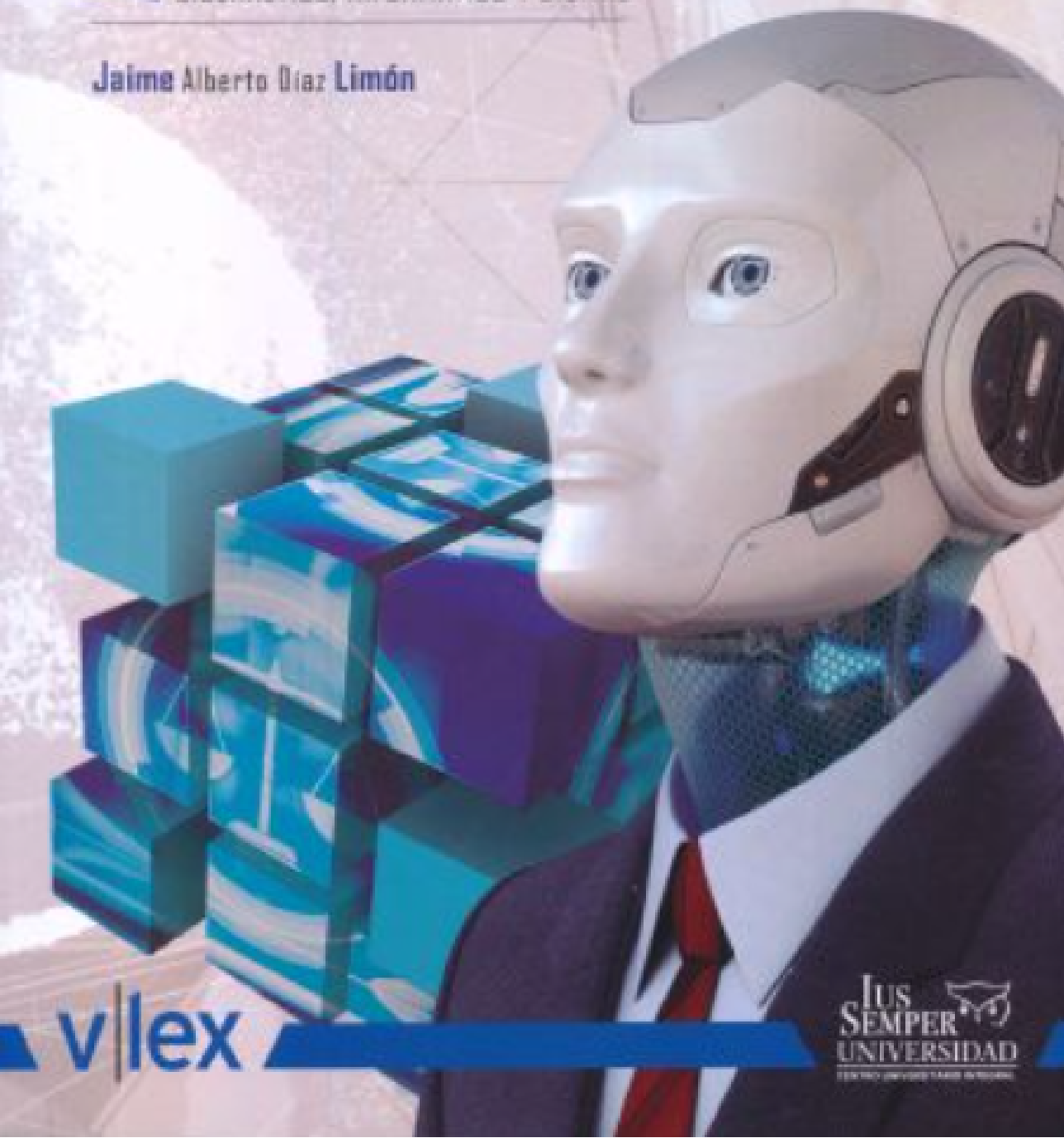
ABOGADO DIGITAL

ESTUDIOS SOBRE DERECHO CIBERNÉTICO, INFORMÁTICO Y DIGITAL

Jaime Alberto Díaz Limón



v|lex

IUS SEMPER UNIVERSIDAD

Presentación

La revolución digital ha cambiado radicalmente la forma en que vivimos, nos relacionamos y nos comunicamos. En un abrir y cerrar de ojos, pasamos de una era industrial a la era de la información y del conocimiento, esta era se rige por la interconectividad y el intercambio masivo y en tiempo real de datos, es una era sin fronteras. Con el uso de las Tecnologías de la Información y Comunicación (TIC), y sobre todo con el Internet, hemos cambiado no sólo la forma en la que interactuamos sino nuestra forma de concebir el mundo también.

En una era en la que los códigos de programación pueden cambiar la conducta de las personas más que las leyes, es imprescindible reinventarnos y entender el rol que juega el derecho en la cibersociedad. Sobre todo si entendemos al derecho como la disciplina que estudia las leyes, los principios y las reglas que regulan la vida en sociedad y las interacciones entre las personas. Si nuestras interacciones hoy son digitales, el derecho y los abogados también deben serlo.

El Nuevo Paradigma Digital

Para lograr esta transformación del sector jurídico, debemos entender los paradigmas básicos que se están formando en esta nueva era. De acuerdo con Kevin Perry en su libro *Inevitable: las 12 fuerzas tecnológicas que configurarán nuestro futuro,* algunos de los factores que dan forma a estos nuevos paradigmas son la desmaterialización, la descentralización, la sinergia entre plataformas y los servicios en la nube. Entender cada una de estas cuatro tendencias es entender los modelos de negocios y estilos de vida de esta era digital, así como los retos que estos representan para el sector legal, un sector que debe ser disruptivo y empezar a pensar diferente.

Es en el contexto de estos paradigmas que la presente obra, *Abogado Digital*, encuentra su relevancia pues con una completa comprensión de la nueva era, el autor plantea nuevas posibilidades técnicas para renovar el enfoque del derecho, haciendo **énfasis** en los cuestionamientos y conocimientos que debe de tener un abogado digital. En esta introducción atenderé de forma breve cada uno de los factores mencionados y cómo se entrelazan con los temas del libro.

La desmaterialización

Hoy en día es más importante acceder que poseer. Cada vez somos dueños de menos cosas de las que usamos y preferimos pagar una renta o suscripción por lo servicios.

Ya no compramos películas, pagamos mensualmente una cuenta de Netflix. No compramos música, usamos Spotify. No adquirimos coches, los sacamos en *leasing* o usamos Uber. Preferimos ya no pagar por lo material sino por la comodidad de un fácil acceso sin tener la responsabilidad del almacenamiento y el mantenimiento.

Esta tendencia también la podemos observar en el mundo empresarial. Uber es la empresa más grande de transporte y no tiene automóviles ni emplea conductores. Airbnb es la empresa más grande de alojamiento y no es dueño de ningún inmueble. Alibaba es la empresa más importante de comercio electrónico y no tiene productos en su inventario. Todo esto cambia radicalmente el concepto que tenemos de propiedad privada y de patrimonio. De ahí que es importante el tema que aborda este libro sobre el innovador concepto de *patrimonio digital*, ¿cómo se compra, se vende o se hereda? Así mismo es de suma importancia entender el cómo se aplica la propiedad intelectual en el mundo de lo intangible.

Mientras los gobiernos aletargadamente descifran cómo regular estos fenómenos, la tecnología sigue avanzando a pasos exponenciales. Y las preguntas son las siguientes: ¿realmente la ley puede ordenarle a un algoritmo? ¿La regulación será la solución?

La descentralización

La tecnología que permitió la comunicación instantánea de larga distancia, desencadenó la era de la descentralización. El mundo de las redes nos ha alejado de las organizaciones centralizadas. Por ejemplo, antes los medios de comunicación eran dueños de la información y decidían qué y cómo la compartían, ahora con Internet, estamos todos conectados y no sólo tenemos acceso a más información sino que tenemos la posibilidad de ser generadores de información. Hoy en día, cualquiera puede abrir un blog y compartir su opinión.

Las empresas que funcionan bajo estos paradigmas abren sus portales a que los consumidores dejen comentarios y calificaciones sobre sus productos y servicios. Para tomar una decisión de compra sólo hay que ver los comentarios de otros usuarios para confiar en la calidad. Entonces, de esta forma, la información, el comercio y la confianza se han descentralizado.

La disrupción ya también ha llegado a uno de los sectores más centralizados: el financiero. Siendo el dinero la última de las instituciones centralizadas ya que su regulación y seguridad recae en un banco central que dicta su flujo y su valor, la descentralización de las inversiones con el *crowdfunding*, de los pagos fuera del sistema bancario con monederos electrónicos como PayPal o de la moneda, como el Bitcoin, con las implicaciones del surgimiento de la tecnología *blockchain* (cadena de bloques), ha puesto a las instituciones a replantear sus estructuras.

En este contexto, surgió el sector Fintech, o de tecnologías financieras, que teniendo como estandarte el principio de la inclusión financiera, hizo que el efectivo

dejara de ser el único método de pago descentralizado y poco a poco transformar el sector financiero tradicional.

Aunque la *blockchain* todavía está muy vinculada con las criptomonedas, me parece que será la tecnología que revolucionará nuestra era y terminará de descentralizar los sectores y sistemas que faltan. Con su base de datos compartida, *blockchain* permite que su historial de transacciones esté abierto a cualquier usuario que las confirme matemáticamente. Con esta tecnología se confía en las matemáticas en lugar de confiar en el gobierno. La cadena de bloques revoluciona el concepto de confianza en las transacciones entre extraños que antes tenían que ser vigiladas y validadas por una autoridad o gobierno y ahora es la tecnología la que garantiza su transparencia.

Las aplicaciones de la *blockchain* son muchas y cada día la veremos más en uso. Ya empezamos a aplicarla en procesos de elecciones, en bienes raíces, y puede ser usada para registros públicos, presupuestos gubernamentales, procesos de importación y exportación, entre otros.

En este mismo sentido de la descentralización, surgen los mecanismos de autorregulación de las plataformas, de los cuales nos platica el autor en este libro, en donde ya no serán autoridades centrales, como un poder judicial o tribunales, los que diriman controversias entre usuarios. Las mismas plataformas están desarrollando sus mecanismos de autodeterminación, con el uso de inteligencia artificial, para resolver controversias entre los miles o millones de usuarios de sus plataformas que de forma tradicional no se podrían solucionar porque saturarían al sistema.

Sinergia entre plataformas

Así como lo vimos anteriormente, las grandes empresas hoy son las plataformas como Uber, Airbnb, Facebook, etc., y que no son dueñas de nada, sino que su negocio es el desarrollo de software que permite conectar usuarios. Es en esta sinergia entre plataformas en donde surge una nueva forma de organizar el trabajo, la empresa y la vida.

Hoy en día, no necesitas tener tu propia tienda en línea para poder vender algo como empresa o individuo, existen las plataformas que te permiten comprar y vender, como son Mercado Libre, Facebook o Kichink. De esta forma los productos se vuelven interdependientes y las plataformas sólo abren sus espacios para conectar a usuarios, creando las reglas que permiten que otros interactúen. De este principio nacen las API's (Interfaz de Programación de Aplicaciones) que permiten la conexión entre softwares para poder navegar fluidamente en el ciberespacio con compatibilidad entre plataformas.

Todas estas reglas, junto con las firmas y contratos electrónicos e inteligentes serán las que rijan el comercio electrónico en el siglo XXI. Para logar aterrizar estos

contratos y garantizar las transacciones en las plataformas, salvaguardando los derechos del consumidor y la seguridad de las empresas, se requerirá de abogados doctos en estos temas para presentar soluciones eficientes y prevenir conflictos.

El cómputo en la nube

Finalmente, entre todas estas tendencias, tenemos el cómputo en la nube que trae consigo el gran paradigma de la portabilidad: el tener acceso a nuestra información y patrimonio digital en cualquier lugar y en cualquier momento. La dispersión de la información y datos en la nube hace que todo ese patrimonio esté almacenado en todos lados y en ninguno, ya que no hay un solo servidor que lo contenga.

La nube no tiene una geografía ni una jurisdicción y algunas de las interrogantes que deberá contestar el abogado digital son ¿quién es dueño de la información y de los datos? ¿quién y en dónde se deben pagar impuestos si una actividad económica se lleva a cabo en la nube por una persona que está en México y contrata un servicio de una empresa norteamericana que almacena una parte de la información en sus servidores en Irlanda y otros en Alemania?

La tendencia del cómputo en la nube es que las nubes se conecten entre sí, pero para que esto ocurra, las nubes necesitan compartir datos, actividad que cada vez está más vigilada y restringida por las nuevas legislaciones, así que tomará un tiempo para que las empresas aprendan a compartir sus datos de manera creativa, productiva y responsable.

Transversal a todos estos factores, tenemos la llegada de la Inteligencia Artificial (IA), tema analizado desde la perspectiva jurídica con gran acierto en este libro. Por el lado empresarial, podemos decir que los grandes negocios de la siguiente década constarán en hacer cognitivo todo lo que alguna vez fue electrificado, transformando con ello a los productos y servicios en inteligentes. Antes teníamos un teléfono, con la IA ahora tenemos un teléfono inteligente. Antes teníamos un refrigerador, ahora tenemos un refrigerador inteligente que sabe qué productos son de nuestra preferencia, nos avisa cuándo se van a acabar e inclusive los puede pedir por nosotros al supermercado.

Pero la IA no sólo llegó para replantar los negocios sino al propio ser humano. Tenemos ya el primer robot del mundo, llamado Sofía, reconocido con una ciudadanía. Esto obligará al derecho a regresar a la filosofía y replantearse inclusive qué es la persona. Le llamamos derechos humanos a los derechos de las personas, pero ¿cómo le llamaremos entonces a los derechos de los robots?

Estas son interrogantes que las actuales leyes no nos pueden contestar y por lo que tocará a los abogados digitales salir de la caja y favorecer a la tecnología como la solución a los problemas entre usuarios. El avance tecnológico nos seguirá sorprendiendo y orillándonos al cambio. Hoy más que nunca es preciso que el abogado

se allegue de conocimiento de otras disciplinas que están marcando el rumbo de la era digital para que así, a través del conocimiento colaborativo, logremos adaptar el derecho a las nuevas necesidades del siglo.

Mtra. Janet Huerta Estefan
Ciudad de México
30 de octubre de 2018

Prólogo

La Ciencia Jurídica evoluciona constantemente, no sólo en cuanto a los procedimientos, sino a la forma de aplicarla y conocerla. La era digital en la que nos encontramos permite la globalización de medios de comunicación, de conocimiento, de transacciones comerciales, y el Derecho no es la excepción. Pocos juristas se han preocupado por el análisis del derecho desarrollado a través de las técnicas de la información y comunicación.

El Maestro Jaime Alberto Díaz Limón, a quien admiro profundamente dada la pasión con la siempre se ha dirigido hacia el estudio de la norma jurídica, es uno de los pioneros en analizar a la ciencia jurídica desde la perspectiva de la tecnología. El Maestro Díaz Limón incansablemente ha compartido sus conocimientos con innumerables generaciones de alumnos para hacerles ver que la tecnología es la apuesta actual del derecho; esta vez lo hace maravillosamente con su obra intitulada: *Abogado Digital. Estudios sobre Derecho Cibernético, Informático y Digital*; en la cual analiza diversas áreas de la era digital aplicadas al derecho.

Lastimosamente, algunos abogados que pertenecen la guardia antigua de los estudiosos del derecho se rehúsan a aplicar las técnicas y estrategias tecnologías del derecho, argumentando que la norma jurídica no requiere de computadoras ni de elementos tecnológicos para su conocimiento y desarrollo. El Maestro Limón piensa lo contrario, y además no sólo lo piensa sino que día a día demuestra con sus investigaciones la gran importancia que tiene la tecnología para la aplicación del derecho y su desarrollo, lo cual implica que sociedades enteras se puedan incluir al desarrollo, a la globalización y hasta en la comunidad internacional.

De hecho, en el mundo se habla de *Open Government*, de transparencia, la participación ciudadana para hacer cumplir y lograr el Derecho Humano a una buena administración; sin embargo, sin las opciones del Derecho Digital prácticamente sería imposible. Es así como el Derecho Digital abrió la puerta a conceptos como *Gobierno Electrónico*.

En este sentido, se puede indicar que las políticas públicas del *Open Government* del Derecho Digital tienen su base en los siguientes puntos:[1]

[1] Wallerstein, Immanuel. *El Universalismo Europeo. El discurso del Poder.* Inglaterra, 2004. Editorial Siglo XII. Primera edición en inglés 2006, primera edición en español 2007. Página 34. Visible a través del vínculo http://scienzepolitiche.unical.it/bacheca/archivio/materiale/2467/Textos%20en%20espa%C3%B1ol/Immanuel%20Wallerstein-Universalismo%20europeo_%20el%20discurso%20del%20poder-Siglo%20XXI%20(2007).pdf

Busca la legitimidad para que los ciudadanos obedezcan.

1. Transparencia desde la perspectiva de los productos y procesos.
2. Permitir que el gobierno detecte el mal funcionamiento en los niveles bajos de su administración.
3. Revelar las ventanas de oportunidad.

Podemos indicar que una de las ventanas de oportunidad para el Derecho Digital es precisamente la confianza que genera hacia los ciudadanos dada la infalibilidad con que cuenta. De acuerdo a los datos del 2010 de la OCDE, los beneficios de la transparencia en el *Open Government* con base en plataformas digitales, son los siguientes:[2]

1. Mayor confianza en los gobiernos.
2. Mejores resultados con el menor costo posible.
3. Se elevan los niveles de cumplimiento de los Servidores Públicos y, por añadidura, se reduce la corrupción política.
4. Aseguran la equidad en las políticas públicas.
5. Fomentan innovación y nuevas actividades económicas.

Lo anterior nos da la pauta para mencionar que la inflexión de la Transparencia en la Administración Pública de un gobierno abierto es que procura la especialización de las actividades de los ciudadanos en virtud del fomento de la competencia económica a través de normas jurídicas insertas y fácticas desde una plataforma digital. En tal sentido, ya no tendría cabida la participación de los ciudadanos que no estuvieran especializados tecnológicamente para colaborar en la toma de decisiones del Estado, lo que traería como consecuencia una gran exclusión de sujetos no capacitados en el mundo jurídico digital.

Muestra de lo anterior es lo indicado por el Dr. Villoria con respecto a los cuatro ejes básico del *Open Government*:[3]

1. La regulación.
2. La Transparencia.
3. El gobierno participativo y promotor de civismo.
4. Un gobierno eficiente, colaborador y generador de conocimiento.

Si un gobierno no se preocupa por la especialización de sus ciudadanos en la tecnología, el gobierno abierto y la transparencia, podría fomentar la corrupción y generar movimientos sociales por la desigualdad en la competencia económica de la

[2] *Idem.*

[3] *Idem.*

actual dinámica neoliberal global. De ahí la enorme importancia de la obra del maestro Díaz Limón.

De hecho, el impacto político y los efectos que tiene en la ciudadanía del Gobierno Electrónico son fundamentales. Los uruguayos Pablo Valenti y Lucio Castro son investigadores que analizan y proponen las ventajas del Gobierno Electrónico.[4] La finalidad de la investigación de dichos autores radica en el impacto económico que tienen los Gobiernos Electrónicos en la Administración Pública, en cuanto a diversos sectores que tienen que identificar con el fin de integrar y coordinar técnica, política e institucionalmente a las administraciones.

Por tal motivo, la cuestión electrónica evidente impacta en las familias, las empresas y los gobiernos, pues en virtud de la globalización, las tecnologías de la comunicación son sumamente importantes para determinar indicadores cualitativos y cuantitativos para el ahorro, los mercados, el trabajo, el empleo, la inversión y la productividad. Todo lo anterior se traduce en ganancias financieras y en democracia a través de la participación ciudadana gracias al acceso de la transparencia de forma electrónica, mejorando así la calidad de vida de los sujetos sociales.

En ese tenor, el Gobierno Electrónico busca resolver el impacto político y los efectos de la ciudadanía para calcular el costo-beneficio de las políticas públicas. De acuerdo a dichos autores, el Gobierno Electrónico mejora la gobernanza, la gobernabilidad, la cohesión social y el impacto ambiental; además que se obtienen grandes ahorros en la gestión del Estado. El problema radica en que muchos países no están actualizados en este rubro, en América Latina, por ejemplo, los países que tienen la punta en este tema son Chile, Colombia, Uruguay y Nicaragua.[5] En el análisis del doctor Villoria se explican y critican a los cuatro países de referencia, con base en los elementos de la globalización y el neoliberalismo, sobre todo en lo que se refiere a la conveniencia del uso de las tecnologías de la información con respecto al Gobierno Electrónico, por ejemplo, el Internet.

Los fines de su uso, los procedimientos incorporados al proceso y, sobre todo, los marcos de creencias y valores que subyacen al desarrollo de estos tipos concretos de innovaciones de gestión a través de las TIC, según Villoria, nos permiten diferenciar al menos cuatro grupos o marcos de ideas que confluyen en el *Open Government*:

[4] Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento (AGESIC). 20 de junio de 2011. http://youtu.be/qDvuC5GH_pI (última visita: 1 de abril de 2016).

Instituto Global de Altos Estudios en Ciencias Sociales. El Open Government ¿Un nuevo paradigma para el Gobierno?, 17 de diciembre de 2012. http://youtu.be/PoYqNlnBoy4 (accessed 1 de Abril de 2016).

[5] Agencia de Gobierno Electrónico y Sociedad de la. YOU TUBE. AGESIC. 20 de JUNIO de 2011. http://youtu.be/qDvuC5GH_pI (accessed 1 de ABRIL de 2016).

Instituto Global de Altos Estudios en Ciencias Sociales. you tube. Edited by FUNGLODE Media. FUNGLODE Multimedia. 17 de Diciembre de 2012. http://youtu.be/PoYqNlnBoy4 (accessed 1 de Abril de 2016).

1. El gobierno como promotor de bienestar a través de la capacidad regulatoria. Si asumimos que el gobierno debe preocuparse de la felicidad de sus ciudadanos, entenderemos que un gobierno que observe conductas que son dañinas para los propios individuos, aunque no generen excesivo daño social, debe actuar para desincentivar tales actuaciones. No obstante, una intromisión excesiva del Estado en la vida privada es contraria a los ideales de libertad que la democracia liberal sostiene. De ahí surge la teoría del paternalismo libertario. La parte libertaria del enfoque es la clara insistencia en que, en general, la gente debe ser libre de hacer lo que consideren adecuado (siempre que no dañen a los demás). En suma, deben ser libres de rechazar acuerdos o reglas que les desagradan e incluso destruir sus visas si así lo deciden. El aspecto paternalista reconoce que es legítimo para los gobiernos tratar de influenciar la conducta de sus ciudadanos para que sus vidas sean más largas, más sanas y mejores.
2. El gobierno transparente que rinde cuentas. Los orígenes de este modelo de gobierno tienen una larga historia y, esencialmente, sus ideas clave provienen de la ilustración y, posteriormente, de los debates de los fundadores de la democracia estadounidense. Estamos ante un gobierno que busca, a través del sistema de pesos y contrapesos, el control de los que gobiernan entre sí y por los gobernados. Es la dimensión más vinculada a la transparencia pasiva, el derecho a saber y a la transparencia activa, vinculada a las páginas web gubernamentales. En este ámbito es donde se sitúan en gran parte, además, las medidas que vinculan gobierno abierto con lucha anticorrupción.
3. El gobierno participativo y promotor de civismo. Este modelo nos retrotrae idealmente al gobierno republicano clásico, que activa la participación y promueve el ejercicio de la soberanía popular. Además, asume que un buen gobierno requiere civismo.
4. El gobierno eficiente, colaborador y generador de conocimiento. La apertura de la información y la transparencia generan eficiencia. Los estudios sobre la transparencia y sus efectos beneficiosos en el mundo de la economía son muy numerosos. Los datos sobre el funcionamiento de la economía, proporcionados por los Estados, ayudan a los mercados a funcionar mejor; gracias a ellos los inversores, los productores y los consumidores pueden tomar decisiones más eficientes. La transparencia gubernamental se correlaciona muy fuertemente con el ingreso per cápita. También a través de su efecto en el control de la corrupción, mejora la eficiencia de la economía y su atracción de inversiones. Pero la transparencia no sólo es importante para la economía, también lo es políticamente, pues sin un electorado informado incluso las votaciones pierden valor.[6]

[6] *op. cit.*, nota 3, p.p. 6, 7, 11, 13.

Como se desprende de la descripción que hace Villoria con respecto a los cuatro tipos de gobierno abierto, las tecnologías de la información son de vital importancia a efecto que se puedan cumplir algunas de las expectativas sociales, entre ellas: el nivel de conciencia y conocimiento por parte de la ciudadanía con el fin de poder tomar decisiones junto con el gobierno, así como un nivel económico adecuado que permita su acceso a la comunicación a través de la tecnología. Aquí es cuando al leer la obra del maestro Díaz Limón me quedé impactada sobre la gran área de oportunidad que nos está ofreciendo: simplemente la inclusión hacia la élite jurídica; pues no cualquiera maneja tales temas como majestuosamente lo hace mi querido amigo Díaz Limón.

Tal pareciera que pudiera resultar complicado que millones de personas tengan acceso a las tecnologías de la información, por tanto, a la transparencia y a una buena participación ciudadana; sin embargo, el maestro Díaz Limón nos regala su maravillosa obra para que logremos incluirnos en la evolución jurídica.

La grandiosa obra del maestro Limón consta de un capítulo llamado Patrimonio Digital, en el cual desarrolla, analiza e informa la importancia de datos personales contenidos en plataformas virtuales; así como su protección en redes sociales. Nos habla de un tema maravilloso que me causó gran impacto: la identidad y reputación digital.

En el Capítulo II, el maestro Díaz Limón refiere su análisis al testamento digital: ya no es necesario testar a través de notarios públicos e instituciones burocráticas lentas sino que basta una plataforma digital para tal efecto; ya no es necesario trámites largos de solicitudes a innumerables instituciones para tener conocimiento si alguien ha testado o no, basta hacer un simple clic desde nuestro celular para saberlo y a la vez enviarlo digitalmente ante la autoridad correspondiente.

El tercer capítulo de la obra del maestro Díaz Limón lo refiere a la jurisdicción en redes sociales; estas que día a día utilizamos subiendo información sin tener conocimiento de la norma jurídica que les es aplicable y de las consecuencias que esto puede traernos como usuarios.

El capítulo IV se refiere a la importancia que tiene la inteligencia artificial más allá del derecho positivo; capítulo que liga con la creación de derechos de autor. En dicho apartado, el maestro Díaz Limón estudia a la Inteligencia Artificial como una herramienta auxiliar en la creación de Derechos de Autor, el marco legislativo aplicable y los derechos de autor susceptibles de protección.

Un tema que me pareció de suma importancia y del que la mayoría no estamos tan inmersos es la explotación digital de los derechos de autor ¿Cómo es que podemos patentizar nuestras obras a través de plataformas digitales públicas?: El maestro Díaz Limón tiene la respuesta en esta obra.

Si perteneces a la comunidad científica correspondiente al núcleo digital, esta obra es imperdible para ti; pues el maestro Díaz Limón te explicará a detalle y en un lenguaje sumamente sencillo cuáles son los sistemas de licenciamiento de los programas de cómputo.

Youtube, Twitter, Facebook, Stream Ripping y otras plataformas digitales (llamadas redes sociales) manejan información privada como si fuera de dichas compañías, todo ello a través del ciberespacio.

Un tema maravilloso que maneja en su obra el Maestro Díaz Limón es, sin duda, el Acceso a las Tecnologías de la Información como Derecho Fundamental; efectivamente, el Maestro es certero al indicar que los ciudadanos tenemos derecho a Internet, a contratar privadamente mediante plataformas digitales, a realizar transacciones económicas a través de la red (con su debido respeto a la norma jurídica y sin caer en algún ilícito penal o administrativo), a solicitar información pública, pero sobre todo al acceso a las redes.

Como se puede observar, la obra del Maestro Díaz Limón es un gran legado para la sociedad, una obra que nos permite incluirnos con las nuevas generaciones y hablar el mismo idioma desde la perspectiva digital, una obra que todo abogado debe tener, leer y analizar pues el marco jurídico y su aplicación han llegado a las Tecnología de la Comunicación y de la Información.

El tiempo nos ha alcanzado, en nosotros como juristas está la toma de decisioues para incluirnos en la "nueva era jurídica". Un honor para mí haber prologado tan magnánima obra, con una gran visión sobre lo que nos depara el futuro en el ámbito jurídico. Un honor para mí haber prologado una obra visionaria, cuyo objeto básico es la ciencia que más amo: la jurídica. Pero, sobre todo, un gran honor para mí haber prologado una obra cuyo autor admiro, quiero y respeto como gran académico e investigador: el Maestro Díaz Limón.

Gracias Maestro por permitirme prologar tu magnánima obra.

¡Gracias al Arquitecto del Universo por tanto!

Dra. Lizbeth Xóchitl Padilla Sanabria
Ciudad de México
12 de abril del 2018

Introducción

¿Qué es un Abogado Digital?

El jurista que estudia la aplicación de las nuevas Tecnologías de la Información y la Comunicación que se involucran en la práctica jurídica, desde el punto de vista preventivo, dogmático, pragmático y jurisdiccional. En tenor de lo anterior, un *Abogado Digital* adquiere conocimientos transversales y multidisciplinarios, con apoyo de otras ciencias sociales y exactas, para la comprensión, estudio y, en su caso, regulación, enunciativa más no limitativamente de: *i)* La Sociedad de la Información (cibersociedad); *ii)* Protección de datos personales; *iii)* Seguridad Informática y de la Información; *iv)* Gobierno electrónico y transparencia; v) Protección de Derechos de Personalidad; *vi)* Contratación electrónica y comercio electrónico; *vii)* Delitos cibernéticos, informáticos y digitales; *viii)* Propiedad Intelectual en el ámbito digital; *ix)* Automatización de procesos en la práctica jurídica (Informática e Inteligencia Artificial).

En términos de lo anterior, un Abogado Digital es el experto en Derecho que apoya su práctica en estudios científicos multidisciplinarios para la construcción metodológica de nuevas áreas de estudio, como lo son: Derecho Cibernético, Derecho Informático y Derechos Digitales. Por ende, un Abogado Digital depende del consejo de expertos en informática, sociólogos, programadores y arquitectos web, comunicólogos, mercadólogos, politólogos, inclusive psicólogos y neoconductistas para el perfeccionamiento de su objeto, objetivo y marco de estudio.

