes, entre otras.

Lo anterior es un escenario impuesto por la realidad social, económica y técnica de la actualidad, que necesariamente afecta las relaciones humanas en todos sus ámbitos, de tal forma que resulta insuficiente la figura clásica del contrato de compraventa, donde las partes de manera directa y sistemática están permanentemente involucradas en la relación contractual.

En concordancia con lo expuesto, es acertado afirmar que han nacido nuevas formas de contratar de modo especial en el ámbito mercantil, cuya regulación se pretende en el ordenamiento español a través de la Ley 7 de 1996 del 15 de enero, sobre Ordenación del Comercio Minorista (LOCM).

La LOCM dedica, dos títulos, el II denominado "*Actividades de promoción de ventas*" y el III cuyo nombre es "*Ventas especiales*" a dictar normas sobre diferentes formas de contratación que parece pueden considerarse <<legalmente>> especialidades o tipos especiales de contratos de compraventa.

De conformidad con lo expuesto, el artículo 36 de la mencionada ley expresa: "Se consideran ventas especiales, a efectos de la presente Ley, las ventas a distancia, las ventas ambulantes o no sedentarias, las ventas automáticas y las ventas en pública subasta"; términos que define en los artículos 38, 53 ,49 y 56 respectivamente.

Para el tema que nos atañe resulta ineludible remitirse al artículo 49, 50, 51 y 52 de la misma ley, ya que dentro del concepto de "venta automática" pueden destacarse características inmersas en las relaciones contractuales de compraventa entre persona – máquina, al referir:

- **“Artículo 49 - Concepto**
    1. Es venta automática la forma de distribución detallista, en la cual se pone a disposición del consumidor el producto o servicio para que éste lo adquiera mediante el accionamiento de cualquier tipo de mecanismo y previo pago de su importe.
    2. Los distintos modelos de máquinas para la venta automática deberán cumplir la normativa técnica que les sea de aplicación.

- **Artículo 50 - Advertencias obligatorias**

    Para protección de los consumidores y usuarios, en todas las máquinas de venta deberán figurar con claridad:

    a. La información referida al producto y al comerciante que lo ofrece: el tipo de producto que expenden, su precio, la identidad del oferente, así como una dirección y teléfono donde se atiendan las reclamaciones.
    b. La información relativa a la máquina que expende el producto: el tipo de monedas que admite, las instrucciones para la obtención del producto deseado, así como la acreditación del cumplimiento de la normativa técnica aplicable.

- **Artículo 51 - Recuperación del importe**

    Todas las máquinas de venta deberán permitir la recuperación automática del importe introducido en el caso de no facilitarse el artículo solicitado.

- **Artículo 52 - Responsabilidad**

    En el caso de que las máquinas de venta estén instaladas en un local destinado al desarrollo de una empresa o actividad privada, los titulares de la misma responderán solidariamente con el de la propia máquina frente al comprador del cumplimiento de las obligaciones derivadas de la venta automática.”

Como puede observarse el Estado español desde la década de los 90’s ha procurado que la regulación legal contractual se adecue a los procesos de modernización de la economía y la realidad de los mercados, a través de la ley 7 del 15 de enero, estableciendo un marco jurídico de mínimos en el sector de la distribución y el comercio minorista.

Según la disposición normativa, es evidente quién es el comprador o adquiriente del producto; empero, pueden surgir dificultades en la determinación e individualización del vendedor, información determinante al momento de analizar la existencia del consentimiento dentro de la relación contractual.

Lo anterior teniendo en cuento que lo referido en el artículo 50 y 52 tiene dos factibles interpretaciones; la primera de ellas, aduce que el vendedor es quien tiene la calidad de oferente, cuyos datos de identificación deben figurar en la máquina; la segunda, referencia al propietario de la máquina expendedora, lo que en definitiva permite afirmar que el titular de la máquina puede ser el dueño de la misma, o la persona que con otro título jurídico la ha situado en aquel lugar determinado y cuya pretensión es lucrarse a través de su funcionamiento.