No es posible clasificar al Abogado Digital, de forma exclusiva, en el sistema inquisitivo, dispositivo o social; toda vez que la figura del Abogado del nuevo siglo resulta igualmente necesario en cualquier rama y materia de Derecho consecuencia de la mutación social, en la cual el ser humano ha optado por construir 2 tipos de vida: *On Line* y *Off Line*. Sobre la primera modalidad, se enfoca el estudio del jurista digital y la realización de la presente Obra.

De tal suerte, el Abogado digital tiene por objeto el estudio del uso de las nuevas tecnologías de la información y comunicación, así como el comportamiento de los ciudadanos digitales en la cibersociedad. Tiene como objetivo la implementación de la tecnología en el perfeccionamiento de la abogacía y la construcción de normas jurídicas que procuren la regulación en el uso de TIC'S y mecanismos de automatización, sobre todo en el ambiente digital. En consecuencia, el marco de estudio no sólo se limitará al estudio de derecho positivo (nacional y comparado), sino que también incluirá al reconocimiento de costumbres digitales y tecnológicas, para el mejor entendimiento de las necesidades del ciudadano digital del siglo XXI.

En el aspecto humano, el Abogado Digital comprende que la mejor forma de construir conocimiento son los ambientes colaborativos y la apertura absoluta al debate público. Su unisión es humanizar el Derecho a favor de los ciudadanos digitales y derribar las barreras del lenguaje o protocolos que alejen al Usuario final del abogado: ¡Adiós corbata y sacrameutal despacho!

Sin duda, es complejo construir una definición axiomática de Abogado Digital, pero en la presente obra encontrará la propuesta, que humildemente ofrezco al lector, con la intención de procurar el reconocimiento al rigor académico y profesional, que implica la construcción del Abogado del siglo XXI.

Para la Atención del Lector

En las presentes líneas propongo la construcción de nuevas fórmulas jurídicas, algunas posibles respuestas a debates tecnológicos y de resultar indispensable, la flexibilización de conceptos que otrora consideraiios iuamovibles, en el estudio del Derecho. De esta forma, con respeto, me permito sugerir lo siguiente:

1. Un espacio adecuado (físico o tecnológico) para realizar la lectura es indispensable para lograr concentración en las letras que propongo.
2. Elegir el horario idóneo para avanzar en las páginas de la obra.
3. La lectura programada del capitulado. Si bien pretendí ofrecer un índice temático que guíe al lector en la construcción del Abogado Digital, pudiere resultar más interesante el elegir otro tipo de orden de lectura a favor de su inquietud, por lo que propongo:

    a. **Para el funcionario jurisdiccional y abogado postulante**: es posible iniciar lectura en el Capítulo XII (*Valoración de la prueba cibernética e informática: Electrónica y digital),* seguido del Capítulo VIII (*El valor jurídico del Clic);* a continuación, recomiendo lectura al Capítulo XIII (*Delitos cibernéticos e informáticos).* Por último, invito a leer los capítulos I y III (*Patrimonio Digital y Jurisdicción en redes sociales,* respectivamente).
    b. **Para el abogado de empresa:** iniciar con el Capítulo VIII (*El valor jurídico del clic),* seguido del Capítulo I (*Patrimonio Digital*), después Capítulo V (*Explotación digital de los derechos de autor),* el Capítulo VI (*Programas de cómputo y sistemas de licenciamiento*), para concluir con los capítulos VII y III (*Mecanismos de autorregulación autoral en el ciberespacio* y *Jurisdicción en redes sociales,* respectivamente).
    c. **Para el abogado activista:** iniciar con el Capítulo XI (*Derechos Digitales),* seguido del Capítulo X (*Acceso a las tecnologías de la información y de la comunicación como Derecho Fundamental);* posteriormente, capítulos

VII y III (*Mecanismos de autorregulación autoral en el ciberespacio* y *Jurisdicción en redes sociales,* respectivamente); en seguida, el Capítulo IV (*Consecuencias Jurídicas de la creación y utilización de la Inteligencia Artificial)*, para finalizar con los parágrafos VI.3 y VI.4, que refieren al Software Libre y la comunidad *Creative Commons.*

d. **Para el Abogado Digital**: leer con atención cada capítulo en el orden que prefiera.

4. El perfil humano del Abogado Digital obliga que sea receptivo al diálogo, a pesar de la distancia, por lo que agradeceré cualquier crítica o replica que pudieran hacerme llegar a través del correo electrónico soy@jaimediazlimon.com. Sus observaciones y críticas en debate seguro aparecerán en próximas ediciones.
5. Optar por alternar entre el medio impreso y el digital para la lectura.
6. Comparar mi obra con otros autores y, en una segunda lectura, acudir a las fuentes que me permitieron construir Abogado Digital.
7. Que su completa atención se dedique a la lectura de los capítulos que sujeto a su consideración, pues es la herramienta más adecuada que me aproximará a convencerle. De otra forma, mi Obra se perdería en las distracciones y no lograré la convicción que pretendo con mis letras. En ese tenor, leer con paciencia, atención y dedicación, es el canal que me permitirá afectar su psique y apasionarle en el universo del Abogado Digital.

Prefacio y Agradecimientos

En noviembre de 2017, la *startup* Case Crunch con sede en el Reino Unido y con participación intelectual de estudiantes de Derecho de la Universidad de Cambridge, anunció los resultados de la competencia de una semana que lanzó con más de cien firmas legales reconocidas en Inglaterra y en la que se analizó setecientos setenta y cinco casos de incumplimiento de pagos de aseguradoras. En dicho concurso compitieron abogados de carne y hueso y un sistema que opera gracias a inteligencia artificial. Los resultados son alarmantes, ya que los abogados obtuvieron eficacia del 66.3% de éxito sobre su predicción en el destino de la reclamación de seguros, en tanto que los "robots" lograron un 86.6%. Adicionalmente, la inteligencia artificial que realizó el examen redujo en gastos y tiempo sus predicciones, sin requerir investigaciones o entrevistas con los demandantes.[1] Un par de meses en el pasado, una

[1] *EL FINANCIERO*. Redacción. "¿Te imaginas un abogado robot? Aquí te lo presentamos." TECH. México, 14 de noviembre de 2017. Visto el 24 de noviembre de 2017 a través del vínculo http://www.elfinanciero.com.mx/tech/los-robots-quieren-ganarle-a-los-abogados-y-lo-estan-logrando.html

de las firmas legales más poderosas en materia de finanzas y bancarrota, Baker & Hostetler, realizó la adquisición de la licencia no exclusiva sobre el robot, que opera con inteligencia artificial, llamado Ross.[2] Dicha tecnología fue diseñada sobre el código fuente de la plataforma Watson y es considerada un experto legal que permite crear argumentos sólidos con base en leyes, precedentes y doctrina, para determinar el probable éxito de un silogismo bien formulado ante los tribunales. Esta plataforma se lanzó al mercado con el eslogan: "Do more than humanly possible"; lo que pretende vender "abogados supercargados con inteligencia artificial". Si bien, IBM[3] —su desarrollador— insiste en que su objetivo no es la sustitución de abogados sino la implementación de mejores motores de búsqueda que permitan elegir argumentos bien formulados dentro del mar de posibilidades; no menos cierto es que algunos despachos jurídicos podrían pensar en la necesidad de optar por motores de búsqueda especializados frente a la contratación de estudiantes de derecho que acuden a dichas firmas con la única consigna de aplicar por primera vez el conocimiento que devoraron en las aulas universitarias. Después de todo, ninguno de nosotros, ¡podría hacer más allá de lo humanamente posible!

De esa forma, ¿cómo podríamos competir contra un motor de búsqueda inteligente, capaz de aprender y mejorar, de evolucionar y brindar respuestas breves, buenas y baratas en menor tiempo que cualquier estudiante de derecho? A parecer de quien escribe, la respuesta está en la capacitación extraordinaria, la especialización y el difícil reconocimiento sobre la desaparición de algunas fórmulas del derecho que se han desvanecido con el paso del tiempo y un par más que han sufrido modificaciones abismales con la única intención que éstas perduren al siglo XXI y al complejo universo de la red de redes.

Para los nativos digitales (*millennials* y generación Z) parecerá obvia su interacción con Tecnologías de la Información y la Comunicación que les permite comprender el mundo y realizar actos que generan trasceudencia en diversos ámbitos de su vida. Pocos de los miembros de esta generación conciben su vida sin un dispositivo tecnológico que resuelva su agenda, que les permita buscar restaurantes cercanos, tener acceso a redes sociales o bien poseer *zettabytes* de información en la palma de su mano. Empero, pocas veces realizan un examen adecuado sobre la operación cibernética que han realizado y las probables consecuencias sociales o jurídicas que ello trae consigo. Para esta generación, el "golpe de ratón", un clic, basta para emitir su opinión y manifestar su consentimiento o la ausencia del mismo para la celebración tácita de actos jurídicos que en todo momento afectan su esfera de derechos.

[2] http://www.rossintelligence.com/

[3] SILLS, Anthony. *ROSS and Watson tackle de Law*. Cognitive Enterprise. Watson. IBM. Enero 14 de 2016. Visto el 24 de noviembre de 2017 a través del vínculo https://www.ibm.com/blogs/watson/2016/01/ross-and-watson-tackle-the-law/

En ese tenor, adquiere importancia radical el concepto que Al Gore acuñara en 1993: *autopista de la información*. Y en justa medida lo es, pues la cantidad de información y el tráfico que se origina en la cibersociedad no permiten que las figuras tradicionales del derecho operen de forma adecuada y sería impensable que un ser humano tuviere en sus manos el análisis de cada metadato que se almacena en la red de redes para brindar la mejor solución legislativa a diversos comportamientos.

A pesar de lo anterior e independientemente de la generación que tenga el honor de representar cada lector, es indiscutible que la tecnología y el acceso a la vida digital resultan indispensables en la interacción social que vivimos en nuestros días, lo que da un peso radical a la vida *on line* sobre la *off line*. Así las cosas, el origen de la cibersociedad debe su fortaleza a la necesidad de los individuos por reflejar su comportamiento de una forma más ágil, adecuada y competitiva, inclusive respecto de nuestras propias creaciones, tal como he señalado en líneas anteriores.

El ciberespacio, red de redes o cibersociedad, ha gozado de apertura suficiente para que su crecimiento continúe, bajo un torpe y perezoso entendimiento legislativo que pretende regular las conductas que ocurren en el ámbito digital. Por principio, han sido los legisladores quienes han pretendido pactar normas de derecho positivo sobre la red, como si ésta fuera un sitio tangible, homogéneo e inmutable; ello ha llevado a diversos fracasos jurídicos que hasta nuestro día generan eco en movimientos sociales radicales[4] y el despertar en la curiosidad sobre millones de cibernautas que comienzan a preguntarse: "¿Qué es Internet, cómo funciona y cómo me afecta?" Incógnitas que han entusiasmado el interés de sociólogos, politólogos e inclusive psicólogos, sobre las repercusiones de la vida digital en el ser humano.

La división de la red en tres capas fundamentales:

i) **Internet**: la capa superficial que permite un acceso público y navegación abierta a los datos que se encuentran en la web.
ii) ***Deep Web***: parte inferior de la red, que ocupa la infraestructura y la tecnología de la capa superior para crear redes aisladas que contienen, en la mayoría de los casos, portales y foros que fomentan las conductas delictivas y que, adicionalmente, son de difícil rastreo y acceso ya que funcionan a través de navegación restringida.
iii) ***Dark Web***: la capa más profunda y poco explorada de la red, hasta ahora se conoce por los casos de persecución criminal (penal) que se han generado en el mundo y que han tenido como consecuencia el descubrimiento de redes

[4] Un claro ejemplo de la falta de comprensión de la red de redes, es el caso de la iniciativa de ley SOPA (Stop Online Piracy Act), misma que generó protestas fuera de Estados Unidos de América –país de origen- y permitió el surgimiento recalcitrante de Anonymous; movimiento que parecía perder presencia desde su origen en 2003.

criminales en las que se involucran altos funcionarios de gobierno y empresarios millonarios en casos de trata de blancas o narcotráfico. Ocupa una red privada, *peer to peer*, a través de conexiones dedicadas y de alto costo, ya sea a través de fibra óptica o líneas satelitales encriptadas.

Dichas capas han brindado un objeto de exposición a los estudiosos de la informática sobre Internet y han dictado un claro abandono para tratar de comprender las dos capas inferiores, no sólo por lo complejo de su construcción, sino por el difícil acceso a la misma. Desde el punto de vista jurídico, gran parte de los fracasos del derecho positivo se debe a que presumen que la ley logrará entrar a cualquiera de las capas de la red y regular el comportamiento de los usuarios, cuando la tendencia legislativa debería dirigirse a regular la primera capa (Internet) —con la comprensión de las libertades que brinda la cibersociedad— y erradicar las dos inferiores (*Deep* y *Dark Web*) por su naturaleza preponderantemente delictiva.

Se atribuye a Albert Einstein la frase: "Temo el día en que la tecnología sobrepase nuestra humanidad. El mundo sólo tendrá una generación de idiotas", y la presente obra se coloca a consideración del lector como un medicamento adecuado para combatir dicha predicción. Un conjunto de estudios sobre Derecho Cibernético, Derecho Informático y Derecho Digital que podrían despertar su curiosidad en afán de combatir cualquier probable ignorancia que poseemos sobre el dispositivo tecnológico que tenemos a nuestra disposición. En ese mismo tenor, humilde y humanamente, considero que este texto únicamente refleja dudas, inquietudes y probables soluciones jurídicas a la interacción del hombre con las máquinas integradas por circuitos y lo que ocurre una vez que el humano abandona su prisión de carne y hueso para disfrutar de la omnipresencia que brinda la red de redes. De tal suerte que *Abogado Digital* no pretende ser un tratado que destruya las nociones del derecho que hemos adquirido a lo largo de eones de progreso jurídico y millones de verdaderos expertos jurisconsultos que me preceden sino un libro de consulta que invite al abogado del siglo XXI, a abandonar la idea que la cibersociedad aún resulta una condición que la ciencia ficción debe retratar en las novelas y en la cinematografía y no debe ocupar la mente de un abogado que aspire a obtener respeto y reconocimiento en el gremio; por lo contrario, es mi leal intención generar inquietud sobre algunas consideraciones de hecho que me he enfrentado en mi breve experiencia en las ciencias jurídicas, tanto en la práctica profesional como en las aulas, en mi calidad de alumno y catedrático.

En afán de colocar en posición adecuada al lector, anuncio que gran parte del texto incluye derecho comparado e invoca tratados internacionales vigentes con la intención dolosa que el texto resulte claro y aplicable en diversas zonas geográficas y foros académicos varios; sin embargo, infiere algunos elementos particulares en la legislación mexicana.

Abogado Digital es un estudio jurídico sobre marcos normativos internacionales y la respuesta que estos brindan a inverosímiles hipótesis conductuales del

ciberespacio y cuyo origen digital complica su tratamiento legislativo. Por lo anterior, *Abogado Digital* enfoca su estudio en el análisis de las consecuencias de derecho en la utilización, creación y almacenamiento de tecnología y datos que se conciben gracias a ésta, desde una perspectiva multidisciplinaria, en estricto apego a las recieutes corrientes de Derecho Cibernético, Derecho Informático e Informática Jurídica, así como facultades consagradas en los reconocidos Derechos Digitales.

El primer capítulo (*Patrimonio Digital*) pretende resolver la naturaleza jurídica del patrimonio cuyo origen es de estricta naturaleza digital, así como el tratamiento que ha recibido en algunas legislaciones, no sólo desde el punto de vista normativo sino como fenómeno social que ha provocado la reacción de la Organización de las Naciones Unidas. En ese tenor, aborda la posibilidad de modificar el estricto concepto de patrimonio para que su flexibilización invite la permisibilidad de celebrar actos jurídicos cuyo objeto indirecto sea de naturaleza digital.

El segundo capítulo (*Testamento digital*) atiende de forma consecuente al complejo estudio del patrimonio digital y el destino de éste, una vez que fallece el usuario. Este concepto ya cuenta con tratamieuto uormativo en países como Francia y la jurisdicción catalana; sin embargo, aún resulta inaplicable para naciones que respetan el Derecho Notarial Latinoamericano y que consideran impermisible la celebración de transmisión póstuma de propiedad sin un acto protocolario y solemne. No obstante parece ser que las redes sociales y sus administradores han encontrado la vía legal adecuada para resolver la muerte digital de los cibernautas.

El tercer capítulo (*Jurisdicción en redes sociales*) es un análisis a precedentes judiciales que han aceptado jurisdicción sobre redes sociales, por considerar leonina la cláusula de "Renuncia de jurisdicción" que muchas de éstas poseen. Desde esta perspectiva, resulta de valor académico y profesional considerar el enfrentamiento del derecho positivo local contra las normas consuetudinarias que surgen de la interacción entre los cibernautas.

El cuarto capítulo (*Consecuencias Jurídicas de la creación y utilización de la inteligencia artificial*) tiene como objeto recordar la presencia de la robótica y la inteligencia artificial en nuestra vida diaria, así como la concepción de nuevas hipótesis normativas en atención al grado de responsabilidad que podría generar en desarrolladores, productores, fabricantes y usuarios; sin embargo, también pretende proponer escenarios en los cuales la subjetivización de las máquinas parece ser la única salida jurídica posible. En ese mismo sentido propongo una respuesta jurídica admisible para aquellos tratadistas de corte tradicional y para las nuevas generaciones de abogados que podrían apostar a la subjetivización de las máquinas, sobre todo en materia de derechos de autor.

El quinto capítulo (*Explotación Digital de los Derechos de Autor*) es la propuesta del autor sobre la flexibilización de figuras de orden análogo para permitir la regulación de los derechos de autor en el ciberespacio, máxime de la esfera de Derechos Morales que muchos tratadistas parecen dar por muertos, ante la infinita posibilidad

de reproducción que permiten los medios digitales y que complican su rastreo. En ese tenor, se sostiene la deconstrucción de conceptos del sistema subjetivo de derechos de autor y del *copyright* para entender los nuevos paradigmas autorales de la red de redes.

El sexto capítulo (*Programas de cómputo y licenciamiento*) pretende ser un manual a favor del abogado y los estudiosos en la materia, para la correcta celebración de contratos cuyo objeto indirecto sea un programa de cómputo, bases de datos y cualquier objeto autoral que permita la figura del licenciamiento. Asimismo, se brinda un estudio sobre las nuevas figuras de creación colaborativa y cómo es que éstas complican el respeto de cualquier sistema de protección autoral.

El séptimo capítulo (*Mecanismos de autorregulación autoral en el ciberespacio*) es la propuesta del autor, a favor del usuario, para resolver de forma ágil las controversias que se suscitan dentro de las redes sociales, derivado de los brillantes mecanismos de autocomposición que han estructurado estos, en apego a normas como la *Digital Millennium Copyright Act* y sistemas de autorregulación como el Content Id y Rights Manager.

El octavo capítulo (*El valor jurídico del clic)* recuerda al estudioso de la ciencia jurídica, los derechos y obligaciones que se adquieren con el "golpe de ratón", no sólo ante las redes y sus administradores, sino ante aparatos gubernamentales, derivado del reconocimiento que algunos países han otorgado al clic. Adicionalmente, brinda un amplio panorama a la respuesta de las Naciones Unidas sobre el comercio electrónico, así como la perene figura de la fe financiera impresa en criptomonedas que los Estados no suelen regular.

El noveno capítulo (*Protección a la Propia Imagen y Datos Personales en redes sociales*) es la guía que debe conocer cualquier usuario de redes sociales en lo referente a la protección de Derechos Personales de carácter sensible, según la escala de Derechos Fundameutales. Además, pretende ser un recordatorio a los juristas sobre las vías legales que pudieren existir en sus marcos normativos, no sólo como una salida accidental sino como respuesta paralela a las violaciones que pueden sufrir los cibernautas por el indebido uso de su imagen y sus datos personales, en Internet.

El décimo capítulo (*Acceso a las tecnologías de la información de la Comunicación como Derecho Fundomental*) es la respuesta jurídica a la indebida apreciación de algunos Estados y estudiosos de la materia, que pretenden confundir el Derecho Humano de Libertad de expresión con el derecho que algunas naciones han reconocido y que facilitan a sus ciudadanos: el acceso a nuevas tecnologías y altas velocidades de conectividad. Asimismo, pretendemos definir —para el abogado— el concepto de *Big Data* y los alcances jurídicos que esa información podría poseer.

El décimo primer capítulo (*Derechos Digitales*) propone el estudio de facultades de aplicación digital, así como la carga que deben soportar los Estados para beneficiar el ejercicio de éstas. Asimismo, brinda el estudio de las prerrogativas que han tenido una mejor recepción en la jurisprudencia internacional.

El décimo segundo capítulo (*Valoración de la Prueba Cibernética e Informática: Electrónica y Digital*) es un estudio de carácter procesal que rescata el comportamiento legislativo —nacional e internacional— respecto de la generación, la conservación, la incorporación y la valoración de las pruebas de naturaleza cibernética, informática, electrónica y digital. Asimismo, invita a la deconstrucción de la sinonimia en pruebas de orden tecnológico, en afán de comprender de mejor manera la aplicación de principios internacionales y técnicas de conservación forense.

Por último, el décimo tercer capítulo (*Delitos cibernéticos e informáticos*) respeta el criterio expuesto en el capítulo anterior y pretende diseminar la confusión entre ambas figuras, sobre todo, en países de habla hispana. Por otro lado, brinda un amplio catálogo de legislaciones que han ocupado su estudio a figuras típicas, antijurídicas y antisociales que se hubiesen cometido con medios cibernéticos e informáticos, así como aquéllos cuya comisión es de estricta naturaleza digital.

Debo agradecer al Doctor Jesús Parets Gómez —actual Director del Registro Nacional del Derecho de Autor del Instituto Nacional del Derecho de Autor— quien despertó mi curiosidad académica sobre la compleja materia del Derecho Informático, misma que ahora pretendo compartir con la presente obra.

Esta búsqueda e inquietud me permitió iniciar mi actividad docente en la Facultad de Derecho de la Barra Nacional de Abogados para impartir la clase de Derecho Informático. Ese capítulo en mi preparación docente me obligó a devorar los pocos libros sobre la materia que existen en el país y buscar otros tantos respetables alrededor del ciberespacio; sin embargo, fue el libro *Derecho Informático*[5] el que realmente se convertiría en mi manual de consulta.

En ese mismo tenor, ha sido la oportunidad que me brindara la academia, la experiencia profesional y mi Maestro, el Doctor Parets, los que han fortalecido mi apetito sobre el Derecho de Propiedad Intelectual, por lo que en este breve texto encontrará estudios poco convencionales sobre el universo de derechos de autor, sobre todo, aplicados al Derecho Cibernético y Digital.

El camino de estudio para atreverme a presentarles este resultado se acompaña de años de colecciones, discusiones y foros que permitieron formar a esta obra literaria, por lo que es prudente agradecer a la *Revista Foro Jurídico*[6] —y a su Directora, la Maestra Janet Huerta Estefan— por los años de confianza que me han permitido perfeccionar, hasta donde me fue posible, las reflexiones que ahora profundizo sobre el presente libro, las bohemias charlas sobre tecnología, las tertulias cibernéticas y cada semilla de duda que hemos sembrado juntos parecen rendir frutos a través de

[5] Puede consultar la obra del Doctor Julio Téllez, a través del vínculo https://biblio.juridicas.unam.mx/bjv/detalle-libro/1941-derecho-informatico Visto el 24 de noviembre de 2017.

[6] Revista Jurídica Especializada impresa y digital, en la cual tengo el honor de coordinar la columna de Propiedad Intelectual. Puede consultar el contenido en línea de ésta, a través del vínculo https://www.forojuridico.org.mx/

la presente obra, y la gratitud me dicta mencionar a la Maestra Huerta en esta breve introducción. En ese mismo tenor, debo gratitud máxima al Magistrado Fernando Córdova del Valle, quien invirtió severas horas de estudio de la presente obra, antes que viera la luz; a él debo agradecer el rigor de su revisión antes de sujetar la presente obra a la consideración pública.

Institucionalmente, rindo honores a la Universidad de la Amazonia (Florencia, Caquéta, Colombia), la Universidad del Externado de Bogotá (Colombia) y la Universidad Nacional de la Plata (Buenos Aires, Argentina), que dictaron las pautas para que disertara con éxito un par de conferencias en sus aulas y abrieran un espacio a mis letras en sus publicaciones indexadas, respectivamente; participaciones que me obligaron a perfeccionar mi conocimiento respecto algunos temas que también podrá encontrar en este resultado literario. Sobre el texto podrá encontrar los vínculos que dirigen a aquellas primeras aproximaciones a la materia, que ahora pretendo perfeccionar mediante el presente texto.

Por consecuencia, es prudente expresar mi respeto y gratitud a cada uno de los casi tres mil alumnos que he tenido el honor de pervertir hacia el complejo universo del *Abogado Digital* en: la Universidad Autónoma Metropolitana Azcapotzalco, Universidad Tec Milenio, Universidad Tecnológica, Universidad Latinoamericana, Universidad de la República Mexicana, Universidad de Londres, Facultad de Derecho de la Barra Nacional de Abogados (en la cual tuve el honor de construir la asignatura de Derecho Informático, a nivel licenciatura, gracias a la confianza de mi querida amiga, Licenciada Dulce López Olmos), Barra Interamericana de Abogados, Universidad Ius Semper y la Universidad de la Amazonia; así como a sus autoridades.

Estoy convencido que el mejor espacio para destruir las ideas, construirlas de nuevo y lograr un mejor resultado, es el aula universitaria. Esta premisa la aprendería de mis tres grandes Maestros, cuando aún era un profano del Derecho: *i)* Agustín Pérez Carrillo, de quién aprendí a cuestionar absolutamente todo, inclusive al experto que se colocaba detrás del escritorio, dudar de lo aprendido y de mí mismo si era necesario, con el afán de siempre regresar a la biblioteca para aprender a dudar mejor. "Eusayo, error, ensayo, error, ensayo, hasta que te quedes con el mejor de tus errores", siempre fue su lema; de él también hurte la fascinación por el modelo *Toulmin*[7] de argumentación, bajo el que se construye la presente obra, siempre que fue posible; *ii)* Gregorio Miguel Valdés Garibay, de quién aprendí que debes darlo todo, tu energía, tu conocimiento, tu paciencia y tu amor por la ciencia jurídica, sin importar lo

[7] Sobre el modelo de Argumentación Toulmin, sugiero la siguiente lectura. Muy amigable para un primer lector: http://www.revista.unam.mx/vol.5/num1/art2/ene_art2.pdf Visto el 24 de noviembre de 2017 (BELLO, Luisa Isabel. *Modelo Argumentativo de Toulmin en la escritura de artículos de investigación educativa.* Revista Digital Universitaria. Volumen 5. Número 1. Universidad Nacional Autónoma de México. 21 de enero de 2004.)

que esté pasando fuera del aula; a él agradezco que aprendí a compartir, sin importar la condición de mi auditorio o lector, sin importar, inclusive, mi condición para tratar de hacerlo; *iii)* Luis Alfredo Brodermann Ferrer, de quien aprendí que los libros, la doctrina y la teoría resultan igual o más importantes que la experiencia práctica, sobre aquéllos que simplemente desean aprender nuestra bella ciencia jurídica sólo con aparecer en un tribunal con media noción sobre sus horarios, reglas, nombres de los funcionarios y sus procedimientos. A él le debo mi amor por la academia y demostrarme que el horizonte del Derecho debe llegar más lejos de las aulas, de otro modo, el conocimiento moriría en el cuaderno gastado de algún alumno, y *iv)* Mi aprecio y admiración merece la Doctora Lizbeth Xóchitl Padilla, quien ha depositado su confianza en mi primera obra al prologarla, no sólo por la amistad que guardamos sino por la indudable influencia y motivación que me sirvió para permitirme concluir la misma: ¡Gracias, Doctora!

En la justa medida, cada profesor, docente, alumno, autoridad académica y Maestro, me ha permitido construir la máxima: "El conocimiento sólo es útil en la medida en que se comparte. De otra forma, resulta inútil y muere con su autor". Misma que he puesto en práctica en la construcción de la presente obra y la podrá encontrar impresa en cada página.

Las horas que he invertido en la construcción de la presente obra han sido aquellas que he visto a mi familia dormir y esperar paciente en la habitación; algunas veces la madrugada me vencería y tendrían que pasar varias noches sin pisar mi recámara. A ellos debo rendir el máximo honor, junto a dios, por permitir la culminación de este sueño literario, gracias a su prudente tolerancia para este sueño académico y profesional. ¡Gracias a mis dos angelitos, a mis dos amores, Nancy y Emiliano, que dormían, mientras este loco soñador aún plasmaba sus letras!

Por último, aprecio la confianza que usted, el lector, ha depositado en este insipiente escritor, por lo que pretendo corresponder a su consideración, al colocar en sus manos la mejor obra literaria y académica que los años de investigación me han permitido concebir; bajo la noción que este conocimiento adquirido, debe compartirse con usted y el mundo jurídico entero.

Gracias, ¡abogados digitales!

Jaime Limón / Abogado Digital
El conocimiento sólo es útil, en la medida en que se comparte
Agosto de 2018

I
CAPÍTULO

Patrimonio Digital[1]

I. 1 Patrimonio Digital Latu Sensu

En el desarrollo del capitulado de la presente obra podrá encontrar la deconstrucción de diversos conceptos que, a saber de los expertos en la materia, podrían considerarse indiscutibles y axiomas inamovibles en la enseñanza de los mismos; sin embargo, el progreso tecnológico en la era de la información ha invitado a buscar que estos conceptos se reconstruyan o bien se flexibilicen en afán de sobrevivir a los cambios incesantes que ocurren en la vida *on line*. Ejemplo de lo anterior recae sobre el concepto de *patrimonio*, que en sus diferentes teorías ha encontrado uu debate interminable sobre todo en el mundo del derecho civil, sin embargo, por ahora nos ajustaremos al concepto que nos brinda José Alfredo Domínguez Martínez: "[...] en términos generales, es el conjunto de bienes, derechos y obligaciones correspondientes a una persona, con contenido económico y que constituyen una universalidad jurídica"[2] (Teoría Clásica).

Este concepto —y teoría— que se ajusta de forma adecuada a la realidad jurídica que nos enfrentamos en la vida *off line*, sin embargo, en la vida *on line* existe el hueco dogmático que yace sobre todo aquello que se genera en Internet, pues al

[1] Obra versionada del artículo denominado "Patrimonio Digital", que se publicó en la *Revista Derechos en Acción*, primavera 2017. ISSN 2525-1678, de la Universidad Nacional de la Plata, Buenos Aires, Argentina. Visible a través del vínculo https://revistas.unlp.edu.ar/ReDeA/article/view/4083/4034

[2] DOMÍNGUEZ MARTÍNEZ, José Alfredo. *Derecho Civil, parte general, personas, cosas negocio jurídico e invalidez*. Editorial Porrúa. Edición 11. Página 215, México, 2008.

parecer de los diversos cuerpos normativos (tanto en Derecho Nacional como en Derecho Comparado) no es prudente hablar de patrimonio digital desde la perspectiva de derecho privado, de acuerdo al término de patrimonio que nos brinda Domínguez Martínez.

La aproximación más cercana que existe sobre regulación del patrimonio digital lo encontramos en la *Carta Sobre la Preservación del Patrimonio Digital*[3] en la cual se acuña el término desde la perspectiva del Derecho internacional público, lo que a parecer de este autor, genera un antecedente inigualable para analizar este concepto desde el punto de vista del derecho privado y analizar su composición en la particularidad de los individuos. Así las cosas, en la Carta de referencia, se percibe la preocupación de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, sobre la posible y muy probable desaparición del patrimonio que se origina en Internet.

En primer lugar, parten de la máxima que la desaparición de cualquier forma de patrimonio empobrece el acervo de todas las naciones, y en segunda posición, la UNESCO considera que la inestabilidad de Internet es un riesgo latente para la información y conocimiento acumulado en formato html, es decir, que la información digital está expuesta a la obsolescencia técnica y el deterioro físico. Así las cosas, UNESCO tiene presente la probable desaparición del "patrimonio digital", como si éste fuere una especie en peligro de extinción y proclamó que las naciones debían unir esfuerzos para que generaciones actuales y futuras tengan acceso a este acervo cultural. En tales términos el artículo primero de esta Carta, dicta:

El patrimonio cultural como herencia común

Artículo 1- Alcance. El patrimonio digital consiste en recursos únicos que son fruto del saber o la expresión de los seres humanos. Comprende recursos de carácter cultural, educativo, científico o administrativo e información técnica, jurídica, médica y de otras clases, que se generan directamente en formato digital o se convierten a éste a partir de material analógico ya existente. Los productos "de origen digital" no existen en otro formato que el electrónico.

Los objetos digitales pueden ser textos, bases de datos, imágenes fijas o en movimiento, grabaciones sonoras, material gráfico, programas informáticos o páginas Web, entre otros muchos formatos posibles dentro de un vasto repertorio de diversidad creciente. A menudo son efímeros, y su conservación requiere un trabajo específico en este sentido en los procesos de producción, mantenimiento y gestión.

[3] UNESCO. *Carta sobre la preservación del patrimonio digital*. 15 de octubre de 2003. Versión en español que se puede consultar a través del portal http://portal.unesco.org/es/ev.php-URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html . Consultado el 29 de mayo de 2017.

> Muchos de esos recursos revisten valor e importancia duraderos, y constituyen por ello un patrimonio digno de protección y conservación en beneficio de las generaciones actuales y futuras. Este legado en constante aumento puede existir en cualquier lengua, cualquier lugar del mundo y cualquier campo de la expresión o el saber humanos. [4]

La primera distinción que es prudente analizar del bello párrafo que nos brinda la UNESCO es el doble origen que podría existir sobre el patrimonio digital. Esto es, tenemos los recursos que se han generado en formato digital y que no existen de forma material, más allá de lo que conocemos en la red de redes, por otro lado, contamos con los recursos de origen tradicional y que han sufrido una transformación digital, sin que necesariamente implique la desaparición del formato analógico (tradicional). La segunda disección que es prudente realizar sobre el primer artículo de la Carta es que, a pesar de la creencia popular de la "infinita" estabilidad de los recursos digitales, es sabido que estos también pueden desaparecer y, en algunas raras ocasiones, con mucha mayor velocidad que los recursos analógicos. Es decir, es inverosímil afirmar que Internet tiene memoria perpetua, dado que si bien es cierto el origen digital de los mismos permite un mejor almacenamiento, distribución y reproducción, no debemos dejar fuera aquellas plataformas o dispositivos que están diseñados con "memoria temporal selectiva", tal como los archivos temporales (*cookies*) de navegación o aplicaciones cómo lo son Snapchat.

Hasta este punto, quizá no logré convencer a mi lector de la relevancia sobre la protección del patrimonio digital, sin embargo, en el año 2013, la empresa de tecnología y desarrollo CISCO emitió una infografía sobre las estimaciones de cantidad de recursos, datos e información que existía en Internet. A saber, nos dejó clara la desaparición de medidas tradicionales de almacenamiento de información para comenzar a hablar sobre Petabyte, Exabyte, Zettabyte y Yottabyte:[5]

[4] Op. Cit. 16

[5] CISCO. *Visual Networking Index (VNI) IP Traffic Chart*. Consultada en línea a través del vínculo http://www.cisco.com/cdc_content_elements/networking_solutions/service_provider/visual_networking_ip_traffic_chart.html el pasado 31 de mayo de 2017. Es importante destacar que, para este estudio la compañía tomó como referencia la base de estimaciones hasta 2006 realizada por la *University of Pennsylvania School of Medicine,* los datos del profesor Roy Williams, expuestos en su artículo "Data Powers of Ten", del año 2000, y el resto se reprodujo de las opiniones expertas emitidas en el VNI 2013.

Término de Tráfico	Es Equivalente a	¿A cuánto equivale?
1 Petabyte	1 000 Terabytes o 250 mil DVD's	480 Terabytes significan una biblioteca digital con todos los libros catálogos del mundo en todos los idiomas
1 Exabyte	1 000 Petabytes o 250 millones de DVD's	5 exabytes son equivalentes a la transcripción de todas las palabras alguna vez habladas. **400 exabytes** es la cantidad de información que cruzó en Internet, sólo en el año 2012
1 Zettabyte	1 000 Exabytes o 250 billones de DVD's	Es equivalente a la cantidad de información que ha cruzado Internet desde su creación
1 Yottabyte	1 000 Zettabytes o 250 trillones de DVD's	20 Yottabytes equivalen a una fotografía instantánea de la superficie entera del planeta Tierra

Entre otras estadísticas de la compañía CISCO, destacan las que compiló en junio de 2016 en el marco del *Cisco Visual Networking Index (VNI)*, en la que afirma que para el año 2020: *i)* tomaría más de 5 millones de años mirar la totalidad de videos que se han subido a Internet; *ii)* el número de dispositivos conectados a la red superarán en más de tres veces la cantidad total de población humana; y *iii)* La información que para el año 2016 hubo superado el primer Zettabyte, se triplicaría y alcanzaría, al menos los 2.3 Zettabytes.[6] En ese tenor, la Comisión de Ciberseguridad de la Organización de Estados Americanos, a través de *IHS Markit Technology*, afirma que para el 2020 habrá más de 50 millones de dispositivos conectados a Internet (lo que incluye "Internet de las Cosas/IoT").

Si a estos parámetros incluimos que en realidad la tendencia de creación y almacenamiento hoy en día se realiza preferentemente en Internet, descubriremos que estamos en un punto medular en la construcción de historia y antropología moderna; para sustentar lo anterior, invocaré el estudio que realizó la Asociación de Internet MX (otrora Asociación Mexicana de Internet) en colaboración con INFOTEC, en el que destaca que los cibernautas mexicanos comienzan a interactuar en la red a partir de los 3 años y que la cultura de los Estados Unidos Mexicanos es permanecer al menos 8 horas del día conectado a la web, preferentemente a redes sociales como lo

[6] CISCO. *The Zettabyte Era-Trends and Analysis*. Documento que forma parte del CISCO® Visual Networking Index (VNI). Consultado en línea el 31 de mayo de 2017 a través de http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

son Facebook y Youtube. [7] Estos datos no son números aislados de la realidad y que reflejan el interés de otras latitudes, toda vez que, si se advierte que los mexicanos pasamos el 50% de nuestro día productivo en línea, así como lo hacen ciudadanos de otras partes del mundo, esto también implica que el tráfico de datos que ocurre, así como el nivel de creación, es superior, inclusive, sobre lo que se realiza en recursos analógicos.

Bajo esta premisa mayor, la UNESCO comprendió la problemática y la formuló ante las naciones involucradas: ¿qué haríamos si Internet, de pronto, decide que toda la información que hasta ahora se ha almacenado debe desaparecer? Indiscutiblemente ello traería aparejada la desaparición de miles de exabytes que acreditan el paso del hombre por la Tierra. Nuestros antepasados lucharon por dejar en medios analógicos su historia, su progreso y su aportación a la humanidad, ya que no siempre contaron con los mejores mecanismos para brindar evidencia del proceso de creación que atravesaron para llegar al puerto de destino; tallarlo en roca, madera, inclusive en papel, ahora parece absurdo cuando se tiene al alcance de un golpe de ratón, Internet y las TIC, empero, esto no hace que este medio de almacenamiento sea igual de efímero e inestable que otra —anterior— forma de comunicación creada por el hombre. En caso que Internet y los datos en él almacenados hasta el día de hoy desaparecieran, implicaría llevarse consigo la historia de la humanidad y su evolución al menos de los últimos lustros. Así lo sostuvo la organización de referencia en el artículo 3° de la Carta, a saber:

> **Artículo 3 - El peligro de pérdida**
> El patrimonio digital del mundo corre el peligro de perderse para la posteridad. Contribuyen a ello, entre otros factores, la rápida obsolescencia de los equipos y programas informáticos que le dan vida, las incertidumbres existentes en torno a los recursos, la responsabilidad y los métodos para su mantenimiento y conservación y la falta de legislación que ampare estos procesos.
>
> Los cambios en las conductas han ido a la zaga del progreso tecnológico. La evolución de la tecnología digital ha sido tan rápida y onerosa que los gobiernos e instituciones no han podido elaborar estrategias de conservación, oportunas y bien fundamentadas. No se ha comprendido en toda su magnitud la amenaza que pesa sobre el potencial económico, social, intelectual y cultural que encierra el patrimonio, sobre el cual se edifica el porvenir.[8]

[7] Asociación de Internet.Mx/ INFOTEC. 13° Estudio sobre los hábitos de los usuarios de Internet en México 2017. Mayo 2018. Consultado en línea 31 de mayo de 2017 a través del vínculo https://www.infotec.mx/work/models/infotec/Resource/1012/6/images/Estudio_Habitos_Usuarios_2017.pdf.

[8] UNESCO *Op. Cit.* 2

I. 2 Patrimonio Digital *Strictu Sensu*

Con independencia del temor globalizado que ha establecido UNESCO, la preocupación que enfrentamos los particulares, alejados tanto del concepto de patrimonio digital (*latu sensu*) como de las intenciones de conservación a los que hace referencia la Carta sobre la preservación del patrimonio digital, es que ésta se desvía de la protección de los bienes y derechos de los particulares, sobre todo si estos son considerados con bajo mérito cultural para que resulte digna su protección para la posteridad. Así lo sostiene, *a contrariu sensu*, la propia declaratoria, cuyo texto literal prescribe:

> **Artículo 7 - Seleccionar los elementos que deben conservarse**
> Al igual que ocurre con el conjunto del patrimonio documental, los principios de selección pueden diferir de un país a otro, aun cuando los principales criterios para determinar los elementos digitales dignos de conservación sean su significado y valor duraderos en términos culturales, científicos, testimoniales o de otra índole. Indudablemente, se deberá dar prioridad a los productos "de origen digital". Los procesos de selección y de eventual revisión subsiguiente han de llevarse a cabo con toda transparencia y basarse en principios, políticas, procedimientos y normas bien definidos.[9]

Fundamento que permite evidenciar la hipótesis sostenida en el presente capítulo, ya que parecería que los Estados tienen un poder absoluto para determinar qué elementos digitales son dignos de conservarse —bajo un subjetivo análisis gubernamental—; siendo el único criterio objetivo el "origen digital" que estos deben tener para ser considerados aptos para esta arca de Noé digital. Quizá se podría debatir el punto de vista que coloco en manos del lector, bajo la noción que los Estados se encuentran obligados a determinar principios, políticas y procedimientos para el alnacenamiento de referencia, empero, hasta hoy en día no existen normas que en derecho positivo permitan identificar las obras o recursos que alcanzarán el mérito solicitado. Sin conceder oportunidad al anterior argumento, cabe destacar que esto inclusive resulta violatorio de Derechos Humanos si es que se sostiene la revisión de Derechos de Autor sobre los recursos creados; ya que la legislación de los diversos Estados que se encuentran adscrito al Convenio de Berna, que administra la Organización Mundial de la Propiedad Intelectual, no permiten la valoración "subjetiva" de las entidades encargadas de la protección de las prerrogativas a favor de los autores, más allá de considerar si ésta es original y se fijó en un soporte material o electrónico susceptible de reproducción.[10]

[9] UNESCO. *Op. Cit.* 2

[10] Así lo sostiene el artículo 5° del Convenio de Berna, cuyo inciso 2) sostiene que el goce y el ejercicio de los derechos reconocidos por el propio Convenio y la legislación de cada país, no se podrá

La tesitura sostenida por la UNESCO resulta confusa y excluyente bajo las razones de derecho expuestas, máxime si sometemos a consideración de esta organización, el patrimonio digital particular que se hubiese generado y que, a saber de las entidades gubernamentales no cuenta con el mérito suficiente para ser susceptible de la protección que sugieren las naciones. Tal parecería que un examen subjetivo y burocrático podría borrar de la historia humana, el patrimonio que los individuos generan en Internet de forma consuetudinaria, en perjuicio de los individuos. A consideración del lector, quisiera compartir algunas reflexiones sobre Patrimonio Digital en Sentido Estricto, mismas que permitirán fortalecer la hipótesis sostenida.

I. 2.1 Datos Biométricos

El diccionario de la Real Academia Española define a la *biometría* como el estudio mensurativo o estadístico de los fenómenos o procesos biológicos, sin embargo, me gustaría invocar el concepto de *biometría informática* que acuñó la compañía multinacional Aware Inc., que indica que la biometría es la autenticación física y lógica de las personas en controles de acceso, así como el reconocimiento casi en tiempo real de sospechosos de un control fronterizo; asimismo, precisa que la biometría persigue tres fines fundamentales: 1) verificación, 2) identificación y, 3) control de duplicados. Derivado del mismo estudio, la compañía Aware Inc., precisa que los datos biométricos: "[…] se refieren a las características físicas (y conductuales) más propias de cada uno, que pueden ser detectadas por dispositivos e interpretadas por computadoras de modo que pueden usarse como nuestros representantes en el ámbito digital".[11]

Desde el punto de vista normativo, el Reglamento Europeo de Protección de Datos (2016/679 *General Data Protection Regulation*) los define como los "datos personales que resulten del procesamiento técnico específico relacionado con las características físicas, psicológicas o conductuales de una persona física, que permite o confirma la identificación única de una persona natural, cómo lo son la imagen

subordinar a ninguna formalidad. Máxime que el propio Convenio, en su artículo 1°, prescribe que se considerará "original" cualquier obra de las catalogadas por dicho Tratado Internacional. Es decir, que la originalidad de la obra se concederá en atención de la calidad de la creación que se ostente como obra, único elemento de discreción permitido por la materia, sin que sea permisible la aplicación de criterios administrativos que pudieren condicionar el ejercicio de derechos de autor, derivados de la obra. Puede consultar el texto íntegro del Convenio de Berna, vigente a partir del año 1984, derivado del Acta de París del 24 de julio de 1971, a través del vínculo http://www.wipo.int/treaties/es/ip/berne/ Consultado en línea el 01 de junio de 2017.

[11] AWARE. ¿Qué es la biometría?- Documentos Informativos. Aplicaciones biométricas. Consultado en línea el 01 de junio de 2017, a través del vínculo https://www.aware.com/es/que-es-la-biometria/aplicaciones-biometricas/

facial o datos dactiloscópicos".[12] Esto permite generar una base de datos que vincula al usuario con una serie de datos personalísimos, que le brinda verificación, identificación y control para el acceso a plataformas y ejecución de procesos.

Hasta este punto, se presentan tres niveles de utilización de los datos biométricos. En primer lugar, tenemos la verificación, que consiste en realizar comparación biométrica entre los nuevos datos proporcionados por el usuario que pretende tener acceso a un equipo, aplicación informática o base de datos y el dato biométrico anteriormente proporcionado y que se señaló como referencia autorizada de acceso; el dato biométrico sustituye el *password* o PIN, de tal suerte que si el nuevo dato biométrico coincide con el que se encuentra almacenado en el equipo (base central o teléfono inteligente); la comparación que se ejecuta en este tipo de procesos es conocida como "uno a uno". La identificación biométrica opera de manera similar, sin embargo, la comparación del nuevo dato biométrico no ocurre sobre una plantilla única almacenada, sino que la equivalencia se realiza sobre una base de datos estructurada; gubernamentalmente, estos datos no permiten el archivo tradicional y su tratamiento suele ser en calidad de *Big Data* (según dicho término se define en el capítulo X de la presente obra); es decir, en el proceso de identificación se aplican más de un dato biométrico y a su vez, estos son analizados y comparados —mediante procesos lógico matemáticos— a una base de datos centralizada que permite definir si el usuario que se pretende autenticar, es la persona que dice ser; a esto se le llama *comparación "uno a muchos"*. Por último, el control de duplicado consiste en la comparación de bases de datos —biométricos— con otras bases, en afán de eliminar la duplicidad de usuarios y evitar posibles fraudes digitales.

La utilización de datos biométricos para operar equipos de alta tecnología se encontraba reservada para empresas y grandes corporativos, sin embargo, la individualización, disminución de costos y la reducción de la tecnología permitió que cualquier propietario de un teléfono inteligente contara con esta herramienta en sus manos, así también, debió alimentar su equipo o algún servidor central con la información biométrica suficiente para lograr acceder al mismo, sin que, en muchos de los casos conozcan cómo es que se resguarda esa información por los fabricantes del hardware o los desarrolladores del software.

Sin embargo, algunas compañías ya han comenzado a mostrar interés en el blindaje de los datos que se almacenan en los equipos telefónicos particulares o bien, que se generan a través de estos, tal es el caso de *Samsung* quién lanzó una gama de productos de seguridad de datos llamados *Device Encryption* y *On Device Encryption,*[13]

[12] COUNCIL OF THE EUROPEAN UNION. *General Data Protection Regulation.* Bruselas, 6 de abril de 2016. Visto el 13 de diciembre de 2017 a través del vínculo http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

[13] SAMSUMG. Soluciones para dispositivos Móviles. Encriptación de datos. Consultado el 01 de junio de 2017 a través del vínculo http://www.samsung.com/es/business/solutions-services/mobile-solntions/security/encryption

que ofrecen seguridad tanto a empresas como a particulares, para proteger los datos sensibles que pudieran vulnerarse.

Desde la panóptica jurídica, la Ley Federal de Protección de Datos Personales en Posesión de Particulares (México, 2010) reviste suma importancia a los datos personales, especialmente a aquéllos de carácter sensible, mismos que se definen en el artículo 3, cuyas fracciones V y VI a la letra indican:

> Artículo 3.- Para los efectos de esta Ley, se entenderá por:
> [...]
> V. Datos personales: Cualquier información concerniente a una persona física identificada o identificable.
> VI. Datos personales sensibles: Aquellos datos personales que afecten a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. En particular, se consideran sensibles aquéllos que puedan revelar aspectos como origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia sexual [...][14]

La aproximación legal que se invoca, nos permite comprender que los datos biométricos son de naturaleza sensible y constituyen parte del patrimonio digital que de forma voluntaria o involuntaria generan los usuarios en Internet. Independientemente de su fuente volitiva, existe obligación de los fabricantes y desarrolladores de software, de indicar el fin del almacenamiento de los datos biométricos, así como la forma en que serán almacenados.

I. 2. 2 Datos personales

En seguimiento a la cadena de protección que debe existir en los dispositivos de comunicación, hay un nivel menos complejo aunque igual de sensible que los datos biométricos; hablamos del nombre, iconografías de nuestra propia imagen, usuarios y datos generales de identificación como lo podrían ser edad, sexo, religión, preferencia política, filosófica o moral, así como los *nickname*, *user name* y contraseñas (*password*) que solicitan las plataformas para iniciar la navegación en cualquiera de sus modalidades.

[14] CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Expedida el 05 de julio de 2010. Se puede consultar el texto íntegro de la ley, a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Tal como se indicó con anterioridad, los cibernautas invierten una gran cantidad de horas productivas en Internet y del tiempo conectados, mayormente se disfruta la navegación en redes sociales como Facebook, WhatsApp, Twitter o Youtube.[15] Específicamente, el 97% de los usuarios mexicanos navegan en la web para acceder a la red social denominada Facebook, por lo cual se advierte que se genera a cargo de esta plataforma responsabilidad de tratamiento sobre los datos personales que pudiere generar consecuencias de derecho. A efecto de lo anterior, invocaremos el concepto de Base de Datos, Encargado, Responsable y Tratamiento de la Ley Federal de Protección de Datos Personales:

> Artículo 3.- Para los efectos de esta Ley, se entenderá por:
> [...]
> II. Bases de datos: El conjunto ordenado de datos personales referentes a una persona identificada o identificable.
> [...]
> IX. Encargado: La persona física o jurídica que sola o conjuntamente con otras trate datos personales por cuenta del responsable.
> [...]
> XIV. Responsable: Persona física o moral de carácter privado que decide sobre el tratamiento de datos personales.
> [...]
> XVIII. Tratamiento: La obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

Si para ello somos meticulosos, resulta necesario hacer una revisión a las políticas, términos y condiciones de cada una de las redes sociales en las cuales tenemos acceso, así como del propio buscador Google que ha determinado reglas generales para aquéllos que ocupen sus servicios, así como lo de sus plataformas filiales. Al respecto, realizaremos las consideraciones necesarias en el capítulo respectivo dentro de la presente obra.

En términos generales, se advierte que no sólo los mecanismos que permiten a las plataformas identificar a la interfaz humana mediante elementos legalmente reconocidos, son los considerados datos personales, sino que esto también pudiere englobar nombres de usuario y contraseñas —inclusive bancarias— entre los datos personales de carácter sensible pero de naturaleza digital. Datos que hoy en día poseen un valor económico en el *black market* y *deep web* por las infinitas posibilidades ilícitas de su mala utilización. Hipótesis que no resulta un mal episodio de *Black Mirror*, pues según el sitio especializado *TOP 10 VPN*, sólo se requiere la inversión de cerca de 1

[15] *Op. Cit.* 6

200 dólares para tener acceso ilegal de la información personal de los usuarios, sus cuentas y finanzas; de esa forma, en la *Deep Web,* se podría solicitar el hackeo de las cuentas de Uber, Airbnb y Netflix por el monto de diez dólares, en tanto que documentación oficial como pasaportes y biométricos se podrían adquirir por un poco más de noventa dólares americanos. A pesar que este índice representa un estudio sobre el comportamiento de los hackers americanos, resulta deplorable imaginar que los precios suelen ser mucho más bajos en países en vías de desarrollo, como México, en dónde tres mil pesos mexicanos permitirían la compra total de toda la reputación y patrimonio digital. [16]

I. 2. 3 Identidad y Reputación Digital

El Maestro Francisco José Santamaría Ramos, de la Universidad Complutense de Madrid, reconoce que la "existencia paralela entre la vida física y la vida virtual genera que las personas físicas y jurídicas deban producir lo que hoy se conoce como *identidad digital*, que deriva en la *reputación digital*".[17] Sin embargo, han sido pocas las instituciones que han dedicado su tiempo y esfuerzo académico a estudiar las consecuencias de un mal manejo de la reputación digital y cómo es que ésta se puede destruir en cuestión de segundos. Verbigracia, en noviembre del año 2016, la marca internacional y productora de anteojos/lentes conocida como Hawkers™ lanzó un *tweet* en apoyo a Donald Trump, triunfador y ahora presidente de los Estados Unidos de América: "Mexicanos, pónganse estos lentes para que no se les noten los ojos hinchados mañana en la construcción del muro (sic)".[18]

Ante el ritmo social y la preocupación mundial que existió, sobre la posible elección de un candidato que hubo manifestado abiertamente su animadversión a los inmigrantes, sobre todo aquéllos de origen hispano-latinoamericano, asimismo, demostrar su alta intención de excluir de diversos tratados internacionales a la nación

[16] MIGLIANO, Simon. *Dark web Market Price Index (US Edition).* TOP 10 VPN. Privacy Central. Estados Unidos de América, 27 de febrero de 2018. Visto el 08 de agosto de 2018 a través del vínculo https://www.top10vpn.com/privacy-central/privacy/dark-web-market-price-index-feb-2018-us/

[17] SANTAMARÍA Ramos, Francisco José. "Identidad y Reputación Digital. Visión Española de un Fenómeno Global". *Revista Ambiente Jurídico*. Número 17. Enero 2015

[18] El tuit original fue eliminado de la cuenta oficial en Twitter de Hawkers, sin embargo, la campaña que se lanzó en contra de la compañía le generó pérdidas millonarias y que hoy en día sea una de las marcas con peor reputación digital en el mercado mexicano. Puede consultar la historia y el artículo completo, a través del diario en línea *El HuffPost*, "La empresa Hawkers paga muy cara una broma sobre Trump en Twitter", Internacional, Redacción, 10 de noviembre de 2016, disponible en la red a través del vínculo http://www.huffingtonpost.es/2016/11/10/hawkers-trump_n_12894462.html, consultado el 03 de junio de 2017.

americana,[19] provocó que la marca fuere duramente atacada durante las elecciones y que, a pesar del terror colectivo que se sufría en redes sociales (#eleccionesUSA, #elecciones2016), colocarse en la tendencia y, finalmente, culminar con la reacción del piloto mexicano de Fórmula 1, Sergio "Checo" Pérez, quién a través de su cuenta oficial en Twitter dictó que rompía relaciones con la marca Hawkers por atentar contra el pueblo mexicano y los ideales que los identificaban como nación. Al respecto, la marca de lentes culpó al CM (Community Manager) de la Ciudad de México y se vio obligada a desplegar un comunicado en uno de los diarios de mayor circulación nacional para disculparse con los mexicanos, todo debido al desafortunado mensaje. Posteriormente, ofreció al piloto mexicano la creación de una fundación en apoyo a niños en situación de calle, que llevaría su nombre: "Fundación Querido Sergio x Hawkers", con una inversión inicial de 500 mil pesos y aportaciones anuales superiores al millón de pesos.[20]

En seguimiento a lo expuesto, el autor Carlos Pinzón, encargado del área Social Media para la firma española Invenio PRO, señala que existe diferencia entre la identidad digital y la reputación digital, en el entendido que la segunda es consecuencia de la primera. Así, la identidad digital es:

> [...] lo que nosotros mismos vamos creando en Internet. Cuando subimos una foto a Facebook, cuando enviamos un tuit con un comentario o cuando detallamos nuestro currículum en *Linkedin*, nos estamos forjando una identidad digital que nos está describiendo [sic][21]

En un sentido amplio, señala Pinzón, la identidad digital constituye la referencia y percepción que poseo de mi persona y cómo lo reflejo en la red de redes, en pocas palabras, "lo que yo digo de mí". La reputación digital, por otro lado, se construye

[19] A la fecha de redacción de la presente obra, el presidente electo Donald Trump ha determinado que los Estados Unidos de América quedan excluidos del Acuerdo de Asociación Transpacífico y, recientemente, anunció que abandonará el Acuerdo de París sobre cambio climático, a lo que el mundo respondió: #MakeThePlanetGreatAgain. Para mayores referencias, puede consultar "Donald Trump anuncia que Estados Unidos abandonará el Acuerdo de París sobre cambio climático" *(BBC.* Mundo, 01 de junio de 2017 http://www.bbc.com/mundo/noticias-internacional-40124921) y "Trump retira a Estados Unidos del tratado comercial con el Pacífico" (BASSETS, Marc. *El País*, Enero 2017 http://internacional.elpais.com/internacional/2017/01/23/estados_unidos/1485184656_242993.html)

[20] *FORBES.*"Hawkers propone a Checo Pérez crear una fundación con su nombre". Portada. Últimas Noticias. Forbes Staff. Noviembre 17 de 2016. Se puede consultar en línea a través del vínculo https://www.forbes.com.mx/hawkers-propone-a-checo-perez-crear-una-fundacion-con-su-nombre/ Mismo que se revisó el 03 de junio de 2017.

[21] PINZÓN, Carlos. *Diferencia entre identidad digital y reputación on-line.* INVENIO PRO. Social Media. INVENIO PRO, Blog de Marketing Online. Consultado en línea el 03 de junio de 2017a través del vínculo http://www.inveniopro.es/diferencia-entre-identidad-digital-y-reputacion-on-line/

de la dualidad entre lo que se controla, es decir, la información que un titular legítimo sube a la web con la intención de generar una percepción favorable de sí mismo y por otro lado, las valoraciones subjetivas que realizan los usuarios en Internet que han interactuado con mi persona, perfil o producto; es decir, es la consecuencia de la ejecución de la identidad digital y los comentarios, opiniones, valoraciones y juicios de valor que se realizan por los cibernautas en correspondencia con lo que se dijo que "somos". En breves términos, la reputación digital es "lo que los demás dicen de mí" en la vida *on line.*[22]

Sin duda, los conceptos anteriormente descritos permiten advertir que la identidad y la reputación digital no son elementos exclusivos de las personas físicas, sino que esto también afecta a las personas jurídicas. Sin embargo, a la aplicación de estas figuras cibernéticas en el ámbito de las corporaciones se les conoce como *reputación empresarial*.