Asunto que toma mayor importancia si en él se involucra la responsabilidad contractual, pues en el escenario en que se generase un perjuicio por parte del vendedor resultará excesivamente complicado precisar quién debe asumir la obligación de indemnizar o resarcir los daños causados.

4. APORTES TEÓRICOS APLICABLES AL TEMA

Es menester aclarar entonces que para la existencia de un contrato se hace necesario que sus partes presten un consentimiento contractual cuyo géminis sea la voluntad individual, respecto de la cual Bercovitz distingue entre voluntad interna y voluntad declarada, planteando lo siguiente "Voluntad interna es aquella motivación o propósito que guía a un sujeto a celebrar un contrato. Voluntad declarada es la voluntad emitida, comunicada al exterior, a través de la cual se exterioriza la voluntad interna." (Rodríguez Cano, 2011, pág. 551)

Agrega también que, para la existencia del consentimiento contractual, no basta con que cada contratante tenga una voluntad interna favorable a la celebración del contrato, sino que es preciso que exista una mutua declaración de voluntad contractual, por lo cual es posible inferir que uno de los requisitos de la voluntad es la obligatoriedad de exteriorizar la misma.

Además, hace una clasificación según el modo en el que se manifiesta, así la voluntad puede ser expresa o tácita, explicando que nos encontraremos frente a la primera cuando se utilizan mecanismos que, por su propia naturaleza o por su derivación del consenso social, están destinados a manifestar una determinada voluntad, como sucede por ejemplo con el lenguaje escrito o hablado.

Por otro lado, habrá una declaración de voluntad tácita cuando alguna conducta desarrollada en el ámbito social tome una posición inequívoca que genere confianza ajena, es decir, actos concluyentes, cuya interpretación y valoración objetiva por terceros permita entender que expresan la voluntad contractual del sujeto.

Cristóbal Alzate Hernández acoge esta misma clasificación precisando que un claro ejemplo de la voluntad expresa es levantar la mano en una subasta, teclear "enter" en una oferta electrónica, o simplemente la firma de las partes en un contrato escrito, actos que aluden a una aceptación explícita y directa.

Al respecto el Código de Comercio colombiano en su artículo 854 contempla "La aceptación tácita, manifestada por un hecho inequívoco de ejecución del contrato propuesto, producirá los mismos efectos que la expresa, siempre que el proponente tenga conocimiento de tal hecho dentro de los términos indicados en los artículos 850 a 853, según el caso.

Es así como el libre consentimiento de las partes que integran el contrato es una exigencia ineludible para este, el cual se manifiesta por la concurrencia de la oferta y la aceptación que recae sobre un objeto, cuyo propósito debe ser la creación de un vínculo jurídico, emanado y exteriorizado por una persona capaz.

Sin embargo, dicha exteriorización no necesariamente debe hacerse de manera verbal, pues la realidad y la lógica nos permiten comprender que las personas tenemos infinidad de métodos para expresar nuestro querer interno, más aún cuando se trata de relaciones jurídicas, un claro ejemplo de ello son los contratos de compraventa a través de máquinas dispensadoras.

Me resulta sustancialmente importante en este punto hacer hincapié en que teniendo en cuenta toda la información planteada, no es del todo conveniente expresar libremente que se contrata con máquinas, pues en realidad se llevan a cabo contratos con personas a través de máquinas.

Por lo cual la relación de obligatoriedad y responsabilidad no debe verse afectada en ningún momento, pues la figura contractual nace plenamente con todo y sus implicaciones, empero es necesario que en el ambiente tecnológico en que se desarrolla un país como Colombia se regule con mayor rigor un tema como estos.

Ya que existen multiplicidad de formas jurídicas contractuales que pueden ocultarse tras la disposición de una máquina dispensadora en un lugar, como lo son el contrato de concesión de espacios, el contrato de arrendamiento comercial, el contrato de consignación, entre otros, los cuales limitarían la responsabilidad en diferentes formas de todos los sujetos intervinientes en ellos.