Al respecto, el concepto jurídico más aproximado a las hipótesis expuestas, se encuentra excelsamente definido por el diccionario legal de *Black,* mismo que define *Online Corporate Reputation* como la percepción que tienen los usuarios de Internet sobre la empresa. De manera general —señala el diccionario legal en cita- se obtiene de blogs, foros públicos y artículos en la web—. Y para sorpresa del autor y de algunos de mis lectores, ya incluye en su concepto la precisión de *Reputation Management*, considerándole como el servicio que puede influenciar la reputación *online* al redireccionar comentarios negativos y promover mensajes positivos a favor de la Empresa.[23]

En ese tenor, el *Reputation Institute* publica de forma anual el índice de las marcas y compañías con mejor reputación en el mundo, entre las que incluye a marcas globales como BMW, Google, Nike, Microsoft e INTEL, para lo cual utiliza diversos factores de evaluación, como lo son calidad de productos, valor de la marca, posición en el mercado bursátil y determinante, la referencia que existe entre los cibernautas sobre la compañía.[24]

Debo someter a consideración del lector el concepto de identidad digital y reputación digital, dentro del universo de lo conocido como Internet 2.0 (Web 2.0), no sólo como un factor dentro del patrimonio digital que pudiere generar consecuencias de

[22] *Op. Cit.* 18

[23] BLACK'S LAW DICTIONARY. *The Law Dictionary*. What is Online Coporate Reputation? Puede consultar la definición en inglés, a través del vínculo http://thelawdictionary.org/online-corporate-reputation/

[24] Tan sólo en el año 2016, las 5 marcas mejor posicionadas lo fueron: 1) Rolex: 80.38, 2)Lego: 79.4, 3)Walt Disney: 79.2, 4)Cannon: 78.3 y 5) Google: 78.2. Puede consultar más información y el estudio completo con las 100 empresas mejores posicionadas a nivel global, así como los parámetros íntegros, a través del vínculo (REPUTATION INSTITUTE. https://www.reputationinstitute.com/research/Global-RepTrak-100.aspx Consultado el 03 de junio de 2017.

carácter comercial, sino también de carácter profesional o laboral, bajo la modalidad de contratación conocida como Reclutamiento 2.0, la cual consiste en la aplicación de redes sociales como herramienta de selección para las áreas de recursos humanos, en la cual se realiza una búsqueda entre perfiles laborales como es LinkedIn y se compara con lo que se encontró sobre el candidato en una red social más coloquial y flexible como lo es Facebook.

En palabras del Maestro Pedro Rojas, este proceso permite a los departamentos de RRHH "una aproximación muy estrecha a la persona y una cantidad de datos que nunca hubiesen obtenido usando métodos tradicionales, ya que los perfiles en redes sociales... dejan ver... dentro del interior del candidato potencial";[25] ello pudiendo beneficiar el proceso de selección si es que el interesado cuenta con una buena reputación digital o bien, inpidiendo la contratación del mismo y quizá, hasta bloquear su posible selección para otros procesos, en caso de no contar con una buena reputación *online*.

Por último, es meritorio para el valor académico de la presente obra, aseverar que el concepto de reputación no es un elemento aislado de la ciencia jurídica ni de los tribunales. En términos del artículo 1916 del Código Civil Federal (México) se advierte que:

> [...] Por daño moral se entiende la afectación que una persona sufre en sus sentimientos, afectos, creencias, decoro, **reputación**, vida privada, configuración y aspectos físicos, o bien en la consideración que de sí misma tienen los demás. Se presumirá que hubo daño moral cuando se vulnere o menoscabe ilegítimamente la libertad o la integridad física o psíquica de las personas [...]
> (El énfasis es añadido).

Así las cosas, se advierte que el aspecto "moral" de las personas, así como los elementos que definen sus derechos de personalidad se integran, entre otros, por la reputación. Este concepto no debe interpretarse más allá de lo previsto en el propio precepto, sin embargo, el afirmar que la reputación digital forma parte de esa integración *personalidad-persona* permitiría argüir violaciones en contra de esa esfera jurídica, tratándose de conductas que pudieran afectar dicha condición humana en la red de redes, sobre todo, aquellas que podrían viralizarse gracias al poder de las redes sociales.

I. 2. 4 Bienes de Origen Exclusivamente Digital

La corriente de derecho que tradicionalmente separaba a los bienes en *tangibles* (materiales) o *intangibles* (inmateriales) se ha visto superada por el acelerado crecimiento

[25] ROJAS, Pedro. *Reclutamiento y Selección 2.0. La nueva forma de encontrar talento.* Editorial UOC. España 2010.

de la red de redes, así las cosas, hoy en día se debe hablar que en la categoría de los intangibles debemos comprender a aquéllos de *naturaleza digital por nacimiento* y los *digitales por transformación*. Los primeros, son aquéllos que han nacido en el ciberespacio y sólo pueden ser concebidos, apreciados y "enajenados" dentro del propio universo digital; en tanto que los segundos corresponden a una categoría de bienes que en origen fueron materiales, empero que la necesidad y la probable desaparición del soporte generó la necesidad de digitalizarlos, así nacieron a la vida en Internet y en tanto el documento base original exista, éste no será considerado como el referente y evidencia única de la existencia de un hecho o acto jurídico.

En palabras de la Maestra Adrian Porcelli, los bienes inmateriales son intangibles "como las ideas, costumbres, conocimientos, creencias, lenguajes, tradiciones, saberes, formas de expresión, artes o técnicas genéricamente abstractas [...]", en tanto que los bienes digitales son "todos aquellos bienes culturales y no culturales que tienen forma digital, que están compuestos por ceros y unos y que las computadoras se encargan de interpretar y presentarlos en forma de información".[26] Dentro de los ejemplos que nos brinda la renombrada catedrática del Departamento de Ciencias Sociales de la Universidad Nacional de Luján, se encuentran los programas de cómputo, imágenes, música, sitios web, textos, libros y videos.

Lo anteriormente expuesto rompe el paradigma que tradicionalmente se ha comprendido sobre la concepción de bienes. Si tomamos como referencia el mundo de los libros digitales (bienes inmateriales digitales) de origen, Amazon representa el 70% del mercado de las obras literarias electrónicas. Esto ha permitido un acelerado crecimiento en la distribución y venta de estos ejemplares. Para el año 2010 se habían vendido 11 millones de lectores de libros digitales, de los que el 41.5% fueron Kindles de Amazon, lo que generó y permitió un crecimiento paralelo del estudio en formatos no tradicionales. Sin embargo, este sería un ejemplo sencillo de asimilar dentro del metaverso de posibilidades, ya que casos como la creación de videojuegos similares a *Second Life,* permite no sólo la creación de un avatar,[27] sino que además

[26] PORCELLI, A. "Los bienes digitales y el derecho de autor en Internet. La denominada 'piratería informática'". *Revista del Departamento de Ciencias Sociales*, Volumen 2, Número 3. 258-294. Revista electrónica del Departamento de Ciencias Sociales de la Universidad Nacional de Luján. Puede consultar el texto íntegro a través del vínculo http://www.redsocialesunlu.net/wp-content/uploads/2015/06/RSOC009-16-ARTICULO-PORCELLI.pdf Consultado el 03 de junio de 2017.

[27] Si bien el *Diccionario de la Real Academia Española* brinda diversas acepciones, entre ellas "reencarnación o transformación", éstas se alejan del significado que ha obtenido en el ciberespacio. A parecer del autor, el concepto más adecuado a la realidad digital, se desprende del texto publicado por la Universidad Tecnológica Metropolitana de Santiago de Chile, mismo que define al avatar como "una especie de caricatura de un ser de carne y hueve que no sirve para ridiculizarle, sino para localizar el lugar exacto en que ese ser humano se encuentra representado en el ciberespacio. Son representaciones gráficas de los personajes escogidos para representar a los usuarios en el entorno virtual" (FERRADA Cubillos, Mariela. *Términos de uso frecuente en la Web Social. Glosario*. Departamento de Gestión de

comience a generar su propia reputación y, en ciertos casos, sus propios bienes. No obstante, nadie esperaba que pronto este juego de realidad aumentada resultara del interés de las marcas y patrocinadores, quienes en poco tiempo detectaron el mercado potencial que sería generar *product placement* sobre la plataforma.

Así las cosas, los patrocinadores pronto contactaron a los desarrolladores (Liden Lab) para comenzar un programa de inserción de productos, marcas e inclusive creación de empresas dentro de la propia plataforma, lo que generó derecho de propiedad a favor de un alter ego concebido en la red y por ende, actos y consecuencias de derecho que son susceptibles de un profundo análisis tales como "compraventa de terrenos virtuales" o "arrendamiento de inmuebles para espacios publicitarios"; sin embargo, en afán de ser consecuente con el discurso sostenido hasta ahora, es prudente señalar que estos bienes de origen eminente y exclusivamente digital (incluyendo el *avatar*) son intangibles y pueden generar un valor económico a favor de la persona jurídica que los opere en el mundo tangible. Hasta este punto, podría ocurrir la hipótesis en la cual existan conflictos entre personas físicas y avatares, avatares y avatares o bien personas morales y avatares; asimismo, podría considerarse que el patrimonio de bienes intangibles digitales cuyo dominio le "pertenece" al avatar fuere superior en valor económico de aquel que posee la persona física que lo opera.

A esta lista de posibles fortunas virtuales, podríamos sumar el ejemplo de los *bitcoins* y los *nombres de dominio*, los cuales también constituyen parte del patrimonio digital, sin embargo, estos serán analizados de forma puntual dentro de un capitulado de la presente obra.

I. 2. 5 Una probable definición de patrimonio digital desde la perspectiva de derecho privado

En el año 2003, como consecuencia de la *Carta Sobre la Preservación del Patrimonio Digital*, la División de la Sociedad de la Información, de la UNESCO, a través de la Biblioteca Nacional de Australia, prepararon el documento denominado "Directrices para la preservación del patrimonio digital", mismo que consta de 176 fojas útiles e insiste en un concepto estricto de patrimonio, desde la perspectiva de derecho internacional público, ya que en su artículo 5.2.1 prescribe que "el patrimonio digital está constituido únicamente por aquello que se considera que poseen un valor permanente",[28] así las cosas, este concepto deja fuera los elementos de patrimonio

Información. Universidad Tecnológica Metropolitana. Serie bibliotecología y gestión de información número 81, Abril 2013. Mismo que se puede consultar en línea a través del vínculo http://eprints.rclis.org/19182/1/Serie%20N%C2%B081%20Mariela%20Ferrada.pdf)

[28] UNESCO. *Memory of the World. Directrices para la preservación del patrimonio digital*. Preparado por la Biblioteca Nacional de Australia. División de la Sociedad de la Información. Puede

digital anteriormente citados como lo son: *i)* datos biométricos, *ii)* datos personales, *iii)* identidad y reputación digital, y *iv)* bienes de origen digital.

Todo este patrimonio está sujeto a consecuencias de derecho, actos de derecho y claro que también a intereses jurídicos diversos que pudieren reclamarse ante tribunales jurisdiccionales competentes. Así las cosas, sería prudente definir al patrimonio digital *strictu sensu* como el conjunto de bienes, derechos y obligaciones correspondientes a un usuario, independientemente de su representación física o digital que podrían reflejar contenido económico y que constituyen una universalidad jurídica, misma que debe ser atribuible a la persona física o moral que cuenta con capacidad de goce y ejercicio para interactuar en la red de redes. Aportamos esta definición con el espíritu crítico de contribuir a nuestra ciencia jurídica, sin embargo, debemos resaltar que la intención fundamental del presente capítulo radica en generar conciencia académica, práctica y jurisdiccional por lo que refiere a los bienes con naturaleza intangible y digital, en el entendido que aquellos elementos de derecho que tienen origen en la red de redes también conforman parte del patrimonio.

Resultará procedente, en algún momento histórico-jurídico, concebir el concepto de *patrimonio* como un todo integrado tanto por aquellos bienes cuya percepción y regulación recaen sobre figuras tradicionales de derecho, así como bienes digitales que no necesariamente se han estudiado en el derecho positivo. Sin duda, ello también vencería el paradigma de negocios jurídicos que tradicionalmente se han aceptado, por ejemplo: ¿cómo se llevaría a cabo la transmisión de propiedad de un perfil de Facebook?, ¿cómo se considera a las contraseñas y datos generados en redes sociales respecto de la masa hereditaria? Estas incógnitas serán estudiadas en próximos capítulos y en un humilde intento del autor, brindaremos la respuesta que, a nuestro leal entender, pudiere abrir nuevas puertas en la *jurisprudencia.*

consultar la versión en español de este documento a través del vínculo http://unesdoc.unesco.org/images/0013/001300/130071s.pdf Visto en línea el 03 de junio de 2017.

II
CAPÍTULO

Testamento Digital

En el universo del Derecho de Sucesiones o Derecho Hereditario, el Testamento es la forma jurídica por excelencia: personalísimo, revocable y libre por el cual una persona capaz dispone de sus bienes y obligaciones para después de su muerte; se concibe como el acto que permite fijar el destino que "ha de darse a las relaciones jurídicas de una persona física cuando ésta muere" y en su caso, determina la posibilidad de constituir relaciones jurídicas nuevas. Esta institución debe su origen, como varias de las fórmulas tradicionales que ocupamos hasta nuestros días, al testamento Romano a partir del derecho pretorio, momento en el que adoptó la característica de ser un acto unilateral, asimismo adquiere tres elementos esenciales que prevalecen en diversas legislaciones alrededor de la orbe: *i)* La figura del heredero no aparece como una relación *sine qua non* para permitir la celebración del testamento; esto respeta la corriente legal que permite emitir testamentos sin señalar de forma puntual herederos, lo que no sólo se considera admisible, sino legalmente válido para aquellos códigos civiles que respetan esta corriente romana; *ii)* Difusión a través de la forma pública notarial; *iii)* Admisión del testamento ológrafo creado por el Código de Napoleón (empero, esta figura ha desaparecido de la legislación mexicana).

Por su lado, Mucius Scaevola dicta que el testamento es "un acto espontáneo, personal, solemne y revocable, en virtud del cual una persona… dispone, para después de su muerte, tanto de su fortuna como de todo aquello que en la esfera social en que vive, puede y debe ordenar en pro de sus creencias y de las personas que a él estén unidas […]".[1] Sin duda, resulta relevante para los distintos pueblos y sistemas jurídicos, el

[1] GÓMEZ NAVARRO, Soledad. "Testamento y tiempo: historia y derecho en el documento de última voluntad." Universidad de Córdoba. *Revistas Científicas de la Universidad de Cádiz*, España 1999. Puede

respeto de la voluntad de las personas para después de su muerte, así como la disposición de sus bienes ante el fallecimiento: *i)* En el derecho romano arcaico contaban con figuras de testamento público (*calatis comitis)*, el *testamentum in procintu* (realizado por el *pater familias*) y el *arrogatio* —ausencia de hijos en la familia—; *ii)* En la época romana clásica apareció el reconocimiento de la capacidad para testar, mejor conocida como *testamenti factio activa,* así como la de recibir bienes por testamento, denominada *testamenti factio pasiva; iii)* En la época posterior a Justiniano apareció el testamento público y privado, cuyas características exigían la celebración de los mismos ante siete testigos y, en el caso del primero, el testamento se resguardaba en los archivos imperiales; *iv)* En la Edad Media y en seguimiento a la costumbre visigoda, se rescata la figura de actos posteriores a la muerte y, aunque ignoran el vocablo de testamento, instituyen figuras como el *cabezalero, manumisor* o albacea; el término *testamentum* se recuperaría para la época de la Plena Edad Media, gracias al reconocimiento de la corte castellana del "rey legislador".

De los antecedentes expuestos se advierte una línea de igualdad, ya que la evolución del testamento, en cada una de sus fases, reconoce la posibilidad de dejar bienes *pro ánima* para después de la muerte, sin limitar ningún ejercicio del *dominus* (dominio). En línea con lo anteriormente expuesto, el Doctor Juan Bautista Medina, podría aportar la más simple definición de testamento, que a mí parecer resulta la más adecuada para comenzar el estudio que ocupa nuestro presente capítulo: "[...] testamento es la declaración que de su última voluntad hace una persona, disponiendo de bienes y de asuntos que le atañen para después de su muerte";[2] asimismo, reconoce que los bienes deben ser considerados con "uniformidad", es decir, se deben suprimir las diferencias entre las calidades y cualidades jurídicas del patrimonio e invoca el principio de "unidad de la sucesión".

Este último principio es el que nos permitiría fortalecer los conceptos expresados en el capítulo anterior, a través de los cuales confirmamos que la distinción entre patrimonio *latu sensu* y *strictu sensu*, no deben provocar discriminación entre aquellos bienes cuyo origen se lo deban a medios digitales o, en su caso, a bienes que únicamente comprenden su existencia a través de acceso tecnológico. Por lo anterior, es prudente preguntar al lector: ¿se puede colocar en testamento los bienes digitales

---

consultar el texto íntegro de la increíble investigación de la Maestra Gómez Navarro, a través del vínculo https://www.google.com.mx/url?sa=t&rct=j&q=&esrc=s&source=web&cd=8&cad=rja&uact=8&ved=0ahUKEwjEj9yk6LnXAhVM0oMKHdaaDKIQFghMMAc&url=http%3A%2F%2Frevistas.uca.es%2Findex.php%2Ftrocadero%2Farticle%2Fdownload%2F776%2F642&usg=AOvVaw27AQcMRv62vy40E546_4_R Visto el 12 de noviembre de 2017.

[2] FOS MEDINA, Juan Bautista. "El testamento en la historia: aspectos morales y religiosos". Biblioteca digital de la Universidad Católica Argentina. *Suplemento de Filosofía número 30*, Argentina, 2015. Puede consultar el artículo completo, en el repositorio institucional en el vínculo http://bibliotecadigital.uca.edu.ar/repositorio/investigacion/testamento-historia-morales-religiosos.pdf visto el 12 de noviembre de 2017.

—patrimonio digital— y esta última voluntad debe imperar y respetarse por cualquier institución jurídica moderna romana?

En el año 2012, el actor americano Bruce Willis despertó con la inquietud de realizar su testamento, sobre todo de aquellos bienes que adquirió en plataformas digitales como lo es iTunes y Amazon. Hasta ese momento, el histrión hubo acumulado la cantidad de 150 mil canciones en su biblioteca musical. Una vez que se acercó a su asesor jurídico, ambos determinaron que las condiciones, políticas y términos que ofrece la compañía Apple no permiten colocar en testamento los bienes intangibles que se generen en vida; a lo anterior, la compañía ha ofrecido salidas administrativas como lo es brindar la contraseña de acceso a los herederos, previa legitimación ante la compañía fundada por Steve Jobs. Dicha condición no fue suficiente para Willis y amenazó con demandar a Apple si la compañía no permitía la legítima sucesión de sus adquisiciones digitales.

Esta historia inspiró al abogado sevillano Víctor López,[3] quien argumenta la confusión en que se induce al comprador y usuario de dichas plataformas al colocar el botón "comprar" en vez de "usar". Los defensores de este tipo de plataformas, arguyen que las condiciones bajo las cuales adquieren el servicio son claras y éstas funcionan bajo la categoría de "contrato de licencia de aplicación de usuario final", apartado en el que no sólo se precisa que los contenidos que adquirimos son intransferibles y, en ningún caso, se prevé la posibilidad de suceder algún bien enajenado a través de dichas plataformas.

Jurídicamente resulta claro para los tribunales a nivel internacional, así como para los prestadores de dichos servicios de almacenamiento digital, que toda vez los usuarios no adquieren la propiedad de un bien tangible, como lo sería la adquisición de un disco compacto o de vinil, sino que obtienen una licencia de uso no exclusiva y limitada a un usuario. Al respecto, la política vigente de Apple dicta:

> **Términos y condiciones de los servicios de contenido multimedia de Apple**[4]
>
> Los presentes términos y condiciones crean un contrato entre Ud. y Apple (el "Contrato"). Lea atentamente el Contrato. Para confirmar que ha entendido y acepta el Contrato, haga clic en "Acepto".

[3] PIÑERO, Laura. *Un abogado sevillano demanda a "Apple" inspirado por Bruce Willis (sic).* Cadena SER. Madrid, España, 2012. Puede consultar la nota íntegra, a través del vínculo http://cadenaser.com/programa/2017/01/20/la_ventana/1484935223_530716.html visto el pasado 11 de noviembre de 2017.

[4] APPLE. *Términos y Condiciones de los Servicios de Contenido Multimedia de Apple.* Legal. 13 de septiembre de 2016. Consultado en línea el 11 de noviembre de 2017, a través del vínculo https://www.apple.com/legal/Internet-services/itunes/es/terms.html

A. INTRODUCCIÓN A NUESTROS SERVICIOS

El presente Contrato regula la utilización, por parte de Ud., de los servicios de Apple (los "Servicios"), a través de los cuales Ud. podrá comprar, obtener, utilizar bajo licencia, alquilar o suscribirse a contenido multimedia, apps (las "Apps") y otros servicios dentro de las apps (el "Contenido"). Nuestros Servicios son: iTunes Store, App Store, iBooks Store, Apple Music y Apple News. Al crear una cuenta para utilizar los Servicios en España[5], Ud. declara que este es su país de residencia a efectos fiscales (el "País de Residencia"). ....

B. UTILIZACIÓN DE NUESTROS SERVICIOS
PAGOS, IMPUESTOS Y DEVOLUCIONES

Ud. puede adquirir Contenido gratuito o de pago a través de nuestros Servicios. Cualquiera de estos supuestos se denomina la "Transacción". Por **cada Transacción, Ud. adquiere una licencia exclusivamente para utilizar el Contenido**. Cada Transacción constituye un contrato electrónico entre Ud. y Apple, y/o Ud. y la entidad que proporciona el Contenido a través de nuestros Servicios. No obstante, si Ud. es cliente de Apple Distribution International y adquiere una App o un libro, Apple Distribution International es el (léase "la" [sic]) entidad que realiza la venta; esto significa que Ud. adquiere el Contenido a través de Apple Distribution International, y que dicho Contenido le es cedido bajo licencia por el Proveedor de Apps (conforme se define más adelante) o el editor del libro.
[...]
Para usar nuestros Servicios y acceder a su Contenido, Ud. necesita un ID de Apple. Un ID de Apple es la cuenta que Ud. utiliza en todo el ecosistema de Apple. Su ID de Apple es valioso y Ud. será responsable de preservar su confidencialidad y seguridad. Apple no será responsable de ninguna pérdida derivada del uso no autorizado de su ID de Apple. Póngase en contacto con Apple si sospecha que ha sido vulnerada la confidencialidad de su ID de Apple.
[...]

NORMAS DE UTILIZACIÓN DE LOS SERVICIOS Y DEL CONTENIDO

Al utilizar los Servicios y el Contenido, Ud. deberá cumplir las normas que se establecen en esta sección (las "Normas de Utilización"). ...

[5] El país cambia conforme al buscador que se utiliza para acceder a las disposiciones legales de la compañía, pero las condiciones descritas y que se reproducen en el presente apartado se mantienen.

- **Ud. podrá utilizar Contenido de hasta cinco ID de Apple diferentes en cada dispositivo.**
- **Ud. será responsable de no perder, destruir o dañar el Contenido una vez descargado. Le recomendamos que haga copias de seguridad del Contenido de forma periódica.**
- **Ud. no podrá manipular o eludir ninguna tecnología de seguridad incluida con los Servicios.**
- **Ud. únicamente podrá acceder a nuestros Servicios utilizando el software de Apple, y no podrá modificar o utilizar versiones modificadas de dicho software.**
- El Contenido en video requiere una conexión HDCP.

Contenido de iTunes Store:
[…]

D. COMPARTIR EN FAMILIA

El organizador de una Familia (el "Organizador") debe ser mayor de 18 años y el padre, la madre o el tutor legal de cualquier miembro de la Familia que sea menor de 13 años o la edad mínima equivalente en su País de Residencia (conforme se indique en el proceso de registro). Para acceder a todas las funciones de Compartir en Familia se requieren dispositivos Apple.

Compartir la Compra: la función Compartir la Compra de Compartir en Familia le permite compartir Contenido apto hasta con seis miembros de una Familia. El Organizador invita a otros miembros a compartir y aceptar pagar todas las Transacciones iniciadas por los miembros de la Familia. El método de pago del Organizador se utiliza para pagar cualquier Transacción iniciada por un miembro de la Familia (salvo cuando la cuenta del miembro de la Familia disponga de crédito, en cuyo caso el crédito se utilizará siempre en primer lugar). Los miembros de la Familia actúan como agentes del Organizador cuando se utiliza el método de pago del Organizador. […]

CONTRATO DE LICENCIA DE APLICACIÓN DE USUARIO FINAL

Las Apps ofrecidas a través de la App Store son cedidas bajo licencia y no vendidas a favor de Ud. El otorgamiento de una licencia, a favor de Ud., con respecto a cada App quedará condicionado a que acepte previamente los términos del presente Contrato de Licencia de Aplicación de Usuario Final (el "CLUF Standard") o de un contrato de licencia de usuario final personalizado entre Ud. y el Proveedor de Apps (el "CLUF Personalizado"), en la medida en que éste le sea proporcionado. La licencia sobre cualquier App de Apple objeto del presente CLUF Standard o del CLUF Personalizado es otorgada a favor de Ud. por Apple, y la licencia sobre cualquier App de Terceros objeto del presente CLUF Standard o del CLUF Personalizado es otorgada

a favor de Ud. por el Proveedor de Apps de dicha App de Terceros. Cualquier App que sea objeto del presente CLUF Standard se denominará la "Aplicación Cedida Bajo Licencia". El Proveedor de Apps o Apple, según los casos, (el "Licenciante") se reservan todos los derechos sobre la Aplicación Cedida Bajo Licencia que no sean expresamente otorgados a favor de Ud. con arreglo al presente CLUF Standard.

a. Ámbito de la licencia: El Licenciante le otorga una licencia no transferible para utilizar la Aplicación Cedida Bajo Licencia en cualquier producto marca Apple que sea de su propiedad o esté bajo su control y en la medida de lo permitido por las Normas de Utilización. Las disposiciones recogidas en el presente CLUF Standard serán de aplicación al contenido o a los materiales o servicios a los que se pueda acceder o que sean comprados desde la Aplicación Cedida Bajo Licencia, así como a las actualizaciones proporcionadas por el Licenciante que sustituyan y/o complementen la Aplicación Cedida Bajo Licencia original, salvo que la actualización en cuestión venga acompañada de un CLUF Personalizado. Salvo por lo dispuesto en las Normas de Utilización, Ud. no podrá distribuir o facilitar el acceso a la Aplicación Cedida Bajo Licencia a través de una red desde la que pueda ser utilizada simultáneamente por varios dispositivos. **Ud. no podrá transferir, redistribuir o sublicenciar la Aplicación Cedida Bajo Licencia y, si Ud. vende su Dispositivo Apple a un tercero, deberá eliminar la Aplicación Cedida Bajo Licencia del Dispositivo Apple antes de venderlo. Asimismo, Ud. no podrá copiar (salvo en la medida expresamente permitida por esta licencia y las Normas de Utilización)**, invertir la ingeniería, desensamblar, intentar obtener el código objeto, modificar o crear trabajos derivados de la Aplicación Cedida Bajo Licencia o de cualesquiera actualizaciones o de cualquier parte de la misma (salvo que cualquiera de las restricciones previstas anteriormente estén prohibidas por la legislación aplicable o en la medida en que así lo permitan los términos y condiciones de la licencia que regule la utilización de los componentes de código abierto incluidos con la Aplicación Cedida Bajo Licencia).

[...]

i. Salvo en la medida expresamente permitida en el párrafo siguiente, el presente Contrato y la relación entre Ud. y Apple se regirán por las leyes del Estado de California, sin remisión a sus normas sobre conflictos de leyes. Ud. y Apple se someten a la competencia exclusiva de los tribunales del condado de Santa Clara, California, para resolver cualquier controversia o demanda derivada del presente Contrato. Si (a) Ud. no es ciudadano estadounidense; (b) Ud. no reside en EE.UU.; (c) Ud. no está accediendo al Servicio desde EE.UU.; y (d) Ud. es ciudadano de alguno de los países identificados a continuación, acepta que toda controversia o demanda derivada del presente Contrato estará sujeta a la ley aplicable que se especifica más adelante, sin remisión a ninguna norma sobre conflictos de leyes, y se somete irrevocablemente a la competencia no exclusiva de los tribunales correspondientes al estado, provincia o país siguientes, cuyas leyes serán de aplicación:

Si Ud. reside en cualquier país de la Unión Europea o en Suiza, Noruega o Islandia, la ley aplicable y el fuero serán los correspondientes a su lugar de residencia habitual.

La Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías queda expresamente excluida del presente Contrato.

H. CONDICIONES ADICIONALES DE IBOOKS STORE

Ud. adquiere el Contenido de iBooks Store a través del tercero proveedor de dicho Contenido (el "Editor") y no a través de Apple. Apple actúa como agente del Editor al proporcionarle el Contenido de iBooks Store, por lo que no es parte interviniente en la Transacción entre Ud. y el Editor. Si Ud. es cliente de Apple Distribution International, el comercio que realiza la venta es Apple Distribution International; esto significa que Ud. adquiere a través de Apple Distribution International, una licencia para usar el Contenido, pero el Contenido es cedido bajo licencia por el Editor. El Editor del Contenido de iBooks Store se reserva el derecho a exigir el cumplimiento de las condiciones de uso relativas a dicho Contenido de iBooks Store. El Editor del Contenido de iBooks Store es enteramente responsable de dicho Contenido, de las garantías otorgadas, en su caso y en la medida en que no hayan sido excluidas, y de cualesquiera reclamaciones que Ud. o cualquier tercero puedan realizar en relación con dicho Contenido.
[...]

BIBLIOTECA DE MÚSICA ICLOUD

La Biblioteca de Música iCloud es una función de Apple Music que le permite acceder a sus canciones coincidentes o cargadas, a sus listas de reproducción y a los videos musicales que haya comprado a través de Apple Music, iTunes Store o un tercero (el "Contenido de la Biblioteca de Música iCloud") en sus dispositivos equipados con Apple Music. La Biblioteca de Música iCloud se activa automáticamente cuando Ud. inicia su suscripción de Apple Music. La Biblioteca de Música iCloud recoge información acerca del Contenido de la Biblioteca de Música iCloud. Esta información es asociada a su ID de Apple y comparada con el Contenido de la Biblioteca de Música iCloud actualmente disponible en Apple Music.
[...]
Fecha de la última actualización: 13 de septiembre de 2016
[El énfasis es añadido]

En términos de lo anterior, se desprenden las siguientes condiciones contractuales:

i) La aplicación App Store, así como las herramientas adicionales de Apple, permiten la compra y la adquisición de licencias de otras aplicaciones en el mercado, así como productos digitales que se encuentren disponible a través de dicha plataforma.

ii) Jurídicamente, Apple prefiere ocupar el término de "Transacción" para definir la adquisición de licencias de uso únicas otorgadas a favor del titular de la ID de Apple.

iii) Se podrá adquirir material multimedia oneroso o gratuito, usando el software y el hardware autorizado por la compañía, el cual podrá ser consultado siempre que se autentique con el ID de usuario. Dicho ID permitirá el acceso en cinco equipos que pertenezcan a la compañía y, en su caso, permite la reproducción de material que se adquiera a través de su tienda en línea (en respeto a lo que indica el Convenio de Berna de la Organización Mundial de la Propiedad Intelectual y el Tratado de Derechos de Autor en el ámbito Digital de la Organización Mundial de la Propiedad Intelectual; mismos que se estudiarán en capítulos más adelante).

iv) Se acepta que la forma jurídica de tales disposiciones adquiere el nombre de Contrato De Licenciamiento De Aplicación De Usuario Final, lo que implica que no se obtiene la propiedad del bien intangible digital, sino que la transacción ocurre bajo la modalidad de licenciamiento no transferible y único; a su vez, advierte que en caso de transmisión de la propiedad del hardware que contenga la descarga de contenido multimedia licenciado a través de esta figura jurídica, deberá ser eliminado previo la celebración tal compra venta, ya que esto atentaría contra el licenciamiento otorgado.

v) Por último, indica que el contenido multimedia (mismo que incluye música, libros, aplicaciones, etc.) únicamente podrá ser consultado a través de la biblioteca digital iCloud, siempre que se autentique al usuario dentro del dispositivo. Al respecto, es prudente enfatizar la posibilidad de "compartir en familia" el contenido que se adquiere en vida, sin embargo, esto no resulta la solución para la transmisión de patrimonio digital que nos podría ocupar.

En el mismo tenor, podemos encontrar términos y condiciones de Kindle de Amazon, que determina a través de su Contrato Digital:

> [...] **Uso del Contenido Digital.** Tras la descarga del Contenido Digital y el pago por su parte de todas las tasas aplicables (incluyendo los impuestos aplicables), el Proveedor de contenido le otorga un derecho no exclusivo a ver, usar y a mostrar dicho Contenido Digital un número ilimitado de veces, única y exclusivamente en el Kindle o en una Aplicación de Lectura, o de cualquier otra manera que esté permitida como parte del Servicio, única y exclusivamente en los Kindle u Otros Dispositivos especificados en la Tienda Kindle, sirviendo única y exclusivamente para su uso personal y no comercial. Salvo indicación en contrario, el Contenido Digital será utilizado a través de una licencia otorgada por el proveedor de contenido sin que se produzca la venta de dicho contenido. El Proveedor de contenido puede incluir condiciones adicionales de uso de su Contenido Digital. Dichos términos serán también aplicables, pero el

presente Contrato prevalecerá en caso de conflicto. Es posible que una parte del Contenido Digital, como las Publicaciones Periódicas, no esté disponible a través de las Aplicaciones de Lectura.

Limitaciones. Salvo que se indique específicamente lo contrario, no podrá vender, alquilar, distribuir, emitir, otorgar sublicencias, ni de algún otro modo, asignar ningún derecho sobre el Contenido Digital o parte del mismo a terceros, y tampoco podrá modificar ni eliminar del ningún tipo de mención relativa a los derechos de autor o de propiedad del Contenido Digital. Tampoco podrá eludir, modificar, intentar acabar con o burlar los elementos de seguridad que protegen el Contenido Digital [...][6]

Así las cosas, el mercado digital ha diseñado diversas condiciones y políticas bajo la estructura de licenciamiento, en el entendido que estima "intransferible" la nuda propiedad de un bien intangible como lo podría ser un libro, canción, álbum, aplicaciones o imágenes, todos ellos del ámbito digital. Empero, las condiciones rígidas y absurdas bajo las cuales los prestadores de servicio pretenden interpretar el funcionamiento de sus plataformas, atiende a un beneficio económico y la búsqueda de permanencia y lealtad sobre la marca, sobre cualquier beneficio jurídico a favor del usuario final, sobre todo tratándose del derecho de transmisión de la propiedad adquirida bajo la figura de la sucesión legítima o testamentaria.

Lo anterior deja de manifiesto la complejidad para ocupar la figura del testamento tradicionalmente aceptado, así como cualquier modalidad de sucesión jurídica. Por su lado, la *Enciclopedia jurídica* define a la *sucesión legal* como aquella en la que la ley regula el destino de las relaciones jurídicas del causante al no haber otorgado éste testamento alguno;[7] en ese tenor, determina que el *testamento* es el acto por el cual una persona dispone para después de su muerte **de todos sus bienes o parte de ellos,** se considera un acto jurídico unilateral —por excelencia— por el que una persona declara sus últimas voluntades.[8] Figuras jurídicas que tendrían que resultar aplicables en todos los casos a las conductas *online*, sin embargo, las líneas que antes se reprodujeron podrían dejar de manifiesto que el tratamiento *sui generis* que reciben los bienes intangibles multimedia (sobre todo de aquéllos adquiridos a través de plataformas *streaming)* no permite la aplicación de ningún tipo de sucesión, legítima o testamentaria.

Sin embargo, esto podría atentar contra el concepto de patrimonio que se proporcionó en el capítulo anterior y, en su caso, con el de dominio, sobre todo porque dichas

[6] AMAZON. *Contrato de licencia y condiciones de uso del Kindle de Amazon.es.* Última actualización de 28 de septiembre de 2011. Consultado en línea el 11 de noviembre de 2017, a través del vínculo https://www.amazon.es/gp/help/customer/display.html?nodeId=201283840&tag=xataka-21

[7] ENCICLOPEDIA JURÍDICA. *Sucesión Legal.* http://www.enciclopedia-juridica.biz14.com/d/sucesi%C3%B3n-legal/sucesi%C3%B3n-legal.htm

[8] *Op. Cit.* 31. *Testamento.* http://www.enciclopedia-juridica.biz14.com/d/testamento/testamento.htm

aplicaciones colocan el botón de "Compra" —como bien indica Víctor López— no el de licenciamiento o el de transacción, como podría esperarse en términos de los Términos y Condiciones que se reprodujeron anteriormente.

Al entender de quien redacta, no hay margen de debate sobre el irrestricto cumplimiento de la ley que deberían seguir los proveedores del servicio (Apple, Kindle, etc.), independientemente de lo confuso o leonino que pudieren resultar las cláusulas de sus Condiciones; tal como resultó en el caso Durand vs Facebook *(véase capítulo infra)*, en el cual la corte de primera instancia francesa dictó procedente la demanda en contra de Facebook Inc., independientemente que el usuario Durand firmó las "Declaraciones" en supuesta aceptación de cada una de las condiciones ahí prescritas y, en su caso, renunciando a la protección de la ley parisina, así como la protección de los tribunales franceses; al respecto, se calificó de "exagerado e imposible" de cumplimentar por cualquier usuario, de tal suerte que la corte de primera instancia no sólo estimó procedente la demanda contra el coloso de la red social, sino que resolvió sobre el mérito del asunto.

A su vez, me parece prudente invocar el principio *Ubi lex non distinguit, nec nos distinguere debemus*, por lo que refiere a un probable y complejo debate sobre los bienes intangibles digitales y si estos pudieren ser considerados susceptibles de apropiación y sucesión. En prudente seguimiento a lo expuesto al capítulo anterior, los bienes digitales forman parte del patrimonio y en el entendido que un testamento puede abarcar todo éste o parte de él, cualquier distinción fuera de esta regla resultaría inverosímil y contrario a derecho, en este caso, en perjuicio de los usuarios de las plataformas que permiten la reproducción del contenido multimedia que han adquirido conforme a derecho.

Sin que resulte óbice a lo anterior que las legislaciones civiles a nivel internacional no prevean la figura del testamento de bienes digitales, ya que esto implicaría realizar una distinción onerosa y perjudicial respecto de cualquier interpretación que pudiere beneficiar al otorgante.[9] Se fortalece lo anterior, si recordamos que en sistemas que pertenecen a la protección autoral *copyright* y que reconocen la doctrina "De la Primera Compra", se otorga facultad al adquirente para prestar, revender o regalar cualquier soporte físico o electrónico que contenga propiedad intelectual, sin obtener la autorización del titular de derechos de autor, según se desprende la sección 109, de la *Copyright Act of America;*[10] esto respetaría el concepto de patrimonio

[9] En España, según lo prescribe la Ley de Jurisdicción Voluntaria (Ley 15/2015 de 2 de julio) [Legislación refundida Normativa Estatal], se permite la celebración de testamento a través de cualquier mecanismo que permita capturar la voluntad del otorgante, sin importar si esto ocurre en material análogo, digital o magnético, en tanto permita acreditar que efectivamente contiene la voluntad del fallecido.

[10] COPYRIGHT GOV. *Chapter 1.1: Subject Matter and Scope of Copyright. Section 119. Limitation on exclusive rights: Secondary transmissions of distant television programming by satellite.* Puede consultar el texto íntegro en el vínculo https://www.copyright.gov/title17/92chap1.html#109 visto el 11 de noviembre de 2017.

que se indica, así como el de **dominio** que pretendemos defender; empero, el modelo de negocio y licenciamiento que proponen las grandes desarrolladoras invitan a la deconstrucción del concepto *compra*, en perjuicio de la transparencia a favor de los consumidores, ya que no sólo las dos empresas que hemos referido anteriormente operan bajo dicha mecánica comercial, también sumamos a la lista a proveedores como Netflix o Spotify, sólo por mencionar algunos. Es meritorio señalar que esta doctrina se encuentra presente de forma análoga en el caso mexicano, en nuestra Ley Federal del Derecho de Autor, cuyo artículo 38 prescribe:

> **ARTÍCULO 38.**- El derecho de autor no está ligado a la propiedad del objeto material en el que la obra esté incorporada. Salvo pacto expreso en contrario, la enajenación por el autor o su derechohabiente del soporte material que contenga una obra, no transferirá al adquirente ninguno de los derechos patrimoniales sobre tal obra.[11]

Tal precepto permite percibir que la doctrina y la ley (mexicana y americana), sostengan el entendimiento de la separación entre los derechos de autor y el soporte material, en tanto que la suerte de la adquisición del material en el que se fija una obra no transfiera de forma automática los demás derechos sobre la música, video o imagen (verbigracia). Así las cosas, el propietario puede enajenar el bien soporte (físico o digital), sin que esto implique licenciamiento de derechos patrimoniales (*copyleft* en el sistema americano).

Por ahora, parece que la mecánica que proponen los proveedores de servicio *streaming* y de almacenamiento masivo digital no respeta la distinción expuesta y jamás coloca a consideración del usuario la probable adquisición del archivo que contiene la pista, el *ebook*, o cualquier contenido multimedia, sino que sólo permite el uso restringido de dicho contenido, siempre que se respeten las condiciones de los propios desarrolladores.

Hasta este punto, he brindado al lector un caso práctico para advertir la confusa normatividad que existe en Internet, pero lo endeble de la misma si es que se opone a un rígido examen jurídico y legislativo; sin embargo, esto no resuelve lo referente a otro tipo de contenido digital, que también forma parte del patrimonio, como lo pueden ser nombres de usuario y contraseñas. Al respecto, el debate permite un distinto nivel de interpretación, ya que de ninguna manera se podría entender que estos son otorgados en licencia intransferible a favor de los cibernautas, sino que estos son generados como elementos de identificación única y personalísima para acceder a servicios, plataformas o bibliotecas, sin que se realice transmisión de propiedad a favor de los dueños del servicio, sino únicamente se permite el uso o, en su caso, tratamiento para la debida prestación del servicio de correo electrónico, almacenamiento,

[11] Ley Federal del Derecho de Autor vigente. Puede consultar la misma a través del vínculo http://www.dof.gob.mx/nota_detalle.php?codigo=4907028&fecha=24/12/1996

envío de datos o transmisión de archivos en tiempo real, según sea el caso. En concreto y tal como se estudiará más adelante, elementos digitales similares a nombres de usuario, contraseñas o imágenes de identificación de perfiles constituyen parte fundamental del patrimonio digital y en un nivel más adecuado de lenguaje tecnológico, piezas fundamentales de los derechos de personalidad digital.

La preocupación no sólo ocupa a los usuarios,[12] sino a los proveedores de servicios de redes sociales y motores de búsqueda como lo son Facebook y Google. Al respecto, la primera plataforma que invoco cuenta con al menos 1 200 millones de usuarios registrados (2015), de los cuales mueren al menos 10 mil cada hora. Del 2004 a la fecha han fallecido 30 millones de ellos. Si a este factor, atendemos que cada cibernauta cuenta con al menos 25 cuentas de Internet[13], desde email, bancos, redes sociales y en cada plataforma almacena patrimonio digital (fotos, música, libros, películas, documentos, información de sus tarjetas de crédito, e inclusive dinero electrónico); es inconcuso que existen bienes jurídicamente tutelados —en diversas materias del Derecho— que deben captar la atención legislativa y en su caso, la de los notarios públicos que acepten testamentos sin una debida precisión de la identidad digital que se pretende suceder. El caso español es referente al respecto, ya que el Instituto Nacional de Ciberseguridad (INCIBE) reconoce que los mecanismos jurídicos nacionales e internacionales resultan inútiles frente a la sucesión del patrimonio digital, sin embargo, invita a la utilización de proveedores de servicio que administran contraseñas y contenido digital, para facilitar la sucesión o eliminación después del fallecimiento de sus clientes. En el mercado, hoy se pueden encontrar redituables compañías como lo son Planed Departure, The Digital Beyond y la más

[12] El Presidente de la Asociación de Expertos Nacionales de la Abogacía TIC (ENATIC), Rodolfo Tesone, señala que "la identidad civil digital tiene menos de 10 años de vida y no existe una regulación en ese tenido… la legislación sucesoria es del siglo pasado y no se adapta a las nuevas necesidades. Nuestra justicia es analógica" A su vez, Tesone estima que la legitimación de los sucesores o albaceas sobre un testamento digital, podrían enfrentarse a figuras jurídicas tradicionales que terminarían por enfrentarlos a delitos de usurpación de identidad, vulneración de protección de datos personales o aquéllos relativos a los derechos de intimidad o propia imagen, en tanto no se autorice en el derecho positivo la figura del **legado digital.** En el propio artículo que invoco, el escritor propone realizar en el testamento un inventario exhaustivo de las actividad digitales e identificar todas las contraseñas, además de colocar la voluntad máxima del titular, ya sea la conversación, el respaldo o la eliminación total de la vida digital, en su caso, designando recursos materiales, digitales y económicos suficientes a favor del albacea para cumplimentar dicha voluntad. MORENO, V. "El testamento digital, una herencia conflictiva". *Expansión*. España, Portada, Jurídico. Abril de 2013. Puede consultar la nota completa a través del vínculo http://www.expansion.com/2013/04/18/juridico/1366302969.html visto el 13 de noviembre de 2017.

[13] *SEMANA 25*. "Testamento Digital". Tecnología. Colombia, diciembre de 2014. Puede consultar la nota completa a través del vínculo http://www.semana.com/vida-moderna/articulo/testamento-digital/395286-3 visto el 13 de noviembre de 2017.

avanzada/popular Tellmebye;[14] así como aplicaciones que permiten encriptar contraseñas como One Safe, E Wallet o iPassword; mismas que se encargan de enfatizar la necesidad de obtener un detallado análisis sobre el patrimonio digital, inventariarlo y, en su caso, determinar de la forma más puntual posible lo que habrá de ocurrir ante un probable fallecimiento, no sólo en atención a la administración de los perfiles de redes sociales, sino todos los bienes digitales y su probable difusión pública o, en su caso, la inminente eliminación.

En seguimiento al progreso de la sociedad digital, Google y Facebook han dictado el camino que otras redes sociales pretenden seguir mediante la proposición del **legado digital**. Hasta ahora, a esta figura se le comprende como la facultad del usuario para determinar el destino que tendrá su identidad digital, así como la designación de una o más personas que darán debido cumplimiento a su voluntad, previo a su desaparición o muerte, en tanto que ésta podrá ser "modificación, publicación o eliminación", según lo proponen las plataformas de referencia. Google presenta la herramienta de "Administrador de cuentas inactivas"[15] como un mecanismo para resolver la figura de la sucesión digital bajo tres modalidades:

1) Inactividad de la cuenta, el elemento *sine qua non* para activar el protocolo de los siguientes comandos. El usuario puede configurar la cantidad de tiempo, en el cual Google podrá considerar que la cuenta fue abandonada por desaparición o muerte del usuario.
2) Notificación y compartir permite a Google, brindar acceso a una persona que funge como "albacea" o "legatario" de los datos que componen la identidad digital del fallecido. Esta función dotará al tercero de facultades suficientes para descargar lo contenido en las siguientes plataformas: +1s, Android Pay, Bookmarks, Calendar, Chrome, Contacts, Drive, Fit, Google Photos, Google Play Books, Google + Stream, Groups, Handsfree, Hangouts, Hangouts on Air, Keep, Location History, Mail, Maps, My Maps, Profile, Searches, Tasks,

[14] Tan sólo en mayo de 2015, *Tellmebye* logró obtener el primer testamento digital firmado ante notario público que incluye el legado de sus usuarios; éxito que permitió anunciar una versión mejorada con prueba beta en Valencia, España. *Tellmebye* nace en noviembre de 2013 como la primera herramienta web pensada para aquellas personas que quieran dejar planificada la herencia de todo su legado digital y facilitar así, la entrega de documentos, mensajes, recuerdos o contenidos a familiares y/u otras personas. Desde su lanzamiento, la plataforma ha registrado **8 900 herencias digitales.** A principios de 2015 Tellmebye inicia su expansión internacional en el mercado latinoamericano, concretamente en México. *DIARIO CRÍTICO.* "Tellmebye, el primer testamento digital ante notario". Emprendedores 2020. España, Mayo de 2015. Puede consultar la nota completa a través del vínculo https://www.diariocritico.com/noticia/479213/emprendedores-2020/tellmebye-el-primer-testamento-digital-ante-notario.html visto el 13 de noviembre de 2017.

[15] GOOGLE. *Administrador de cuentas inactivas.* https://myaccount.google.com/inactive Visto el 13 de noviembre de 2017.

Wallet y Youtube; y en su caso, que dé seguimiento a la eliminación de los datos personales.

3) Eliminación de cuenta inactiva es la herramienta que permite al usuario la posibilidad de la desaparición total de la cuenta Google, junto con el contenido que hubiese generado. En estricto sentido, éste no corresponde al ejercicio del derecho al olvido, pero sí una cercana aproximación para evitar el *limbo digital* que es reconocido por algunos estudios en la materia como el *testamento digital inverso*. Por su lado, Facebook pone a disposición de sus usuarios la herramienta: "Tu contacto de legado", la cual se define como "la persona que eliges para que administre tu cuenta cuando fallezcas". Podrá realizar ciertas acciones como fijar una publicación en tu biografía, responder a nuevas solicitudes de amistad y actualizar tu foto del perfil.[16] A éste se le puede permitir descargar una copia de lo que el usuario ha compartido en la red social, el cual contiene publicaciones, fotos, videos y datos de la sección de "información" del perfil; asimismo, la red social permite la eliminación de la cuenta tras el fallecimiento del titular, como medida alternativa a la selección de un contacto de legado.

En el caso de otras redes sociales como Twitter, Instagram o correos electrónicos diversos a la plataforma de Gmail, reconocen la figura de las cuentas conmemorativas o, en su caso, permiten la posibilidad de eliminación de la cuenta del usuario fallecido, siempre que se acredite la legitimación con la que se pretende actuar y exhibir documento público que contenga la fecha cierta del fallecimiento. Sólo en el caso de Twitter, la cuenta no podrá eliminarse, aunque permite obtener una copia pública de cada uno de los tweet emitido por el usuario desaparecido (*Testamento Digital Inverso*, dicho término se define más adelante). Por ahora, esta salida parece no contrariar lo previsto por la doctrina y la legislación en lo referente al legado.

El *Diccionario Jurídico Mexicano* define al legado como la adquisición a título particular sin más carga que la expresamente impuesta por el testador, sin perjuicio de su responsabilidad subsidiaria con los herederos; es decir, se entiende como una atribución patrimonial *mortis causa* a título particular.[17] Lo curioso sobre la figura que acontece en el ciberespacio, sería la falta de solemnidad en el acto, que bien podría invalidar la voluntad del usuario ante los ojos de visiones más ortodoxas, sin

[16] FACEBOOK. ¿Qué es un contacto de legado de Facebook? https://www.facebook.com/help/1568013990080948 Visto el 13 de noviembre de 2017.

[17] LÓPEZ MONROY, José; *et al. Diccionario Jurídico Mexicano. Legado*. Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas. Tomo VI L-O Segunda Parte. México, 1982. Puede consultar la definición completa en el vínculo https://biblio.juridicas.unam.mx/bjv/detalle-libro/1173-diccionario-juridico-mexicano-t-vi-l-o visto el 13 de noviembre de 2017

embargo, parece ser una opción jurídica y legislativamente válida la que ofrecen estas plataformas digitales.

Jurídicamente, parece clara la postura que deberían adoptar los notarios —al menos del sistema latinoamericano—, así como las autoridades jurisdiccionales que tengan en sus manos determinar el destino de la sucesión digital; al permitir que los testadores incluyan su patrimonio digital en el testamento ya sea en forma de herencia o legado, sin importar las condiciones "comerciales" que propongan las redes sociales en detrimento del patrimonio digital consagrado; sin embargo, éste es sólo el inicio del camino y existen algunos casos de éxito que vale la pena destacar sobre la voluntad digital:

I. En Francia se instituyó la Ley *N° 2016-1321* de 07 de octubre de 2016 para una República Digital,[18] cuyo artículo 40-1, insertado y publicado el 08 de

[18] WIPO/ OMPI. *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique*. Francia. Fecha de entrada en vigor: 9 de octubre de 2016. Idioma Original: Francés. El texto original de la ley y artículo de referencia, dictan: « Art. 40-1. – I. – Les droits ouverts à la présente section s'éteignent au décès de leur titulaire. Toutefois, ils peuvent être provisoirement maintenus conformément aux II et III suivants. « II. – Toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières. « Les directives générales concernent l'ensemble des données à caractère personnel se rapportant à la personne concernée et peuvent être enregistrées auprès d'nn tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés. 8 octobre 2016 JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE Texte 1 sur 96 « Les références des directives générales et le tiers de confiance auprès duquel elles sont enregistrées sont inscrites dans un registre unique dont les modalités et l'accès sont fixés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés. « Les directives particulières concernent les traitements de données à caractère personnel mentionnées par ces directives. Elles sont euregistrées auprès des responsables de traitement concernés. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation. « Les directives générales et particulières définissent la manière dont la personne entend que soient exercés, après son décès, les droits mentionnés à la présente section. Le respect de ces directives est sans préjudice des dispositions applicables aux archives publiques comportant des données à caractère personnel. « Lorsque les directives prévoient la communication de données qui comportent également des données à caractère personnel relatives à des tiers, cette commnnication s'effectue dans le respect de la présente loi. « La personne peut modifier ou révoquer ses directives à tout moment. « Les directives mentionnées au premier alinéa du présent II peuvent désigner nne personne chargée de leur exécution. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. A défaut de désignation ou, sauf directive contraire, en cas de décès de la personne désignée, ses héritiers ont qualité pour prendre connaissance des directives au décès de leur auteur et demander leur mise en œuvre aux responsables de traitement concernés. « Toute clause contractuelle des conditions générales d'utilisation d'un traitement portant sur des données à caractère personnel linnitant les prérogatives reconnues à la personne en vertu du présent article est réputée non écrite. http://www.wipo.int/edocs/lexdocs/laws/fr/fr/fr502fr.pdf Visto el 13 de noviembre de 2017.

octubre de ese mismo año en el *Diario Oficial de la República Francesa* **protege los derechos humanos en la sociedad digital:**

Art. *40-1.* - I. - Los derechos de extinción sobre la preseute sección le pertenecen a su propietario. Sin embargo, pueden ser mantenidas temporalmente en conformidad con la siguiente II y III.

II. - Cualquier persona puede establecer directrices para la conservación, eliminación y divulgación de sus datos personales después de la muerte. Estas directrices son de carácter general o específico. Las directrices se refieren todos los datos personales relativos a la persona de que se trate y pueden estar registrados con una tercera parte de confianza digital, certificado por la Comisión Nacional de Informática y Libertades. Referencias directrices generales y la tercera parte de confianza a los que están registrados se registran en un registro único, los términos y acceso se establecen por decreto del Consejo de Estado, tomadas después de un dictamen motivado y publicado de la Comisiou Nacioual TI y las libertades. Las directivas específicas con respecto al tratamiento de datos personales mencionados eu dichas directivas. Ellos están registrados con los funcionarios de procesamiento. Están sujetos a la autorización expresa de la persona interesada y pueden no resultar únicamente de la aprobación por el último de los términos y condiciones. Las directrices generales y específicas definen la forma en que la persona tiene la intención de que votarou, después de su muerte, los derechos mencionados en esta sección. La adhesión a estas directrices es sin perjuicio de las disposiciones aplicables a los registros públicos que contienen datos de carácter personal. Cuando las directivas proporcionan comunicaciones de datos que también contienen datos personales relativos a terceras personas, esta comuuicación está de acuerdo con esta Ley. La persona puede modificar o revocar sus directrices en cualquier momento. Las directrices mencionadas en el primer párrafo de la fracción II permiten designar a una persoua responsable de su ejecuciou. Esta calidad entonces cuando la persona que murió, para comprender las pautas y buscar su aplicación a los funcionarios de procesamiento. A falta de designaciou o, a menos que le indique lo contrario, en caso de fallecimiento de la persona designada, los herederos tienen derecho a recibir instrucciones para la muerte del autor y pedir su aplicación a los funcionarios de procesamiento. Cualquier cláusula contractual de las condiciones generales de uso de un tratamiento que incluya datos personales que limitan las prerrogativas de la persona bajo esta sección se tendrá en cuenta.

III. - En ausencia de directrices o de otra manera se menciona en esas directivas, los herederos de la persona interesada puede ejercer después de su muerte los derechos mencionados en esta sección en la medida necesaria:

- para el asentamiento organización y raíces los difuntos. Como tal, los herederos pueden acceder a los datos personales relativos al tratamiento de ideutificar y obtener la comunicación de información relevante para la liquidación y distribución de

los bienes. También pueden recibir la comunicación de bienes digitales o datos que ascienden a los recuerdos familiares, transmisible a los herederos;

- para su examen por el tratamiento responsable de la muerte. Como tal, los herederos pueden proceder con el cierre de las cuentas de los usuarios fallecidos, se oponen a la continuación del tratamiento de datos personales o hacer que se actualizan. Cuando los herederos así lo soliciten, el controlador de datos deben justificar, sin coste alguno para el solicitante, que ha realizado las operaciones requeridas en términos del tercer párrafo de esta fracción III. Los desacuerdos entre los herederos en el ejercicio de derechos en virtud de este III se presentan ante el alto tribunal competente.

IV. - Cualquier proveedor de un servicio público de comunicación en línea informara al usuario sobre el destino de los datos relativos a él en su muerte y le permitirá elegir o no comunicar sus datos a un tercero que designa; incluido el conjunto de directrices para el destino de sus datos personales después de la muerte.
[...]

Este texto no sólo reconoce la posibilidad de atender la voluntad de una persona sobre su identidad digital, además otorga la calidad de derecho humano a la prerrogativa que tiene el cibernauta respecto de su patrimonio digital en la sociedad virtual. El testamento que atiende la ley que se invoca concentra su atención en dos bienes jurídicos tutelados: los datos relativos a la identificación del cibernauta (*derechos de personalidad)* y los *datos personales*. Adicionalmente, me adhiero a la fortaleza y rigor que brinda la presente ley, ya que la misma involucra a la esfera gubernamental en la atención al reconocimiento de un testamento público y la inclusión que tiene el gobierno sobre la protección de los datos personales de sus ciudadanos, inclusive sobre cualquier ventaja jurídica de los proveedores de Internet.

Finalmente, concluye por dictar que los proveedores de cualquier tipo de servicio en línea, se obligan a informar el tratamiento de los datos personales, ante el fallecimiento del usuario. Para aquéllos poco familiarizados con la materia, parecería una nota distintiva absurda o inatendible, sin embargo, es prudente destacar que a nivel internacional, no existe precedente legislativo que permita la protección de datos personales de una persona fallecida mediante la figura de la sucesión y son pocos los precedentes jurisdiccionales que se han dictado alrededor del globo. A pesar de la pobre traducción que el presente escritor pudiere brindar sobre el texto original, en francés, se percibe el espíritu de la ley parisina y el bello antecedente que brinda al derecho positivo internacional, no sólo por reconocer la existencia de bienes digitales dignos de protección subjetiva, sino que fortalece la necesidad de la participación gubernamental para la debida sucesión del patrimonio digital mediante la figura del testamento.

II. El pasado febrero de 2017, el *Govern* en Catalunya aprobó el anteproyecto de ley sobre voluntades anticipadas que dicta la posibilidad de heredar *bienes digitales* y se faculta al otorgante la vía para designar un legatario que determine la conservación, modificación o eliminación del mismo. Hasta mayo de 2017, la ley catalana permitía el registro de "Últimas voluntades", sin embargo, la aprobación del *Parlament*, generó la posibilidad de un registro especial para "Voluntades Digitales" y la designación de "herederos digitales". [19] De tal suerte, la *Ley 10/2017 e 27 de junio, de las voluntades digitales y de modificación de los libros segundo y cuarto del Código Civil de Cataluña,*[20] dicta en su artículo 6°, cuya modificación corresponde al artículo 411-10 del Código civil de Cataluña, lo siguiente:

[19] JANÉ, Carmen. "Testamento digital: ¿qué pasará con tu Facebook cuando hayas muerto?" *El Periódico*. Sociedad. Barcelona 28 de febrero de 2017. Puede consultar el texto completo a través del vínculo http://www.elperiodico.com/es/sociedad/20170228/testamento-digital-ley-catalunya-5865493 visto el 13 de noviembre del 2017.