REFERENCIAS BIBLIOGRÁFICAS

ALZATE HERNÁNDEZ, Cristóbal (2009), "*Fundamentos del contrato, Segunda edición*", Ibáñez: Bogotá, D.C.

ARRUBLA PAUCAR, Jaime Alberto (2008), *"Contratos mercantiles, Tomo I".* Diké: Bogotá, D.C.

ASENSIO, Alberto De Miguel (2001), "*Derecho privado de internet".* Pág. 164. Civitas ediciones: Madrid.

BLANCO, Alberto (1948); "*Curso de Obligaciones y Contratos en el Derecho Civil español, segunda edición*" Pág. 174. Cuba: La Habana.

BONFANTE, Pietro, (1929), *"Instituciones de derecho romano".* Pág. 399-400. Reus S.A.: Madrid.

CÁRDENAS RINCÓN; (2015), *"Derecho del comercio electrónico y de internet".* Pág. 11. Editorial Legis: Bogotá.

Código Civil, trigésimo cuarta edición, 2015. Leyer Editores.

Comunicación del 14 de septiembre de 2001 por parte de la Comisión al Consejo y el Parlamento Europeo – Iniciativa europea de comercio electrónico, comunicado 97, pág 157.

DE MIGUEL ASENSIO, Pedro Alberto (2001), *"Derecho Privado en Internet, segunda edición",* Civitas: Madrid.

Decreto 0591 de 1991, (febrero 26); *Por el cual se regulan las modalidades específicas de contratos de fomento de actividades científicas y tecnológicas*; Recuperado el 15 de septiembre de 2016 de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=1360

Decreto 4176 de 2011, (noviembre 3), *"Por el cual se reasignan unas funciones del Ministerio de Comercio, Industria y Turismo a la Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales -DIAN- y a la Superintendencia de Industria y Comercio, y se dictan otras disposiciones"*.

DIEZ-PICAZO, L. & GULLÓN, A. (1984) *"Sistema de Derecho Civil, Vol.1"*. Tecnos: Madrid.

Directiva 891392/CEE relativa a la aproximación de las legislaciones de los estados miembros sobre máquinas, recuperado el 06 de octubre de 2016 de http://www2.uca.es/serv/comite_empresa/salud_laboral/web/rd1435.htm

Directiva 98/34/CE del Parlamento Europeo y del Consejo, del 22 de junio de 2008. Recuperado el 10 de septiembre de 2016 de http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=celex%3A32008L0098

FERNÁNDEZ SESSAREGO, Carlos. (2000), *"El supuesto de la denominada autonomía de la voluntad"*, Gaceta jurídica: Lima.

GONZÁLEZ AGUILAR, FERREYROS SOTO & CARRASCOSA LÓPEZ (2004), *"Los contratos en la sociedad de la información, Formularios de contratos información e Internet"*, Comares: Granada.

HINESTROSA, Fernando (2007), *"tratado de las obligaciones, tercera edición"*, universidad Externado de Colombia: Bogotá, D.C.

Investigación de la tecnología, la comunicación, el entretenimiento y el comercio electrónico; Recuperado el 12 de septiembre de 2016 de http://www.pabloburgueno.com/tag/equivalencia-funcional/

RINCÓN CÁRDENAS, Erick (2015) *"Derecho del Comercio electrónico y de Internet, segunda edición"* LEGIS S.A: Bogotá-Colombia.

RODRÍGUEZ CANO, Rodrigo Bercovitz (2011), *"Tratado de Contratos, Tomo I"*, Tirant lo Blanch: Valencia.

RODRÍGUEZ CANO, Rodrigo Bercovitz (2011), *"Tratado de Contratos, Tomo II"*, Tirant lo Blanch: Valencia.