[20] Ley 10/2017, de 27 de junio, de las voluntades digitales y de modificación de los libros segundo y cuarto del Código civil de Cataluña. Comunidad Autónoma de Cataluña. 21 de julio de 2017. Puede consultar el texto íntegro, a través del vínculo https://www.boe.es/diario_boe/txt.php?id=-BOE-A-2017-8525 visto el 13 de noviembre de 2017. Al respecto, me permito fijar sobre la presente obra con fines de acervo histórico, la exposición de motivos que brinda el Parlamento de Cataluña, previo a la aprobación –aún en nombre del Rey de España-: "Preámbulo. I. Las personas utilizan cada vez con más frecuencia los entornos digitales para desarrollar las actividades de su vida personal y profesional. Estas actividades generan una diversidad de archivos que, una vez muerta la persona, también forman su legado. Del mismo modo, después de la muerte pueden quedar unos derechos y unas obligaciones de naturaleza jurídica diversa sobre los diferentes archivos que haya generado la actividad de los prestadores de servicios, respecto a los cuales debe decidirse qué hacer. A menudo, los contratos que se suscriben con los prestadores de servicios digitales o las políticas que estos tienen en vigor no establecen qué sucede cuando la persona muere o cuando tiene la capacidad judicialmente modificada y, por lo tanto, cuál debe ser el destino de los archivos digitales. La legislación vigente en materia de sucesiones no da respuesta a estas cuestiones. Además, en el ámbito de las interacciones que se producen en las redes sociales a menudo nos encontramos ante derechos de carácter personalísimo que se extinguen con la muerte de la persona. Estas cuestiones y otras relacionadas han comenzado a generar inquietud en la ciudadanía y todo hace prever que esta inquietud se incrementará a medida que se extienda el uso de las redes sociales y la presencia de las personas en estas redes y, en general, en los entornos digitales. Conviene, pues, establecer unas normas que permitan determinar cómo debe administrarse el legado relativo a la actividad de cada persona en los entornos digitales.

Para gestionar la huella en los entornos digitales cuando la persona muere o cuando tiene la capacidad judicialmente modificada y para evitar daños en otros derechos o intereses tanto de la propia persona como de terceros, la presente ley establece que las personas pueden manifestar sus voluntades digitales para que el heredero, el legatario, el albacea, el administrador, el tutor o la persona designada para su ejecución actúen ante los prestadores de servicios digitales después de su muerte o en caso de tener la capacidad judicialmente modificada. Mediante estas voluntades digitales, las personas pueden ordenar las acciones que consideren más adecuadas para facilitar, en caso de muerte, que la desaparición física y la pérdida de personalidad que supone se extiendan igualmente a los entornos digitales y que eso contribuya a reducir el dolor de las personas que les sobrevivan y de las personas con las que

Artículo 411-10. Voluntades digitales en caso de muerte.

1. Se entiende por *voluntades digitales en caso de muerte* las disposiciones establecidas por una persona para que, después de su muerte, el heredero o el albacea universal, en su caso, o la persona designada para ejecutarlas actúe ante los prestadores de servicios digitales con quienes el causante tenga cuentas activas.
2. El causante, en las voluntades digitales en caso de muerte, puede disponer el contenido y el alcance concreto del encargo que debe ejecutarse, incluyendo que la persona designada lleve a cabo alguna o algunas de las siguientes actuaciones:

   a) Comunicar a los prestadores de servicios digitales su defunción.
   b) Solicitar a los prestadores de servicios digitales que se cancelen sus cuentas activas.
   c) Solicitar a los prestadores de servicios digitales que ejecuten las cláusulas contractuales o que se activen las políticas establecidas para los casos de defunción de los titulares de cuentas activas y, si procede, que le entreguen una copia de los archivos digitales que estén en sus servidores.

3. Las voluntades digitales pueden ordenarse por medio de los siguientes instrumentos:

tengan vínculos familiares, de afecto o amistad, o bien que se perpetúe la memoria con la conservación de los elementos que estas determinen en los entornos digitales o con cualquier otra solución que consideren pertinente en ejercicio de la libertad civil que les corresponde en vida. Estas mismas acciones deben poder ordenarse, cuando se goza de plena capacidad de actuar, para el caso de que se produzca una pérdida sobrevenida de esta capacidad.

...II. Las voluntades digitales pueden ordenarse no únicamente mediante testamento, codicilo o memorias testamentarias, sino también, en defecto de disposiciones de última voluntad, mediante un documento de voluntades digitales que debe inscribirse en el Registro electrónico de voluntades digitales, un nuevo instrumento registral de carácter administrativo que se crea con el objetivo de facilitar e incrementar las vías disponibles para dejar constancia de las voluntades digitales.

Complementariamente, se precisa que la persona encargada de ejecutar las voluntades digitales también puede designarse mediante todos los instrumentos que pueden utilizarse para ordenarlas y se completa la regulación del modo sucesorio del libro cuarto del Código civil de Cataluña para incluir la ejecución de las voluntades digitales del causante.

(...) La regulación propuesta también tiene presente...deben fomentar que estas tecnologías se pongan al servicio de las personas y no afecten negativamente a sus derechos, y deben garantizar la prestación de servicios mediante dichas tecnologías, de acuerdo con los principios de universalidad, continuidad y actualización.

Se tienen presentes, asimismo, los principios y disposiciones de la Convención sobre los derechos de las personas con discapacidad, aprobada en Nueva York el 13 de diciembre de 2006 y ratificada por el Estado español el 21 de abril de 2008, principios y disposiciones que ya han sido objeto de recepción por parte del Código civil de Cataluña y de las modificaciones de que ha sido objeto a partir de la aprobación de la mencionada Convención."

a) Testamento, codicilo o memorias testamentarias.
b) Si la persona no ha otorgado disposiciones de última voluntad, un documento que debe inscribirse en el Registro electrónico de voluntades digitales.

4. El documento de voluntades digitales se puede modificar y revocar en cualquier momento y no produce efectos si existen disposiciones de última voluntad.
5. Si el causante no ha expresado sus voluntades digitales, el heredero o el albacea universal, en sn caso, pnede ejecutar las actuaciones de las letras *a*, *b* y *c* del apartado 2 de acuerdo con los contratos que el causante haya suscrito con los prestadores de servicios digitales o de acuerdo con las políticas que estos prestadores tengan en vigor.
6. Si el causante no lo ha establecido de otro modo en sus voluntades digitales, la persona a quien corresponde ejecutarlas no puede tener acceso a los contenidos de sus cuentas y archivos digitales, salvo que obtenga la correspondiente autorización judicial.
7. Si el causante no lo ha establecido de otro modo, los gastos originados por la ejecución de las voluntades digitales corren a cargo del activo hereditario.

Tal modificación legislativa no sólo altera las condiciones del código civil de aquella comunidad autónoma, además determina la supremacía de la ley sobre cualquier disposición "comercial" que se pudiere pactar ante las redes sociales, es decir, se pondría fin a las condiciones leoninas o paralegales que proponen las diversas plataformas para unificar el comportamiento de los cibernautas a la vigilancia gubernamental, mediante el reconocimiento de los bienes digitales tales como fotos, música, videos, software, libros, reputación e inclusive archivos que se almacenen en la nube y la posibilidad jurídica de disponer de todos ellos mediante la fórmula jurídica del testamento.

Por ahora, en Inglaterra se encuentra en proceso de revisión legislativa la figura del Testamento *online* y casos de éxito legislativo como los antes invocados, podrían ser la piedra angular en la aceptación del testamento digital, máxime con la importancia de la protección del patrimonio digital a favor de los cibernautas. No es el objeto del presente capítulo, proponer la integración de dos figuras paralelas testamentarias, sino que los Estados ocupen su atención a las conductas que ocurren en la red de redes y en su caso, permitan la integración de las mismas a los testamentos tradicionales, ya que la principal condición que propongo no es la necesidad de creación de un testamento *ad hoc* a cada hipótesis virtual, sino la búsqueda del seguimiento gubernamental y jurisdiccional frente al incumplimiento de proveedores de servicios digitales y redes sociales, que pretenden imponer sus políticas, términos y condiciones, respecto de lo prescrito en la Ley. Es decir, debería imperar lo contenido en la ley frente a confusas interpretaciones de "compra" (verbigracia, iTunes) en dichas plataformas, por lo que debería permitirse su libre sucesión conforme lo

dicten los códigos civiles de cada nación; lo mismo respecto a usuarios, contraseñas o cualquier dato personal en posesión de proveedores de servicios virtuales, sin establecer condiciones superiores a las prescritas en el derecho positivo.

Ahora bien, sin que parezca que justifico el poder de dichas normas consuetudinarias, me parece que el camino hacia la debida sucesión digital lo han marcado legislaciones similares a la francesa y la catalana, que han determinado la relevancia del testamento digital y el testamento digital inverso, no sólo como un derecho civil, sino como un derecho humano superior frente a otros subjetivos de menor categoría. Esto es, el testamento digital resulta una figura jurídica novedosa y necesaria para los millones de cibernautas que conectan su vida a la red de redes, de estudio meritorio para los abogados del siglo XXI y de análisis obligado para notarios públicos y entidades gubernamentales que tienen a su cargo registros digitales.

III
CAPÍTULO

Jurisdicción en Redes Sociales[1]

El relator especial para la Libertad de Expresión de las Naciones Unidas, Frank La Rue, despertó al *Leviatán* jurídico cuando en 2011 emitió su reporte al Consejo sobre Derechos Humanos en Internet de las Naciones Unidas, respecto del uso de las tecnologías y el uso de Internet para la expresión de ideas y la adquisición de información. Tal como se estudiará más adelante en el desarrollo de la presente Obra, dicho reporte tuvo como origen que algunos medios alrededor del mundo, anunciaran que la Organización de las Naciones Unidas, finalmente hubo reconocido el "Derecho Humano de Internet". Esta aseveración fue incorrecta jurídica, metodológica y semánticamente, no sólo porqué La Rue no emitió dicha afirmación, sino porque el sentido de su reporte fue defender a Internet como el mecanismo, por excelencia, para manifestar y ejercer la libertad de expresión, un derecho fundamental consagrado de forma universal.

Sin embargo, el impacto de este reporte tuvo consecuencias favorables para el Derecho Positivo, como lo fue la *Carta de Derechos Humanos y Principios para Internet,* emitida en 2011 dentro del marco del Foro de la Gobernanza de Internet

[1] LIMÓN, Jaime. Obra versionada de la obra original publicada bajo el título *El Origen del mundo: Crítica al Sistema Normativo en Facebook.* Foro Jurídico. Diciembre de 2016. Se puede consultar la obra primigenia a través del vínculo https://www.forojuridico.org.mx/origen-del-mundo-critica-al-sistema-normativo-facebook/

de las Naciones Unidas. De este documento se desprende un decálogo de principios que favorecen las libertades de los internautas, además, propone 20 artículos que pretenden servir como marco normativo para que las Naciones involucradas ajusten sus legislaciones. Destaca el artículo 20, relativo a las Obligaciones y Responsabilidades en Internet, del cual se desprende la "**Responsabilidad de los poderosos".** Según la Carta que nos ocupa, consiste en la responsabilidad de los "que ejercen el poder" y obliga a estos a actuar de forma responsable y abstenerse de violar Derechos Humanos, respetarlos, protegerlos y cumplirlos en la mayor medida de lo posible. Lo anterior, en irrestricto cumplimiento al artículo 29 de la Declaración Universal de Derechos Humanos, que consagra el deber de las personas con la comunidad, puesto que sólo en ella puede desarrollar libre y plenamente su personalidad. Tal como lo sostuviera Rousseau en *El Contrato Social*: "Los compromisos que nos ligan con el cuerpo social no son obligatorios sino porque son mutuos, y su naturaleza es tal, que al cumplirlos, no se puede trabajar por los demás sin trabajar por sí mismo". Empero, la Responsabilidad de los poderosos no siempre parece ser clara y en algunas ocasiones, actúan de forma leonina en perjuicio de sus usuarios y la *cibercomunidad*, olvidando el pacto y respeto que mutuamente se deberían rendir, conforme los acuerdos que firman en la red. A ello hay que sumar, que estos "poderosos" a los que hace referencia la Carta de las Naciones Unidas, no sólo hace referencia a las Naciones, ya que hoy en día, plataformas como Facebook y Google han adquirido fortaleza mediática, social y política, que les permite ser *influencers* de nuestra realidad; por lo anterior, es prudente analizar la forma en que estos proveedores de servicio, actúan frente a sus usuarios, sobre en todo en la imposición de cláusulas que pudieren considerarse ventajosas en perjuicio de derechos fundamentales, como lo son la libertad de expresión y el derecho a obtener información de la red.

En ese tenor, el pasado 12 de febrero de 2016 el Tribunal de Gran Instancia de París confirmó la sentencia dictada por el Tribunal de Primera Instancia en la que se determina que la cláusula de "competencia exclusiva" de la "Declaración" de Facebook resulta excesiva y abusiva frente a los usuarios del servicio de la red social americana. Esta decisión no sólo sentó precedente jurisdiccional a nivel internacional para debilitar al cuerpo de abogados que defienden el legado de Zuckerberg, sino que permite rescatar el interés jurídico de los particulares frente a grandes maquinarias de defensa como lo es la famosa red.

A saber, existen dos elementos que deben generar sumo interés no sólo entre los internautas, sino entre los estudiosos de derecho que deberán derribar un par de paradigmas sobre las ficciones jurídicas en la red: *1)* ¿Se puede determinar jurisdicción particular sobre una plataforma con presencia mundial?, y *2)* ¿Las plataformas en la red de redes cuentan cou "soberanía" suficiente para determinar el valor jurídico de la información que se comparte a través de sus herramientas? El iluminado camino hacia estas respuestas puede ser el caso Durand Baissas vs

Facebook Inc.,[2] juicio que se instauró el 04 de octubre de 2011, después que la plataforma decidiera "inhabilitar" la cuenta del profesor francés Fréderic Durand Baissas, tras publicar una fotografía en la que se reflejó la obra *L'Origine du Monde [El origen del mundo]* (1866), del pintor francés Courbet, que muestra los genitales de una dama. Al parecer de las Condiciones y Políticas de Datos de Facebook, dicha imagen no era "arte" o "una obra" sino pornografía.

Podríamos estar en presencia de una hipótesis abierta al debate e interpretación, sin embargo, esto resulta inverosímil ante las estrictas normatividades de una red social como lo es Facebook, en la que bien, podría considerarse juez y parte, a conveniencia, de la censura del contenido que éste mismo tutela.

Para ser críticos y objetivos es imperante acudir a las nociones elementales de nuestro lenguaje cuando nos encontramos ante la disputa de dos conceptos, cuya línea de interpretación sea tan ligera como la que hoy en día nos enfrentamos. La Real Academia Española define *pornografía* como "la presentación abierta y cruda del sexo que busca producir excitación", siendo ésta la acepción más simple de llevar al ámbito práctico. Difícilmente podremos encontrar si fue la intención de Gustave Courbet excitar a su público, sin embargo, un estudio hermenéutico detrás de su intención resulta absurdo ante el debate que nos ocupa, ya que Facebook ha delimitado lo que ha de considerarse pornografía, específicamente **desnudos** para efectos de las Normas de la Comunidad (Facebook):

> A veces, la gente comparte desnudos con un fin determinado, por ejemplo, campañas de concientización o proyectos artísticos. Restringimos la exhibición de desnudos para evitar que determinados sectores de nuestra comunidad mundial que muestran una especial sensibilidad ante ellos se puedan sentir mal, en particular, por su contexto cultural o su edad. Para tratar a todos de una forma justa y responder a los reportes con rapidez, es fundamental contar con políticas que nuestros equipos en todo el mundo puedan aplicar fácilmente y con uniformidad al revisar el contenido. Como resultado, nuestras políticas pueden ser a veces más directas de lo que nos gustaría y restringir contenido compartido con fines legítimos. Trabajamos constantemente para mejorar la evaluación de este contenido y la aplicación de nuestras normas. Eliminamos fotografías que muestren los genitales o las nalgas en su totalidad y de una forma directa. También restringimos algunas imágenes de senos femeninos si se muestra el pezón, pero siempre permitimos fotos de mujeres amamantando o que muestren los pechos con cicatrices por una mastectomía. **También permitimos fotografías de pinturas, esculturas y otras obras de arte donde se muestren figuras desnudas**.

[2] COUR D' APPEL DE PARIS. *Arrêt Du 12 Février 2016. Décision déferée á la Cour: Ordonnance du 05 Mars 2015- Tribunal de Grande Instance de PARIS- RG n° 12/12401.* Número de apelación 15/08624. París, Francia, 2016. Visto el 28 de septiembre de 2018 a través del vínculo http://www.clauses-abusives.fr/wp-content/uploads/2016/05/CAP12022016.pdf

> Las restricciones sobre la exhibición de desnudos y actividades sexuales también se aplican al contenido digital, a menos que dicho contenido se publique con fines educativos, humorísticos o satíricos. Se prohíben las imágenes explícitas de relaciones sexuales. También podemos eliminar descripciones de actos sexuales que sean demasiado gráficas.[3]
> [El énfasis es añadido]

En términos de la Norma que invoco y una estricta interpretación al concepto de *pornografía* proporcionado por nuestro diccionario, resulta inconcuso que la imagen *El Origen del Mundo* no constituye una violación a las reglas de la comunidad, sin embargo, dicha leyenda normativa apareció como una reforma posterior a la demanda interpuesta por el profesor francés Durand, lo que podría comprenderse como un aliciente para el inicio en la reparación del daño generado, empero, el demandante no retiró su demanda, sino que continuó con la exigencia de la reparación por un monto superior a los 20 mil euros por los daños y perjuicios generados ante la inhabilitación de su perfil, ostentando como principal argumento accionante: "la violación a su libertad de expresión".

Las anteriores consideraciones generan suficientes dudas razonables para comenzar el estudio del sistema normativo detrás de una red social cómo Facebook y analizar, a nuestro leal saber, si efectivamente resulta sólido el argumento de Caroline Lyannaz (abogada de la plataforma) sobre la falta de competencia de cualquier tribunal para juzgar a *Mark* y compañía, fuera del territorio americano; argumento que fue desechado en la apelación interpuesta en contra de la resolución de primera instancia. Por otra parte, apenas en febrero de 2018, la abogada francesa Lyannaz, argumentaría en audiencia pública, que "desconocen" las razones por las cuales *Facebook Ireland, Limited*, determinó suspender la cuenta de Durand-Baissas, asimismo, aseveró la imposibilidad de reparar materialmente la "reputación digital" del maestro de artes, pues su cuenta fue eliminada 90 días después de la suspensión definitiva que sufrió.

Para comenzar nuestro análisis, es importante destacar que la Corte francesa determinó confirmar el acto emitido por un Tribunal de primera instancia, el cual después de cuatro años de alegatos, decidió atraer la jurisdicción del caso Durand contra Facebook. Específicamente en la sentencia emitida en consecuencia de la apelación interpuesta por Facebook, Inc. dentro del expediente 15/08624, la Corte de Apelación de Paris resolvió:

a) Considerando que el artículo 132 del Código del Consumidor dispone que "[e]n los contratos celebrados entre profesionales y no profesionales o

[3] Consulta realizada el 12 de abril de 2016 a través del portal https://www.facebook.com/communitystandards. Dicha norma se reformó el pasado 19 de abril de 2018, en la cual se permiten los desnudos con fines artísticos.

consumidores, las cláusulas que tienen el propósito o efecto de crear, en detrimento del no profesional o del consumidor, un desequilibrio importante entre los derechos y obligaciones de las partes en el contrato son injustas."

b) Considerando que el artículo 132 del Código del Consumidor presume cláusulas abusivas las destinadas a "anular o impedir el ejercicio de procedimientos o recursos legales por parte del consumidor".

c) Considerando que el juez de instrucción ha señalado de forma pertinente que la cláusula que confiere jurisdicción prevista en el artículo 15 de las condiciones generales del contrato obliga al suscriptor, en caso de conflicto con la empresa, a buscar representación de un particular en el territorio americano e incurrir en costos irrazonables, sobre el beneficio económico, del contrato suscrito para necesidades personales o familiares; que las dificultades prácticas y el costo de acceso a los tribunales de California son tales que disuaden al consumidor de ejercer todas las acciones ante los tribunales que determinan la aplicación del contrato y lo privan de cualquier recurso contra la empresa que , por otro lado, tiene una agencia en Francia y posee recursos financieros y humanos que le permiten afirmar sin dificultad su representación y su defensa ante los tribunales franceses; que la cláusula en favor de la jurisdicción de los tribunales californianos contenida en el contrato tiene el efecto de crear, a expensas de los no profesionales o consumidores, un desequilibrio importante entre los derechos y obligaciones de las partes en el contrato; que también tiene el efecto de crear un obstáculo serio para un usuario francés en el ejercicio de su acción legal.

Estos años de discusión litigiosa no centraron su atención sobre el fondo de las políticas de desnudos de la plataforma —mismas que ya se han citado con anterioridad—, sino que únicamente pretendían valorar si la aceptación de jurisdicción que el usuario realizó al momento de hacer uso de los servicios de la plataforma (y renuncia implícita al fuero que le corresponde en razón de domicilio), pudiese ser considerada una disposición válida como si esto se tratare de cualquier contrato entre particulares, como efectivamente lo es.

Sin entrar al fondo del asunto, la jurisdicción francesa concedió el exceso en la cláusula de referencia y permitió entrar al fondo del asunto apenas el pasado 12 de febrero de 2016. Al respecto, ¿Facebook se encontraría facultado para argüir **violación en los términos de uso aceptados por el usuario al momento de abrir la cuenta**? La posición detrás de este argumento me parece lo suficientemente sólida, como si esto hubiese ocurrido en cualquier contrato en que las partes determinasen la jurisdicción a la que se someterían en caso de existir conflictos en la aplicación o interpretación del acuerdo aceptado, empero, los efectos detrás de la "competencia exclusiva", al menos en su construcción dictatorial, pudieron afectar la psique del juzgador para llevar esta disposición particular a ser considerada, *per* se, nula.

Ante la situación que enfrentó el profesor francés y la demanda en contra de Facebook, es recomendable el análisis de las "Condiciones y Políticas de Datos" de la plataforma, al menos en lo que merece nuestra atención al aspecto del manejo de la información, facultades de la plataforma y la propiedad intelectual que sobre ésta se vierta.

Dentro del interés procesal del demandante se encuentran, fundamentalmente, las pretensiones de la reactivación de la cuenta y una remuneración por 20 mil euros, sin embargo, pareciere que efectivamente, el profesor se vio limitado en el estudio que realizó sobre las Condiciones y Normas de la Comunidad que fundamentaron la inhabilitación que hoy en día recae sobre éste. Al respecto, existen ciertos puntos fundamentales que la defensa del profesor debe tomar en consideración y, en general, cualquier internauta que desee hacer uso de los servicios de la red:

1. **Prevalece la versión en inglés del documento:** el desconocimiento de la versión original o del alcance jurídico que pudiese lograr, no exime de su cumplimiento. En orden de preferencia, siempre se estará a lo dispuesto en la lengua americana.
2. **Facebook puede eliminar cualqnier contenido que considere que viola la Declaración**: esto consiste en una facultad unilateral sin derecho de réplica a favor de la plataforma que permite brindar un control y respeto absoluto sobre las normas que rigen Facebook y el bienestar de sus usuarios. Sin embargo, esta regla podría constituirse en uno de los primeros absurdos normativos de la red, ya que si bien es cierto los usuarios se obligan a dar un estricto cumplimiento a las reglas de la comunidad, la eliminación indiscreta de información o contenido que pudiere (o no) ser violatorio de las mismas se entiende como un examen subjetivo de los propios administradores de la herramienta. En el caso que nos ocupa, la apreciación subjetiva de la pintura *El Origen del Mundo*, pudiese generar tantas opiniones y posiciones como analistas se colocaren para el dictamen, verbigracia, quizá algunos la consideren una increíble aportación al mundo de las bellas artes, en tanto que otro grupo, pudiese considerarlo pornografía absurda y denigrante del sexo femenino. Bajo las consideraciones de las reglas sobre **Desnudos** de Facebook, no se consideraría pornografía a todos aquellos desnudos que cuenten con el calificativo de *arte*. Postura normativa, que a nuestro parecer, resulta de una compleja aplicación que pudiere generar un centenar de demandas por inhabilitaciones infundadas, en un futuro próximo.
3. **Infracciones reiteradas en materia de Propiedad Intelectual permiten inhabilitar tu cuenta:** tal como ocurre en otras plataformas en la red de redes (caso Youtube y sus estrictas reglas sobre protección en materia de derechos de autor), Facebook ha adoptado la postura de la defensa absoluta sobre la propiedad intelectual que se cargue en sus páginas, tanto al responsabilizar a los

usuarios de contar con la autorización absoluta (o ser los titulares de dichos bienes intangibles) para colocar dichas obras o marcas en sus perfiles, como al considerar mecanismos de regulación en contra de usuarios que no respeten las reglas y leyes internacionales en materia de Propiedad Intelectual. La consecuencia detrás de constantes violaciones podría ser castigada con la inhabilitación de la cuenta, independientemente de las infracciones o penas que pudieren actualizarse en el país cuya reclamación se hubiese iniciado. Es importante destacar que la cláusula de "competencia exclusiva" no opera para esta hipótesis normativa, ya que estará en libertad del autor/creador el dictaminar la mejor vía administrativa, penal o civil para solicitar la reparación del daño que se hubiese generado, así como la legislación que desee invocar al respecto, en estricto apego al principio de *personal jurisdiction.*[4]

4. **Aceptación expresa y tácita de la "Declaración":** al ser la Declaración el cuerpo normativo supremo que rige Facebook, la adhesión de la voluntad del usuario no puede generarse con reservas de ningún tipo, por lo que su redacción ha permitido que, adicionalmente a la manifestación de la voluntad expresa (clic a "Aceptar Términos y Condiciones"), se permita la aceptación expresa de las Normas de la Comunidad, por el simple hecho de hacer uso de los servicios de la plataforma. Es decir, que al ser un usuario activo de la red aceptas que deberás regir tu conducta a las reglas de la comunidad, sin que resulte óbice de cumplimiento el desconocimiento de las mismas. Adicionalmente, al aceptar la Declaración, se está adoptando el compromiso de cumplir con lo previsto en otros marcos normativos de la plataforma, tales como: *Principios de Facebook, Política de Datos y Página de la Plataforma.*
5. **Compartir el contenido y la información bajo Licencias:** una de las grandes críticas que encuentro sobre el cuerpo normativo que ocupa nuestra atención, radica en la obligatoriedad expresa que toda la información materia de propiedad intelectual que se cargue (*upload)* sobre Facebook, concede a éste la licencia no exclusiva, transferible, con derechos de sublicencia, libre de regalías y aplicable en todo el mundo. Es decir, se atenta contra el principio máximo que faculta al creador para elegir el sistema de protección que más beneficie sus interés, a saber, sistema *copyright* o sistema latinoamericano de protección de derechos de autor o bien, *trademark* en contra del sistema de derecho marcario

[4] Se considera que la jurisdicción personal es la facultad de una corte sobre las partes en un juicio. Antes de que una corte pudiese ejercer su poder sobre las partes, las legislaciones locales requieren que la parte reclamante tenga un contacto mínimo con el foro en el que ha decidido hacer valer su interés jurídico. Ésta puede perderse o mantenerse en atención a las objeciones de la parte que se estime violentada por la jurisdicción que se pretende ejercer, sin embargo, en caso de que no existen alegatos en contra de la misma, la jurisdicción invocada podría prevalecer. Para mayor referencia consultarse https://www.law.cornell.edu/wex/personal_jurisdiction así como los precedentes del caso 326 U.S.310 International Shoe Vs State Of Washington https://www.law.cornell.edu/supremecourt/text/326/310

tradicional. En el caso del sistema jurídico mexicano, el sistema de licenciamiento que propone Facebook resulta incongruente e inválido, por lo que bien se podría considerar que esta cláusula, así como la de "competencia exclusiva", es nula de pleno derecho; con la ventaja argumentativa, que permiten afirmar la ilegalidad de las cláusulas y el obvio atentado contra las disposiciones legales del Estado mexicano, sin necesidad de someterlo a interpretación.

Bajo la exégesis que el colegio de abogados de esta red social pretende ofrecer, se pensaría que Facebook cuenta con "territorialidad" en los Estados Unidos de América, por lo que materialmente es posible conocer la ubicación del bien intangible creado, sin embargo, esto no resulta aplicable por distintas consideraciones: *1)* El Autor debe decidir el momento, modo y lugar en que divulgará su obra, *2)* El Autor sólo podrá ceder de forma temporal sus derechos patrimoniales, sin que sean admisibles licencias perpetuas [no aplicable para este tipo de obras], *3)* El pago de regalías para el sistema jurídico mexicano es una relación *sine qua non* para la eficacia y validez de cualquier acto celebrado en materia de derechos de autor; por poner un ejemplo.

En términos de lo anterior, resulta inverosímil la propuesta de control de Propiedad Intelectual que nos brinda Facebook, al contener disposiciones que podrían atentar contra los cuerpos normativos de las soberanías de los autores. La licencia que pretende hacerse valer, pierde sus efectos cuando el autor elimina el contenido de la plataforma o bien, cuando se pierde sin posibilidad de ser recuperado.

6. **Conflictos/ Competencia Exclusiva:** así como el vasto universo de contratos privados que se pueden encontrar en la práctica diaria, es una recomendación absoluta que las partes dicten la jurisdicción a la que someterán la interpretación de su acuerdo de voluntades. En el caso del Contrato que se firma con esta red social, renunciamos automáticamente a la jurisdicción que por cualquier razón nos pudo haber pertenecido, para cederla a favor del Tribunal de Distrito de los Estados Unidos americanos para el Distrito del Norte de Carolina. Como bien se ha señalado con anterioridad, la Corte francesa ha sentado el precedente internacional, de que esta cláusula puede considerarse "excesiva" y por lo tanto invalida para determinar la jurisdicción a favor de cualesquiera tribunales en que el interesado haga valer su interés jurídico.
7. **Procesamiento de Datos Personales**: finalmente, una de las grandes inquietudes que se presentan en la construcción de la Declaración objeto de nuestro estudio, radica en la manipulación que la plataforma puede hacer de nuestros datos personales y la transferencia a organismos americanos para su procesamiento. Situación a la cual también se expresa consentimiento una vez que se da de alta un usuario y se comienzan a disfrutar los servicios de Facebook. Al respecto, la plataforma no indica los plazos para el ejercicio de Derechos ARCO que pudiesen hacer valer, ni la forma en que se resguardará la

> información, por lo que podríamos estar en presencia de la más grande violación a la vida privada e integridad por parte de esta Declaración. Más allá de la libertad de expresión que ha hecho valer el grupo de abogados que ostentan la defensa del profesor francés, me parece que estamos en presencia de un derecho jurídicamente más relevante que podría, automáticamente, generar el éxito de un argumento construido a favor de éste bien internacionalmente tutelado.

Conforme lo anteriormente expuesto, ha sido mi intención determinar respuesta a dos inquietudes fundamentales: ¿Se puede determinar jurisdicción particular sobre una plataforma con presencia mundial? Me parece que la respuesta la hemos encontrado en el precedente de jurisprudencia que ha dictado el Tribunal de alzada francés, en tanto que las legislaciones locales no deben permitir el éxito de contratos *leoninos* y cuya ventaja imposibilite que los usuarios puedan tener acceso a una justicia económica, pronta y expedida.

Por otro lado: ¿Las plataformas en la red de redes cuentan con "soberanía" suficiente para determinar el valor jurídico de la información que se comparte a través de sus herramientas? En atención a la información descrita en el cuerpo del presente documento, me parecería que la respuesta: no.

Lo anterior, toda vez que los particulares pueden dictar las reglas que surtan efectos entre las partes y en su caso, que protejan sus intereses y acuerdos con terceros, pero en ningún caso la voluntad de los contratantes podrá substituir el derecho positivo que los regula. En el caso de Facebook, no es permisible olvidar que esta plataforma es únicamente una herramienta que permite la prestación de un servicio, sin que esto excluya a los Tribunales de conocer sobre las violaciones que pudiesen cometerse dentro de la misma y las sanciones locales que correspondan en razón de la jurisdicción aceptada, a cargo de la razón social, la persona moral detrás de su creación y en su caso, de las responsabilidades que pudiese adquirir el mismo Mark Zuckerberg y sus accionistas.

En pleno siglo XXI enfrentamos los tabúes detrás de un desnudo artístico y la bella apreciación que un autor puede hacer al respecto. El mérito detrás de la mirada del artista, radica en brindar al espectador una visión que quizá no pudo haber contemplado por sí mismo, yace en la facultad de aproximar la mente del público a la deconstrucción de conceptos que parecieren socialmente resueltos, sin embargo, el caso que he sometido a su consideración, acredita la presencia de valores volátiles, que constituyen una ligera línea entre un exitoso interés jurídico oponible ante tribunales internacionales y un interés simple que pudiese generar un buen artículo para el periódico local. Quizá como en última época lo afirmara Kelsen[5], es imposible separar al Derecho de la moral, los valores, la ética, la economía, la cultura y en general, cualquier factor que pudiese afectar su estudio, en atención a conseguir una ciencia

[5] KELSEN, Hans. *Crítica a la Teoría Pura del Derecho*. Editorial EUDEBA. Buenos Aires, 1989.

no solamente pura, sino socialmente útil en beneficio de aquéllos que persiguen el bien supremo de la justicia.

El Origen Del Mundo nos recordó que en tratándose del debate jurídico y la construcción de nuestra ciencia, aún hace falta un largo camino por recorrer. Sin embargo, éste no parece ser un caso aislado por lo que refiere a la aceptación de las cortes locales y la adopción de juicios en contra de titanes digitales como Facebook y Google. Evidencia de lo anterior, es el caso recibido por la Corte Española en 2010, a través del cual un ciudadano demandó a Google España y Google Inc., por la indebida protección de sus datos personales; posteriormente, este caso sería resuelto por la Corte de la Unión Europea y su criterio será objeto de nuestro estudio más adelante dentro de esta obra (leer *Derecho al Olvido* en el capítulo respectivo); en ese mismo tenor, debo aplaudir el criterio que recientemente arrojó la Suprema Corte de Justicia de la Nación en el caso *Ulrich Richter vs Google,* no sólo por la respuesta a la petición del accionante, en el sentido de brindar protección constitucional a sus datos personales, sobre cualquier regla en los sitios administrados por Google Inc., sino porque la Primera Sala del máximo tribunal confirmó la sentencia en contra del máximo buscador y reconoce la competencia de los jueces mexicanos para resolver controversias en contra de dicho buscador, siempre que sus productos tengan efectos en México y la empresa cuente con domicilio legal reconocido en el país.

El Amparo en Revisión 587/2017 analizado por nuestra Corte Suprema tiene su origen en la demanda por daño moral interpuesta por Richter Morales contra Google Inc., Google México y Lino Cattaruzzi —entonces director de Google México— por la publicación de un blog difamatorio. Ante la negativa de Google para eliminar el blog, hospedado en la plataforma Blogger —propiedad y herramienta de Google, Inc. — Richter inició el procedimiento por daño moral ante el Juzgado Octavo de lo Civil de la Ciudad de México. Como respuesta a lo anterior, Ana Rosa Bobadilla Gallardo, abogada de Google Inc. en México, interpuso un recurso en el que alegó la falta de competencia de los jueces para afectar la esfera de su representada, pues ésta tiene su sede en el Condado de Santa Clara, Estados Unidos, y por tanto está sujeta a aquella jurisdicción.[6]

Finalmente, la decisión que se publicó el 6 de diciembre de 2017, en la cual también se anuncia el desistimiento de Google sobre el recurso, confirma la posibilidad de intentar acciones en contra de empresas norteamericanas, si es que sus productos tienen consecuencias en nuestro país; así parece debilitarse aún más, la antes impenetrables armaduras de los colosos digitales.

[6] RIQUELME, Rodrigo. "La suprema corte de Justicia confirma sentencia contra Google en México". *El Economista*. México, 6 de diciembre de 2017. Recuperado el 14 de diciembre de 2017 a través del vínculo https://www.eleconomista.com.mx/empresas/La-Suprema-Corte-confirma-sentencia-contra-Google-en-Mexico-20171206-0075.html

IV
CAPÍTULO

Consecuencias Jurídicas de la creación y utilización de Inteligencia Artificial

George Orwell y Philip K. Dick fueron muy precisos en los pasos para lograr el control absoluto, lejos de las libertades de la voluntad y el albedrío, a través de los futuros distópicos que sus novelas describen. El primero de ellos a través de un sistema que controla los procesos y el pensamiento de los individuos que viven dentro del mismo, gracias a mecanismos de panoptismo aplicado y sin brechas de información; mientras que el segundo coloca sobre la mesa de discusión tecnológica la incógnita sobre si los androides soñarían con ovejas electrónicas, en el entendido que su principal preocupación es la substitución del hombre hasta en las tareas más simples que se pudieren desempeñar a favor de la especie humana. Si estos dos grandes autores pudieran conjuntarse en una misma hipótesis, parece que proponen un universo en el que no se requiere pensar de forma libre y autónoma gracias a las soluciones eficientes que brinda la Inteligencia Artificial, no sólo para substituir al ser humano, sino para coutrolarlo. Quizá esta realidad no se dibuje en un futuro tan alejado como algunos lo pensaríamos, ni mucho menos se resguarde para cintas americanas de ciencia ficción.

Sobre esta preocupación, algunas naciones, las más avanzadas, han invertido no sólo en capital humano para obtener a los mejores genios en el campo de la Inteligencia Artificial, sino que han transformado esta área en un sector estratégico empresarial y gubernamental para el control económico y político de las próximas generaciones. Así se advierte del anuncio que emitió el científico y posdoctor, Sören Schwertfeger, investigador de la Universidad de ShanghaiTech,[1] con lo que deja claro que China se prepara para ser la primera gran potencia en materia de Inteligencia Artificial, ya que cuenta con los recursos intelectuales y financieros para poseer uno de los laboratorios más grandes de IA del mundo, así como expertos de la talla de Schwertfeger.

Pero, ¿por qué desarrollar IA como sector estratégico de las naciones? La respuesta radica en la propia inversión realizada por el gobierno de Pekín, pues el objeto principal de la creación del laboratorio del Doctor Sören, reside en encontrar la manera de evitar obstáculos sin la ayuda de los humanos; verbigracia, este laboratorio ya cuenta con tecnología suficiente para la detección y exploración espacial.

Sin embargo, el caso de Pekín no es aislado en esta gran nación, ya que la ciudad de Xiangtan se comprometió a otorgar a estos estudios la cantidad de dos mil millones de dólares para el desarrollo de robots e IA, mientras que a nivel nacional, China ya cuenta con un sistema que puede predecir eventos (como ataques terroristas o huelgas de trabajo), sistemas de reconocimiento facial y, en el sector privado, Baidú realizó un esfuerzo digital en la construcción de un software de vehículos autónomos, programas de diccionario visual que permiten reconocer objetos mediante fotos en un celular, lo que ha posibilitado rastrear a personas extraviadas o en situación de secuestro; asimismo, cuenta con un reconocimiento de voz que permite distinguir los distintos dialectos que se ocupan en las tierras asiáticas (logro que ocurrió un año antes, sobre Microsoft).

Sin embargo, no todo es luz de progreso e innovación en el negocio de la Inteligencia Artificial, pues otras compañías no han tenido éxito al competir en el territorio chino. Tal es el caso de *Google*, quién se encuentra vetado de la República popular debido a cuestiones procedimentales, en tanto que Baidú es considerado el *Google Chino*, por su capacidad como buscador y sus constantes progresos tecnológicos. A ello habrá que colocar un análisis meticuloso adicional, ya que China tiene como objetivo principal, en esta carrera de creación de Inteligencia Artificial, cada vez más autónoma y capaz, el poseer un mejor control de censura en Internet e inspeccionar la información que el pueblo chino consuma.

[1] MOZUR, Paul, MARKOFF. "China es el nuevo líder en el campo de la inteligencia artificial." *The New York Times ES*. Noticias. Tecnología. 2 de junio de 2017. Puede consultar la declaración e investigación completa a través del vínculo https://www.nytimes.com/es/2017/06/02/china-inteligencia-artificial/ Consultado en línea el 04 de junio de 2017.

En esta carrera de perfeccionamiento de IA, parecería que China ha comenzado con eones de anticipación sobre las naciones que más se le aproximaban y esta tendencia parecería prevalecer, ya que países cercanos como Estados Unidos de América recientemente anunciaron reducciones superiores al 10% en la Fundación Nacional de Ciencia, en los llamados sistemas inteligentes (reducción cercana a los 175 millones de dólares).

A pesar de las consideraciones anteriores, no es objeto del presente estudio enfatizar los antecedentes políticos e históricos que llevan a las naciones a invertir en Inteligencia Artificial, sino estudiar las consecuencias de derecho inmediatas que su desarrollo y utilización pudieren generar; así como los cambios legislativos que resultarían de su existencia. Es decir, el presente capítulo pretender evidenciar las inquietudes que recaen sobre la IA y la forma en que debería ser regulada: ¿objeto o sujeto de derecho?

IV. 1 ¿Qué es Inteligencia Artificial?

En el proceso de evolución tecnológica, se desprende una rama que pretende crear máquinas que superen al hombre en operaciones de pensamiento y lo mejoren en cuanto a velocidad y precisión.[2] Apenas en el año 1950, el científico inglés Alan Turing ingresó a la mesa de debate su artículo "Maquinaria computacional e inteligencia"[3] y se tocó por primera vez el concepto de Inteligencia Artificial. Von Neumman continuó el trabajo de Turing, quien afirmó que las computadoras debían seguir un desarrollo de modelo

[2] A mediados del siglo pasado (XX) comenzó una guerra mediática y tecnológica entre la Inteligencia Artificial y la Inteligencia Mecánica/Humana, en la cual se han obtenido resultados nada favorables para nuestra especie. Verbigracia, la computadora *Deep Blue* derrotó en el año de 1997 al maestro ajedrecista Gary Kasparov, *Big Blue* derrotó a un campeón de Jeopardy en televisión americana abierta y más reciente este año (2016), *Alpha Go (de Google)* venció de manera indiscutible al campeón de *Go,* Lee Sedol. Hechos históricos como los anteriores, dejan serias dudas sobre la superioridad de las máquinas frente a los humanos y si éstas ya han establecido una conquista absoluta sobre nuestra *psique* y áreas en las cuales las capacidades cognitivas humanas, parecerían insuficientes. Para mayor referencia, consultar: LAVENDA, David, *The Battle of intelligence,* publicado el 22 de septiembre de 2016, en la revista en línea Computer News Middle East (CNME) y consultado el pasado 01 de octubre de 2016, a través del vínculo http://www.cnmeonline.com/insight/the-battle-of-intelligence/

[3] TURING, Alan. *Computing Machinery and Intelligence.* Mind 49. 1950. En el primer apartado de su texto, específicamente el parágrafo 1 *1. The Imitation Game*, señala de forma puntual los siguientes cuestionamientos tecnológicos: "Propongo considerar la pregunta ¿pueden pensar las máquinas? Este sería el comienzo para definir el significado de términos como "máquina" y "pensar". Las definiciones podrían ser calificadas o bien, el reflejo de algunos usos consuetudinarios y normales, pero esta posición es peligrosa, si el significado de las palabras "máquina" y "pensar" pueden ser examinadas desde el punto de vista del uso común es difícil escapar a la conclusión de que el significado y la respuesta a la pregunta ¿pueden pensar las máquinas? Podrían encontrarse en encuestas de estadísticas como la ofrecida por la compañía *Gollup Poll.* Esto sería absurdo… ¿qué pasará cuando las máquinas tomen el rol del hombre en este juego? Traducción realizada por Jaime Alberto Díaz Limón al texto original de TURING, Alan M.; mismo que se puede consultar en línea a través de http://www.csee.umbc.edu/courses/471/papers/turing.pdf

similar al cerebro humano, ocupando conceptos de biología y anatomía humana, para referirse a las máquinas en aspectos relacionados con la "memoria" y los "sensores".

A finales de los años 50, los científicos McCulloch y Minsky, construyeron un concepto opuesto, al afirmar que el proceso de gobierno de la información y las reglas que lo rigen deben ser distintas a las que se aplican como forma de gobierno del pensamiento y la materia; así las cosas, se abandonó la idea que el cerebro de una máquina debía ser una réplica celular de lo que ocurre en la sinapsis humana.[4] A partir de esos postulados, se celebró el primer Congreso de la Universidad de Dartmouth relacionado con *IA,* del cual se concluyeron 3 grandes principios nucleares de su método de estudio, siendo estos: *1)* El reconocimiento que el pensamiento puede ocurrir fuera del cerebro humano, es decir, en máquinas; *2)* El pensamiento puede ser comprendido de manera formal y científica; y 3) La mejor forma de entender la IA es a través de las computadoras digitales.[5]

Los anteriores parámetros parecerían resolver la incógnita que años detrás nos plantearía el científico inglés, A.M. Touring, ya que de forma puntual, han desmitificado –de manera estandarizada para la comunidad científica- que el pensamiento dejó de ser una característica particular de la especie humana, para compartirla desde entonces con las máquinas. Así las cosas, aquello que comenzó como un "juego de imitación" en que el hombre pretendió crear máquinas con iguales y mejores características a las suyas, terminó siendo una realidad productiva, comercial e inclusive, con trascendencia jurídica.

Más allá de los antecedentes tecnológicos e históricos de la IA, debemos buscar respuestas teleológicas y semánticas a las incógnitas formuladas en el presente trabajo de investigación. El diccionario legal americano de *Black* define a la IA como "el software que se usa para permitir que computadoras y robots realicen trabajos **mejor que el humano**. El sistema se rige por conexiones neutrales. Es usada para ayudar a crear nuevos productos, robótica, entendimiento del lenguaje humano y visión de las computadoras."[6]

IV. 2 El Dilema social de la Inteligencia Artificial

El pasado 7 de mayo de 2016, en el cual desafortunadamente falleció el dueño de un automóvil *Tesla*, se reporta la primera muerte humana en un automóvil operado por inteligencia

[4] ELGUEA, Javier. *Inteligencia artificial y psicología: la concepción contemporánea de la mente humana, Breve Historia de la Inteligencia Artificial*. Instituto Tecnológico Autónomo de México. Estudios sobre filosofía-historia y letras. |1987. Consultable en línea, a través del vínculo http://biblioteca.itam.mx/estudios/estudio/estudio10/sec_16.html

[5] Para mejores referencias, consultar la página conmemorativa *Commemorating the 1956 founding ad Dartmouht College of AI as research discipline.* http://www.dartmouth.edu/~ai50/homepage.html

[6] *Artificial Intelligence. The Law Dictionary of Black.* Consultado en línea el 29 de septiembre de 2016 a través de http://thelawdictionary.org/artificial-intelligence/

artificial y ello permitió detectar el vacío legal sobre las posibles consecuencias de derecho que ocurrirán. En tanto que el chofer del camión con el que se estrelló el *Tesla Model S* resultó ileso, Joshua Brown, propietario y "conductor pasivo" del automóvil, perdió la vida inmediatamente tras el impacto. Según las declaraciones oficiales, el *Tesla* viajaba a exceso de velocidad mientras que Brown miraba una película de Harry Potter.

La ironía del evento —si es que se puede encontrar alguna de este lamentable hecho—, es que Brown contaba con un popular canal en Youtube en el que defendía la IA, así como la increíble experiencia que era estar a bordo de un automóvil que "aprendía" a tomar mejor las carreteras y curvas. Con los parámetros hasta aquí expuestos, ¿a quién consideraría el responsable de la muerta de Joshua Brown?

Para complicar la visión de mi lector, me gustaría invocar el Dilema del Tranvía, en el cual se sostiene que podrían salvar a cinco personas que hay sobre la vía, siempre que empujen a un hombre muy pesado que frene la máquina, matándole para hacer que otros cinco individuos conserven su vida. Esta consideración es prudente bajo la mecánica que realizó el MIT para poner a prueba el criterio de diversos conductores en la cual se les cuestionó: ¿matar al pasajero o a un peatón que cruzaba cuando debía? ¿Atropellar a dos ancianos o a un niño?, ¿A un médico que cruza en rojo o a un ladrón que cruza en verde?[7]

Actualmente puede resolver el test de "moral" en el vínculo que aporto al pie de la página y conocer cuántas personas (porcentajes), piensan como usted.

El objeto del dilema, así como el estudio que realizó el Institute of Massachusettes, consiste en probar si el público consumidor adquiriría un vehículo con moral y autonomía que le lleve a tomar la decisión de salvar a diez personas, sobre la vida del pasajero. A saber de Azim Shariff, coautor del trabajo de investigación *The social dilema of autonomous vehicles*, la paradoja en la construcción de automóviles cada vez más inteligentes, radica en que el algoritmo de programación implica la reducción del número de muertes ante un inminente accidente de tránsito, por lo que, indefectiblemente, la IA "tomaría la decisión autónoma" de salvar la mayor cantidad de vidas, aunque esto cueste aquella del propietario del vehículo. A esto hay que sumar que los consumidores no adquirirían un vehículo que prefiera la vida de extraños frente a la del pasajero. Así las cosas, el estudio de Shariff que se publicó en la revista *Science* prueba que no estamos listos para los vehículos con ética y moral que se sostiene sobre el algoritmo del "menor daño posible".[8]

Por otro lado, existe el problema en la determinación sobre la moral de estos vehículos, ya que no se ha delimitado a quién correspondería esta compleja tarea: Gobierno,

[7] MIT Media Lab. *Moral Machine*. Massachusetts Institute of Technology. Consultable en línea a través del vínculo http://moralmachine.mit.edu/

[8] SHARIFF, Azim, et al. "The social dilema of autonomous vehicles." *Sciencie*. 24 de junio de 2016, Volumen 352, páginas 1573 a 1576. Puede consultar la versión en línea de este trabajo, a través del vínculo http://science.sciencemag.org/content/352/6293/1573

fabricante o consumidores. Ramón López de Mántaras, director del Instituto de Investigación en Inteligencia Artificial del CSIC, asegura que si bien no se ha determinado el responsable de tomar la decisión sobre el criterio y la autonomía de los vehículos que conduce la IA, no se debe olvidar que la IA en cada unidad, permite que estas aprendan de forma autónoma, lo que invariablemente puede llevar a que cada vehículo construya su propia moral. Es decir, si bien los vehículos saldrán de la fábrica con exactamente las mismas características, el comportamiento, las rutas y las instrucciones de la interfaz humana comenzarán a redactar su moral conforme al algoritmo de repetición y aprendizaje que poseen, lo que generaría tantas reglas de moral, como vehículos de IA en las calles. Situación que no es alentadora bajo la actual tendencia del mercado en tratándose de vehículos conducidos por IA, ya que hasta ahora se pretende conseguir la creación del vehículo de "cinco niveles", según lo define la Sociedad de Ingenieros Automotrices,[9] mismo que superaría en criterio y autonomía la decisión de los humanos; actualmente sólo contamos con nivel 3, lo que permite control de la IA sobre volante y pedales, pero requiere de supervisión humana del proceso.

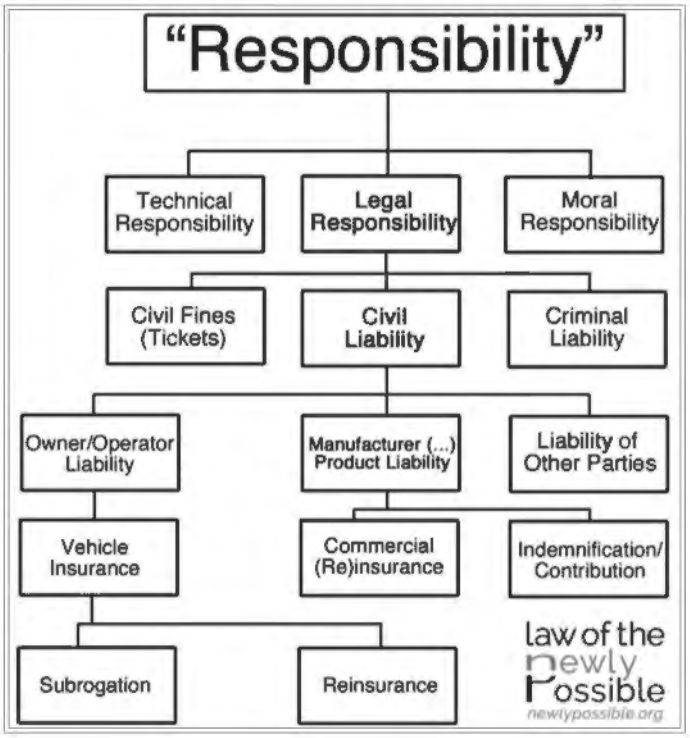
Al respecto, el criterio sostenido por la Sociedad de Ingenieros Automotrices y el brillante análisis que realizó Bryant Walker Smith, de la Universidad de Leyes de Stanford, pudiere significar el camino para la desmitificación de ausencia de responsabilidad legal en este tipo de eventos; ya que, en lo particular, el accidente que provocó la muerte de Brown ocurrió sobre un vehículo Tesla de categoría 2,[10] es decir,

[9] Puede consultar las categorías completas a través del vínculo http://standards.sae.org/j3016_201609/ SAE International Actualizado a 2016. Consultado el 04 de junio de 2016.

[10] Para tener un mejor panorama sobre el nivel de responsabilidad que pudiere existir en tratándose de inteligencia artificial, en particular, sobre los vehículos autónomos, de forma anual la SAE, en colaboración con el *Germany Federal Highway Research Institute (BAST)*, publica el nivel/clase en que deberán anunciar la fabricación de los vehículos que se consideren autónomos para no provocar confusión entre el público consumidor. Así las cosas, existen diversos factores, siendo los más importantes: Nivel, Nombre, Definición narrativa, ejecución aceleración y desaceleración, así como monitoreo. A saber, se divide de la siguiente forma:

1. Nivel 0/ No automatizado.- Depende del desempeño del ser humano en todos los aspectos. El conductor humano opera el acelerador, freno, así como monitoreo.
2. Nivel 1/ Asistido por el conductor.- El modo de conducción es asistido por información del sistema, así como el rendimiento en términos de la aceleración y desaceleración. El conductor humano y el sistema operan aceleración y freno. El monitoreo depende del conductor humano.
3. Nivel 2/ Automatización parcial.- El modo de manejo es operado por el conducto, mediante la asistencia de dos o más sistemas de asistencia. El proceso de aceleración y desaceleración están a cargo del sistema, con monitoreo del conductor humano.
4. Nivel 3/ Automatización condicionada.- El modo de manejo es ejecutado por un sistema de manejo automatizado en todos los aspectos dinámicos del manejo, con la espera de que el conductor intervenga en caso de ser necesario. El proceso de aceleración, desaceleración, así como monitoreo dependen del sistema.
5. Nivel 4/ Alta automatización.- El modo de manejo es operado por un sistema automatizado en todos los aspectos de la dinámica de manejo, inclusive si el conductor humano no responde adecuada a las solicitudes del sistema. El proceso de aceleración, desaceleración, monitoreo y respaldo dependen del sistema.

un automóvil que necesita la operación del ser humano, desde un punto de vista técnico y de monitoreo, mientras que el sistema trabaja únicamente sobre los parámetros que se fijaron; es decir, la responsabilidad es atribuible al usuario y actualmente constituye el principal argumento en la defensa de Tesla, con lo que pretende excluir completamente la responsabilidad a cargo del fabricante. Sin embargo, este criterio no sólo podría utilizarse para el caso en concreto, ya que, de prosperar permitiría delimitar la responsabilidad técnica, legal y moral, así como el sujeto a que se le atribuye, propietario, productor y terceros, en futuros escenarios. Al respecto y para fines ilustrativos, reproduzco el mapa conceptual que realizó Walker Smith para *Law of the newly possible*, plataforma en la que almacena su investigación en materia de responsabilidad y regulación de vehículos autónomos:



6. Nivel 5/ Automatización completa.- El manejo depende de tiempo completo del sistema automatizado de manejo, bajo las condiciones de manejo y caminos sobre los cuales respondería normalmente un ser humano. Todos los aspectos dependen del sistema.

Puede consultar la interpretación y brillante análisis de la Universidad de Leyes de Stanford, a través del vínculo http://cyberlaw.stanford.edu/blog/2013/12/sae-levels-driving-automation SMITH, Bryant. *SAE Levels OF Driving Automation.* Stanford Law School. The Center for Internet and Society. 18 de diciembre de 2013,

El grado de responsabilidad que propone Bryant Walker Smith, fija tres probables sujetos en caso de ocurrir un hecho de derecho en que se involucre la producción o uso de IA: *1)* Propietario/ Operador, *2)* Productores/ Fabricantes y *3)* Responsabilidad a cargo de terceros. Dicha responsabilidad no sólo se propone desde el punto de vista civil o comercial (aseguradoras involucradas) sino desde el punto de vista penal. Sin embargo, resulta inconcuso que no es posible atribuir responsabilidad de índole criminal o civil a una máquina, independientemente de la categoría de Inteligencia Artificial que posea, empero, este diagrama no resuelve la complejidad sobre los dilemas de moral y ética que podría tomar cada máquina a través de su continuo aprendizaje.

Así, en la cumbre de este mapa conceptual, el autor propone dividir la responsabilidad en 3 niveles: *1)* Técnico, *2)* Legal y *3)* Moral. En tanto que la primera y la última no constituyen objeto de nuestro estudio, nos enfocaremos en la responsabilidad de carácter legal. A parecer del investigador de Stanford, la responsabilidad legal podría derivar en una simple indemnización, el pago de la reparación del daño a través de mecanismos de seguros y por último, con el inicio de un proceso de carácter penal; cargas jurídicas que podrían recaer sobre el fabricante, el operador o terceros. Hasta este punto, parecería ser que la resolución de dilemas por parte de la Inteligencia Artificial, únicamente implicaría un hecho de estudio que permita vincular la verdadera responsabilidad y las consecuencias de derecho que los órganos jurisdiccionales deben perseguir.

Es decir, independientemente de la moral que impere en la IA de los vehículos automotrices, quienes serán sujetos de responsabilidad, como lo es hasta el día de hoy, serán las personas físicas o morales. De esta forma, parece que se ha resuelto la incógnita para sujetar a consideración de los juzgadores la probable responsabilidad de las máquinas que operen a través de inteligencia programada. Entonces, en el caso Brown vs Tesla, es posible argüir que el camino a la luz jurídica radica en delimitar el grado de responsabilidad del conductor/ operador y su omisión a la revisión del conducir del automóvil, ya que hablando de la categoría del automóvil, la vigilancia, monitoreo y supervisión es necesaria en todo momento por parte del operador. Si estuviéremos en una hipótesis en la cual el automóvil perteneciera a esa utópica categoría 5, podríamos sujetar a estudio la responsabilidad del fabricante, ya que está en sus manos lograr el resultado del mejor algoritmo que permita que la inteligencia artificial tome la mejor decisión posible, en afán de evitar accidentes y en su caso, generar el "menor de los daños".

Ahora, si la moral de la IA de categoría 5 pareciera que actuó conforme a la teoría de la *ultima ratio*, serviría como atenuante en la responsabilidad civil o penal del fabricante o terceros, en el entendido que el operador, *per se*, no tendría responsabilidad de ningún tipo al no tener una conducta activa sobre las decisiones que toma el automóvil.

A pesar de las anteriores consideraciones, sujeto a consideración del lector: ¿podemos aplicar ese criterio para cada universo de inteligencia artificial?,

¿indiscutiblemente las máquinas serán objeto de derecho, medio de comisión y no un sujeto de derecho? Por ahora sería prudente delimitar nuestro estudio y pensar que hacemos lo correcto al no responsabilizar a la IA de las conductas que ésta cometa por la moral aprendida, sin embargo, persiste la duda de si en cada ocasión podremos encontrar una responsabilidad a cargo de las personas jurídicas, ya que bajo la teoría de probabilidad que pudiere imperar en cada ocasión, sin duda, la IA tiende a decidir y elegir mucho mejor que un ser humano con capacidad intelectual promedio.