SECO CARO, Enrique. (2009). "*el contrato mercantil de compraventa*. Marcial Pons: Barcelona

UMAÑA CHAUX, Andrés, (2005) *"Algunos comentarios sobre el principio del equivalente funcional en la Ley 527 de 1999"*, en: *Revista de Derecho Comunicaciones y Nuevas Tecnologías*, Universidad de los Andes, Bogotá.

URBANO SALERNO, Marcelo (2003), *"Contratos civiles y comerciales"*. Pág. 11. Oxford University Press: México.

GALERÍA DE FOTOGRAFÍAS

Memorias del XXII Congreso Iberoamericano de Derecho e Informática

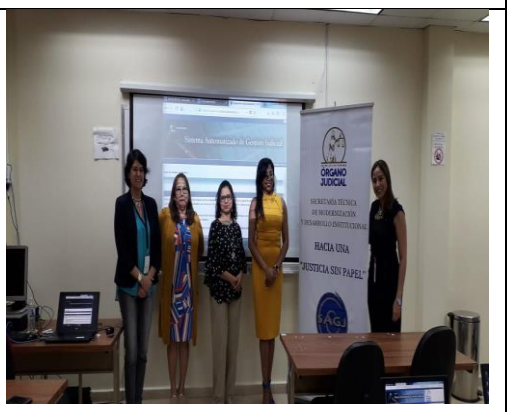
Junta Directiva de APANDETEC

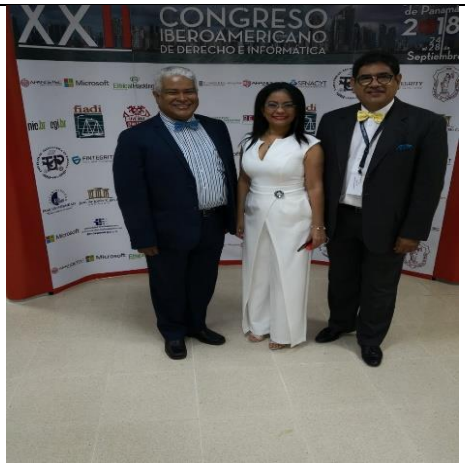
Miembros de APANDETEC y el Administrador de la Autoridad de Innovación Gubernamental, ingeniero Irvin Halman, previo a su conferencia de apertura Avances del gobierno electrónico – Panamá 2.0.

Mesa de debate: Protección de datos personales vs libertad de expresión

Magistrado José Ayú Prado Canals y miembros de APANDETEC posteriormente a la presentación de su conferencia El acceso a la justicia, la digitalización y las nuevas tecnologías.

Mesa de debate: Procesos electorales: Bots y manejo de tendencias en redes sociales, participan Mgter. Karen Flores, Ing. Álvaro Andrade, Dra. Cristina Torres Ubillús, Honorable Diputada Katleen Levy y Lic. Ricardo Lombana

		
Marlon Fetzner, abogado de Microsoft con la ponencia Cloud Computing e Inteligencia Artificial		Panel de discusión TIC, Perspectiva de Géneros y Grupos Vulnerables
		
Ingeniero Juan Pablo Quiñe durante su conferencia Magia, Innovación y Pensamiento Hackers		Participantes del taller: Expediente Judicial Electrónico dictado por el Órgano Judicial en el congreso.
		
Ingenieros Eduardo Snape y Hubert Demercado luego de su conferencia Eso fue gato de casa: Ataques internos, riesgos y estrategias de mitigación.		Finalización del reconocido conferencistas Dragón Jar

		
El Magistrado Abel Zamorano, asistente del evento, visita el stand del Órgano Judicial en el marco del XXII Congreso Iberoamericano de Derecho e Informática		El profesor Francisco Flores, presidente de la Comisión designada por la Facultad de Derecho de la Universidad de Panamá junto a Yoselin Vos presidente del Congreso y Augusto Ho presidente de FIADI
		
Miembros de APANDETEC, durante la realización del congreso		Miembros de APANDETEC, promoviendo distintos hashtags alusivos al evento
		
Presentación de SICASTENIA		Presentación de SICASTENIA