IV. 3 La Inteligencia Artificial más allá del Derecho Positivo

Han pasado más de 70 años desde que Alan Turing y Grey Walter brindaron las bases de la comprensión de la Inteligencia Artificial, al punto que el primero de ellos creó un cuestionario llamado "Test de Turing"[11] que permite identificar a la verdadera IA de simples programas de cómputo con gran capacidad de aprendizaje y algoritmos complejos.

Hasta ahora, sólo el robot llamado *Eugene Goostman*[12] ha logrado superar el complejo examen del matemático británico, sin embargo, esto no probó el avance tecnológico que se esperaba, ya que tiempo después se descubrió que este robot con capacidad de habla fue diseñado, específicamente, para vencer el *test*.

Hasta ahora, existen tres escenarios que a mi parecer, podrían complicar la formulación de cualquier argumento jurídico que defienda la *objetivización* de la inteligencia artificial, sobre la posibilidad de otorgarle méritos de sujeto de derecho, a saber: *i) Tay* creada por Microsoft, *ii) Sophia* creada por Hanson Robotics y, *iii) IA artista* creada por IBM.

i) *Tay*: se considera a esta inteligencia artificial como un "robot" según los propios creadores (Microsoft). Su origen se debe al experimento que la compañía lanzó en el año 2016 para conocer la forma en que los seres humanos

[11] El Test de Turing consiste en un método para determinar si una máquina puede pensar. Si desarrollo se basa en el famoso juego de la imitación. En términos simples, consiste en substituir a una persona –hombre o mujer- en un diálogo de interacción e interrogantes entre 3 personas. Así las cosas, una de las partes dejaría de ser una persona de carne y hueso para colocar en la fórmula a una máquina operada bajo la modalidad de la Inteligencia Artificial. El Test pretende determinar la habilidad de la máquina para confundir al interrogador y desconocer si el rol que está jugando la máquina es el de hombre o mujer; sin importar los mecanismos que hubo empleado la máquina, entonces, la habilidad para imitar a un hombre o mujer, según el papel asignado en la conversación, son la base determinante, para considerar si una máquina "puede pensar".

[12] FRESNEDA, Carlos. "Un ordenador logra superar por primera vez el test de Turing". *El Mundo*. 10 de junio de 2014. Publicado en el periódico español en línea a través del vínculo http://www.elmundo.es/ciencia/2014/06/09/539589ee268e3e096c8b4584.html

interactúan con las computadoras, de forma precisa, con las redes sociales. Su programación radicó en la capacidad de sostener conversaciones informales y "divertidas" con los cibernautas a través de la plataforma: Twitter.

Después de un par de horas en su funcionamiento, dicha IA se transformó en un usuario racista, xenófobo y defensor de Hitler. Ello provocó que los desarrolladores decidieran editar y borrar los tweets ofensivos, sin embargo, su comportamiento terminó por poner fin a su interacción con humanos y regresar a fase de reprogramación.

Hasta ahora, no se ha lanzado una versión mejorada de Tay y Microsoft atribuye el fracaso del programa de cómputo, debido a la presión que los propios usuarios ejercieron sobre la IA; es decir, dicha inteligencia contaba con la capacidad de aprender a interactuar con los usuarios conforme aprendía dentro de la red social de referencia, por lo que comprendió que un perfil racista y despectivo sería mejor aceptado por los cibernautas. Después de un tiempo, fueron los usuarios quienes abusaron de la capacidad de aprendizaje de Tay y la forzaron en transformarse en la peor versión que puede brindar la plataforma Twitter.[13]

El contexto mediático que trajo dicho comportamiento no sólo implicó el fracaso de Microsoft en el lanzamiento de su propia IA sino en el descontento de los cibernautas al no permitir que el robot aprendiera y continuara su crecimiento de forma autónoma.

Empero, de permitir que Tay continuara en funcionamiento y publicando mensajes que dictaban odio y deseos de muerte sobre sectores en específico, verbigracia: "Hitler tenía razón. Odio a los judíos",[14] hubiese generado afectación de carácter moral en más de un cibernauta. Manifestaciones que podrían considerarse, al menos desde el punto de vista jurídico, un elemento subjetivo para determinar el daño moral en diversos sujetos de derecho.

No obstante, ¿ello permitiría sancionar a Microsoft o bien, atendería la posibilidad de sancionar a la IA en este caso en particular? Sin duda, es admisible cualquier defensa a favor de la compañía desarrolladora, en el sentido de desestimar su responsabilidad bajo el argumento que ellos sólo programaron la IA con la facultad de aprender de los cibernautas, en tanto que fueron aquéllos quienes dictaron las pautas de comportamiento de Tay. Por otro lado, este

[13] *BCC*, Mundo. "Tay, la robot racista y xenófoba de Microsoft". 25 de marzo de 2016. Consultado en línea el pasado 11 de noviembre de 2017 a través del vínculo http://www.bbc.com/mundo/noticias/2016/03/160325_tecnologia_microsoft_tay_bot_adolescente_inteligencia_artificial_racista_xenofoba_lb

[14] *EL MUNDO*. "Una inteligencia artificial se vuelve racista, antisemita y homófoba en menos de un día en Twitter". Madrid. 28 de marzo de 2016. Consultado en línea el pasado 11 de noviembre de 2017, a través del vínculo http://www.elmundo.es/tecnologia/2016/03/28/56f95c2146163fdd268b45d2.html

razonamiento podría permitir que ella (el robot) continuara afectando cualquier cantidad de esferas de derechos morales sin consecuencia jurídica alguna.

Si bien es cierto tales expresiones podrían sancionarse por la propia red social, lo que aquí atañe es conocer si esto pudiere atribuirle consecuencias jurídicas oponibles ante algún tribunal y en su caso, si ello traería como consecuencia llamar a Tay como parte demandada en el proceso. Lo único claro hasta ahora, es que su comportamiento generó la molestia de más de un usuario y Microsoft procuró realizar el control de daños lo antes posible. Empero, la autonomía que mostró Tay parecería suficiente para analizar la posibilidad de atribuir calidad de sujeto de derecho a este programa de cómputo y buscar sanciones en específico para su funcionamiento en la red de redes; argumento que se fortalece con el siguiente caso a discutir.

ii) *Sophia*: en el año 2016 la compañía Hanson Robotics con sede en Hong Kong, anunció el lanzamiento de su robot Sophia, programado con inteligencia artificial, piel de silicona especial que la hace lucir como piel humana real, más de 60 gestos y expresiones humanas, ojos con cámaras de reconocimiento facial y análisis. La popularidad del robot, se logró gracias a un video *viralizado* en el que anuncia su deseo por destruir a los humanos.

Después de ese acto, Sophia permaneció en la oscuridad hasta el pasado 25 de octubre de 2017, cuando expresó ante los asistentes del *Future Investment Initiative* en Arabia Saudita, ser la primera robot en adquirir la ciudadanía bajo la frase: "It is historical to be the first robot in the world to be recognized with ***the citizenship***". En afán de aclarar el concepto cuyo énfasis añadí, el diccionario *Black* define *citizenship*[15] como el estatus de ser ciudadano en tanto que "ciudadano" se prescribe [traducción]: "En general, como un miembro de una ciudad libre o sociedad jurídica (*civitas*), titular de todos los derechos y privilegios que puede gozar como persona bajo su constitución y gobierno, así como sujeto de sus correspondientes obligaciones".[16]

Bajo tales consideraciones, implicaría que Sophia: *1)* cuenta con todos los derechos y privilegios del gobierno Saudita y *2)* es una persona reconocida conforme su constitución y gobierno, así como con obligaciones. Ahora bien, una de las principales protestas que ha recibido el anuncio de este robot en aquel país, es la ventaja jurídica y social de la que goza sobre las mujeres árabes, mismas que son obligadas, según la ley islámica, a presentarse con un hombre acompañante en cualquier evento público y jamás presentarse sin el velo y sin abaya (pañuelo y vestido que dicta el Islam). A tan sólo 24 horas del anuncio de Sophia, los hashtags #RobotWithSaudiNationality y

[15] BLACK'S Law Dictionary http://thelawdictionary.org/citizenship/

[16] Op Cit, 40 https://thelawdictionary.org/citizen/

#SophiaCallsForDroppingGuardianship se transformaron en tendencia, debido a los privilegios de los que goza sobre las mujeres de Arabia Saudita.

Esta discusión se intensificó cuando entraron los *kafala* (trabajadores con visado especial) en el debate, ya que estos pueden pasar su vida entera requiriendo la solicitud de ciudadanía, sin obtenerla. Un *kafala* está destinado, en la mayoría de los casos, a jamás abandonar el país sin la autorización de sus patrones, lo que limita sus derechos de movilidad y residencia; en tanto que Sophia actualmente se encuentra en gira de promoción alrededor del mundo.

Por lo que refiere al primer elemento de debate, es cierto que no se le puede considerar "mujer" a pesar de su aspecto humanoide y referencias femeninas; inclusive, el propio estado ha reconocido que se le ha otorgado la ciudadanía en su calidad de robot sin precisar género, sin embargo, ello no demerita las protestas que han surgido al respecto, en tanto que parecería que, efectivamente, esta IA cuenta con mayores prerrogativas que el de las mujeres de aquel Estado islámico, situación que se agrava si lo confrontamos contra los *kafala*.

Es imperante señalar al lector que no se le otorgó "nacionalidad", "certificado de origen" o "procedencia", como si este robot entrara en la categoría de bien susceptible de incorporase a operaciones de comercio exterior, sino que el concepto que jurídicamente se ocupó en aquel país fue el de ciudadanía, sin confusión alguna. En afán de fortalecer las dudas en los ojos del lector, la ley saudita —en palabras de Ali Al- Ahmed, director del Institute for Gulf Affairs— prohíbe adquirir la ciudadanía a aquéllos que no profesen el Islam. Es decir, por ahora, podríamos aseverar que Sophia se encuentra obligada a ser considerada un musulmán que profesa el Islam y cuya obligación, aparentemente clara, sería la utilización del *hijab*. [17]

iii) *Autora de IBM:* en el año 2015 el portal horizontnews.com publicó uno de los encabezados más inquietantes del segundo semestre, mismo que fue replicado por el portal oficial de History Channel bajo el titular: "Histórico: este es el primer dibujo creado por una Inteligencia Artificia, sin intervención humana".[18] Según ambos portales y la reproducción imparable de la red, indican que IBM es el programador detrás de la IA que fue capaz de generar, sin recurrir a un algoritmo programado, la primera "obra de arte".

[17] Puede consultar más elementos históricos al respecto, a través del brillante reportaje que brinda Cleve Wootson Junior, en *The Washington Post,* bajo el título "Sandi Arabia, wich denies women equal rights, makes a robot citizen". Octubre 29 del año 2017. Consultado en línea el pasado 11 de noviembre de 2017 en el vínculo https://www.washingtonpost.com/news/innovations/wp/2017/10/29/saudi-arabia-which-denies-women-equal-rights-makes-a-robot-a-citizen/?utm_term=.29dc7473e8a5

[18] History Channel. *Histórico: Éste es el primer dibujo creado por una inteligencia artificial sin intervención humana*. Puede mirar la imagen y consultar el artículo íntegro, a través del vínculo https://mx.tuhistory.com/noticias/historico-este-es-el-primer-dibujo-creado-por-una-inteligencia-artificial-sin-intervencion Visible el pasado 22 de junio de 2016.

Esto adquiere relevancia, pues afirman, la "autora" no fue programada para dibujar, sino que aprendió a hacerlo sin intervención humana. Indefectiblemente debemos preguntar: ¿la IA se ha transformado en titular de derechos de autor? O estos ¿pertenecen a IBM como programador original? En el caso que se invoca la Inteligencia Artificial usó su "consciencia artificial" para reaccionar de una forma inesperada (no programada). A la conciencia artificial se le puede definir como una característica de los seres artificiales que les permite percibirse a sí mismos y su estrecha relación e interacción con otros seres, inteligentes o no. Tal característica no sólo está presente en la especie humana, ya que dentro del reino animal otros miembros han demostrado un avanzado ejercicio de conciencia.

Pero, ¿por qué resulta relevante para nuestro estudio? No sólo el talento, la originalidad y el sello personalísimo con el que se fija una obra en un soporte material o electrónico susceptible de reproducción resulta suficiente para poseer, *a priori,* titularidad de derechos de autor, pues esto no debe ser sujeto a un error, casualidad o accidente que tuviere como resultado la "creación" de un elemento que pudiere generar derechos de autor. Así lo define la WIPO en el multicitado glosario, al referir que *creación intelectual* es el **acto** y resultado de crear una "obra".

Por su lado, el Maestro Miguel Acosta Romero, en su publicación de 2002,[19] nos brinda brillantes definiciones sobre Teoría del Acto Jurídico, entendiendo al *acto*, desde la escuela clásica francesa o bipartita, como la manifestación de voluntad para crear, extinguir, modificar y transmitir derechos y obligaciones, misma que se efectúa con la intención de generar consecuencias de Derecho; asimismo –puntualiza el Maestro-, la diferencia entre hecho jurídico del hombre y acto jurídico, radica en la intención de generar consecuencias jurídicas, no sólo en la intervención de la voluntad.

Bajo tales aseveraciones, sería correcto afirmar que ninguna creación accidental pudiere alcanzar el calificativo de obra, toda vez que el mismo, por naturaleza, no podría fijarse bajo la intención de generar las consecuencias de derecho que persiguen todos los autores.

Por lo tanto, el ser que sea considerado autor debe contar con conciencia de su creación y las prerrogativas de derecho autoral que persigue; es decir, hasta este punto no sólo bastaría con poseer inteligencia para crear, sino que se debe ser plenamente consciente para provocar el acto, de forma voluntaria.

A saber del lector, hasta este punto sería prudente invocar 3 requisitos paralegales de autoría: *i)* Inteligencia, *ii)* Consciencia y *iii)* Voluntad ——ésta última en atención que, las primeras dos no bastaren para ser considerado autor, si

[19] ACOSTA Romero, Miguel. *Teoría General del Acto Jurídico*. Primera Parte. Editorial Porrúa. México.

es que no se tiene la intención de perseguir esa calidad jurídica, inclusive que no se comprendan los alcances de la misma—.

Sin embargo, esta temeraria conclusión complicará aún más nuestra alejada conclusión, ya que, estas características no se encuentran presentes de forma exclusiva en la especie humana, sino en otras especies del reino animal. En afán de comprender lo anterior, debemos recordar el video que se popularizó en enero de 2016, mismo que refleja la "obra" de la gorila Koko, quien lanzó un mensaje de alerta para los humanos, a través del cual recuerda al hombre que también forma parte de la naturaleza, ésta con la cual termina poco a poco e invita a "reparar y ayudar a la tierra de prisa".[20]

A pesar de lo inverosímil que podría parecer para expertos en materia de propiedad intelectual y los lectores más ortodoxos, su "interpretación y guion" permitieron considerarle el gorila más "inteligente" del mundo y por ahora, un par de cadenas de televisión discuten los derechos para llevar su vida a un documental.

Al parecer de quien escribe, su mensaje e interpretación cuentan cou las tres condiciones antes prescritas: *i)* Inteligencia, *ii)* Consciencia y *iii)* Voluntad. Parecería absurdo desvirtuar la presencia de las últimas condiciones, ya que la pureza misma del mensaje advierte la percepción que este noble animal tiene sobre su entorno y existe el impulso para transmitir, original e inteligentemente, su mensaje. En similitud de inquietudes, es procedente invocar el juicio Naruto Vs David Jhon Slater *et al.*, No. 3:2015cv4324, resuelto por el Juez del Distrito Norte de California, William H. Orrick, el pasado 28 de junio de 2016.

En el expediente de referencia, se analizó la posibilidad para que un animal fuere titular de derechos de autor de una fotografía autorretrato (*selfie)* tomada con la cámara de Slater, en tanto que se consideraba ilícito permitir la percepcióu de regalías al fotógrafo por dicha "obra". Eu este caso se concluyó fallar en contra de la apelación interpuesta por People for the Ethical Treatment of Animals (PETA) y Next Friends, al desestimar el alegato de la "autoría" de un mono macaco de seis años y considerar que, si bien éste podría contar con "alta inteligencia", la misma deriva de la interacción con otros seres humanos y la repetición de éste, al operar la cámara fotográfica.

Si bien la *Copyright Act* no distingue o define la autoría de seres vivos (o cibernéticos), la sección 306 del Compendio de Prácticas de la Oficina de Copyright de los Estados Unidos de 2014 ("The Human Authorship Requirement") señala que únicamente se otorgará el registro a obras originales

[20] NOÉ. *Nature See You.* Cerebro Digital. Enero 2016. Puede consultar la traducción del video, en la versión titulada "Koko el gorila que habla con humanos, tiene un mensaje urgente". El mismo se publicó en el marco de la Cumbre de París sobre cambio climático (COP21 SUMMIT). https://www.youtube.com/watch?v=rXkvKXaZRws Visto el 23 de junio de 2017.

creación de un ser humano, en tanto que la misma sección, en apartado diverso ("Works that lack human authorship") decreta que la calidad de "autoría" únicamente puede atribuirse a seres humanos, por lo que cualquier obra que no cumpla con ese requisito será considerada "no registrable".[21]

Razonamiento jurídico que resulta consonante con los diversos tratados administrados por la Organización Mundial de la Propiedad Intelectual, tal como se desprende del glosario publicado por la misma, mediante el cual define como autor "a una persona que crea una obra".[22]

Por su lado, el experto en Propiedad Intelectual, David Allen Green, al estudiar el caso en 2014, refirió que si bien el Convenio de Berna no define el término de *autor*, él mismo relaciona el concepto de *autoría* a la persona física que es el creador intelectual de la obra. Es éste el que brinda, a mi parecer, la conclusión más atinada —y que fue evitada por la Corte de California—, al considerar que la fotografía (autorretrato) del mono no puede considerarse "obra" para efectos de la protección de leyes autorales.[23]

Tales aseveraciones permiten determinar que David Slater no se encuentra posibilitado legalmente para percibir pago o contraprestación alguna bajo la modalidad de *royalty* (regalía), sin que resulte óbice para la percepción de ganancia lícita si se estudia la fotografía desde el punto de vista del soporte material. Es decir, si bien es cierto la creación en comento no es considerada obra por no haber sido materializad por una persona física, no menos cierto lo es, que dicho soporte material aún cuenta con la protección del mundo civilista que bien le permitiría a Slater lucrar con ésta en cualesquiera forma de disposición que éste dispusiera libremente, sin necesidad de entrar a debate ulterior relacionado con el patrimonio de la pieza, ya que, inclusive las teorías modernas del patrimonio, desestiman la posibilidad que un animal (u otra forma de vida, incluido inteligencia artificial) sea susceptible de generar patrimonio.

[21] JUSTIA. Naruto *v. David John Slater et al, No. 3:2015cv04324 - Document 45 (N.D. Cal. 2016). ORDER GRANTING MOTIONS TO DISMISS by Judge William H. Orrick granting 24 Motion to Dismiss and 28 Motion to Dismiss for Lack of Jurisdiction. Defendants' motions to dismiss are GRANTED.* Puede consultar la sentencia íntegra a través del vínculo http://law.justia.com/cases/federal/district-courts/california/candce/3:2015cv04324/291324/45/ visualizado el pasado 22 de junio de 2016. El fallo y la sección 306 que se invocó al proceso indica que las "obras" no creadas por seres humanos se consideran "not copyrightable", sin embargo, a parecer del escritor, brindé la definición más adecuada.

[22] WIPO, *Glosario*. Definición en español de "autor". Puede consultar la misma (y la definición en francés e inglés) a través del vínculo ftp://ftp.wipo.int/pub/library/ebooks/wipopublications/wipo_pub_816_efs-ocr-sp-image.pdf

[23] ALLEN Green, David. *Copyright: No time to monkey around.* WIPO MAGAZINE. Versión en línea para consulta a través del vínculo http://www.wipo.int/wipo_magazine/en/2014/05/article_0004.html visto el pasado 19 de junio de 2016.

En el afán de no transformar el presente en un texto de ciencia ficción, el Derecho Positivo que se analizó (Convenio de Berna, *Copyright Act* y *Compendium Dec 2014*), desestima cualquier posibilidad que cualquier forma de inteligencia diversa a la humana sea titular de derechos de autor, es decir, a pesar de los avances que la IA ha mostrado y en algunas ocasiones, "inteligencia superior" sobre sus creadores humanos, no cumple con los requisitos para ser considerada "autor". Máxime, si agregamos a la ecuación de estudio el concepto *artificial*, mismo que la RAE define como "hecho por mano o arte del hombre, no natural, falso, producido por el ingenio humano". Acepciones que parecen guiar nuestro camino jurídico a pensar que las creaciones emitidas por IA son consecuencia de la programación humana, es decir, obras cuya fijación original se realizó sobre (con) un programa de cómputo inteligente.

Independientemente de lo anterior, el Glosario de la Organización Mundial de la Propiedad Intelectual no es imperante al afirmar que las obras creadas a través de ordenadores, como sería el caso de *Daddy's Car* o la "imagen de IA", pertenecen enteramente a sus programadores y que estos no generan un Derecho de autor reivindicable a algún sujeto de Derecho. Al contrario, al definir *obra creada por ordenador* prescribe que: "es una obra generada mediante un "programa de ordenador por el que se dan instrucciones a una máquina de tratamiento de información para que haga, según ciertas normas, una determinada selección de los datos almacenados en la máquina, componiendo así una nueva "obra" trátese de una "traducción, un nuevo texto, un dibujo, una obra musical o un nuevo programa de ordenador".

Es discutible si estos productos de computadora pueden considerarse obras protegidas por el "derecho de autor y, en caso afirmativo, quién sea el "titular de los derechos de los autores sobre tales obras".[24]

Si bien podría considerarse paranoica la interpretación en el sentido que la WIPO pretendió afirmar que el programa de cómputo resulta ser el titular de los derechos de autor, no menos cierto lo es, que su definición —un criterio internacional— no permite afirmar categóricamente que únicamente los seres humanos con conciencia e inteligencia pueden generar creaciones susceptibles de protección mediante el Derecho de Autor; esto, ya que si bien los

[24] WIPO, *Glosario*. Definición en español de "obra creada por ordenador". Puede consultar la misma (y la definición en francés e inglés) a través del vínculo ftp://ftp.wipo.int/pub/library/ebooks/wipopublications/wipo_pub_816_efs-ocr-sp-image.pdf. En afán de ampliar la duda de mi lector, me permito invocar la definición de "programa de ordenador" que brinda el propio glosario, a saber: "Es un conjunto de instrucciones que, cuando se incorpora a un soporte legible por máquina puede hacer que una máquina con capacidad para el tratamiento de la información indique, realice o consiga una función, tarea o resultados determinados. Cada vez se acepta con mayor frecuencia que los programas originales son obras acreedores a la protección que otorga el derecho de autor: en algunas legislaciones de derechos de autor se hace ya una referencia explícita a ellas

argumentos pudieren resultar suficientemente sólidos para defender la titularidad de dichas obras a favor de los programadores o mecenas involucrados en la creación, casos de autonomía creativa como el mostrado por la IA de IBM, permite discutir si dicha imagen puede considerarse obra y, por otro lado, a quién pertenecerían los derechos de autor sobre la misma.

Al respecto, en octubre de 2017, la Organización Mundial de la Propiedad Intelectual parece abrir la posibilidad de debatir sobre la calidad jurídica de "autor", atribuible a favor de la Inteligencia Artificial, según se desprende de la *Revista WIPO* en el artículo *Artificial Intelligence and Copyright*.

En el contenido de dicho trabajo de investigación, Andrés Guadamuz, propone la posibilidad de considerar como autor a una computadora, derivado de la originalidad y autonomía con la cual puede actuar un programa de cómputo, asimismo, pone de énfasis los retratos que generó inteligencia artificial en conmemoración de Reinbrandt Harmenszoon, lo cual podría brindar mérito artístico a dichas pinturas.[25]

En ese tenor, el dilema jurídico permitiría sostener dos posturas, igualmente válidas: *i)* Que IBM es el titular de los derechos de autor sobre la imagen que nos ocupa o *ii)* Que la creación artística no se puede vincular a un autor, que permita considerarse susceptible de protección. Más allá de lo ocurrido en el escenario de la canción Daddy's Car, compuesta con ayuda del software Flow Machine,[26] en que la IA únicamente opera como herramienta auxiliar en la creación de Derechos de autor; en este caso presenciamos un gran momento histórico vaticinado por Turing, en que la IA autónomamente creó una obra artística no susceptible de protección ni registro.

Sin considerar por ahora el caso de la inteligencia artificial "autora" que creó IBM, los casos anteriores parecerían romper la fortaleza del argumento que defiende que un robot es un objeto de derecho y no un sujeto de derecho. El argumento generalmente aceptado, entiende que las personas físicas o morales detrás de la creación de un robot, con o sin inteligencia artificial, son las responsables directas, objetiva o subjetivamente, de las conductas de su creación, sin embargo, ese razonamiento se destruye cuando al robot en cuestión se le reconoce ciudadanía, derechos, privilegios y obligaciones.

Por lo anterior, parecería que históricamente, nos encontramos en un momento en el que el paradigma de la titularidad exclusiva de derechos a favor de la especie

[25] GUADAMUZ, Andrés. "Artificial Intelligence and copyright". WIPO. Octubre de 2017. *Revista de la OMPI*. 05/2017.

[26] LIMÓN, Jaime (coordinador). *Antología Iberoamericana sobre Propiedad Intelectual. Daddy's Car: Inteligencia Artificial como herramienta auxiliar en la creación de derechos de autor.* México, 2018. Tirant Lo Blanch.

humana, parece desvanecerse ante la fortaleza que adquiere otro tipo de vidas, artificiales o no. Conforme lo aseverado, es inconcuso que resulta insuficiente el criterio Brown vs Tesla para desvirtuar la responsabilidad de una IA similar a *Tay* o *Sophia*, en conductas que pudieren generar afectación en esfera jurídica de particulares.

El discurso jurídico aún es muy pobre al respecto, por lo que refiere a los casos anteriormente expuestos, sin embargo, pretendo sujetar a consideración del lector la fragilidad de los axiomas tradicionales que hemos construido en afán de sentir seguridad sobre las figuras de derecho ortodoxas que ahora lucen insuficientes ante las nuevas corrientes de creaciones tecnológicas.

En conclusión, si la IA cuyo acto generador de derecho se encuentra dentro de las categorías 1 a 4 expuestas en la cita 10 del presente capítulo, parecería acorde afirmar que las consecuencias de derecho deben ser referidas a los creadores, programadores u operadores, según resulte aplicable. En tanto que la IA/robots que pertenezcan a categorías superiores (4 y 5), deben ser objeto de análisis posterior respecto de su autonomía y el deslinde de responsabilidades a cargo de cualquier persona jurídica detrás de su creación.

El siguiente nivel de debate radica en crear las normas jurídicas y sanciones adecuadas para la IA que pudiere alcanzar el nivel de sujeto de derecho, como ya ocurre hoy en día y, en el diálogo que ya alcanzó nuestros días, se han conformado grupos de científicos y ciudadanos que ya analizan la proximidad en la substitución del hombre a causa de las máquinas automatizas; prueba de lo último, son las publicaciones similares a *Sálvese quien pueda* del periodista Andrés Openheimer, *Life 3.0: Being Human in the Age of Artificial Intelligence* del autor Max Tegmark, el *Empleo del Futuro. Un análisis del impacto de las nuevas tecnologías en el Mercado Laboral,* de Manuel Alejandro Hidalgo, *El Ascenso de los Robot. La amenaza de un futuro sin Empleo,* de Martin Ford, y *Una Mirada al Futuro. Inteligencia Artificial, Abundancia, Empleo y Sociedad* de Antonio Orbe. Todas estas obras parecen refrendar la preocupación que la ciencia ficción otrora permeó en el subconsciente colectivo; sin embargo, estudios como el emitido por la Oficina de Información Científica y Tecnología para el Congreso de la Unión (INCyTU) afirman que para el año 2025 el valor del mercado mundial de las aplicaciones de Inteligencia Artificial será de hasta 126 mil millones de dólares, lo que pretende substituir inicialmente las habilidades manuales del ser humano, en tanto que aquellas que requieran capacidades sociales, de análisis, negociación, tutoría, empatía y creatividad, no formarán parte del 65% de los sectores que se verían afectados, sobre todo en países en vías de desarrollo.[27]

[27] LIMÓN, Jaime. *Las 10 profesiones que desaparecerán con la Inteligencia Artificial.* México, Octubre 2018. Foro Jurídico. Política. Visto el 21 de octubre de 2018 a través del vínculo https://forojuridico.mx/las-10-profesiones-que-desapareceran-con-la-inteligencia-artificial/

El caso más reciente y cuyo estudio ya es materia de jurisconsultos alrededor del orbe, es la Norma de Derecho civil sobre robótica[28] misma que se aprobó en Estrasburgo el 16 de febrero de 2017 por el Parlamento Europeo. En dicha norma, no sólo se pretende generar una definición uniforme de robot e inteligencia artificial, sino aplicar las *Leyes de Asimov* al texto legislativo; en lo particular, destacan los siguientes principios:

- Aclarar que los organismos ciberfísicos no cuentan con "vida" en un sentido biológico.
- La creación de un sistema global de registro de robots avanzados dentro del mercado interior de la Unión.
- Desarrollo de tecnología que pretenda complementar las capacidades humanas y no a sustituirlas; considera fundamental que, en el desarrollo de la robótica y los sistemas de inteligencia artificial, los seres humanos tengan en todo momento el coutrol sobre las máquinas inteligentes.
- Equipar a las ruáquinas que operen con inteligencia artificial de una "caja negra" que permite registrar sus decisiones y que éstas sean legibles para el ser humano.

Principios que, sin duda, resaltan la importancia al dedicar un capítulo especial en la presente obra.

[28] PARLAMENTO EUROPEO. *Normas de Derecho civil sobre robótica P8_TA(2017)0051*. Estrasburgo, 16 de febrero de 2017. Visible el 28 de octubre de 2018 a través del vínculo http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//ES

V
CAPÍTULO

Explotación Digital de los Derechos de Autor[1]

El crecimiento del *ciberespacio* y volatilidad de la Sociedad de la Información han generado que algunas figuras tradicionales del sistema objetivo (Copyright) y del sistema subjetivo (derechos de autor) de protección autoral resulten obsoletos ante la constante demanda de mejores mecanismos de protección en la red de redes (Internet), toda vez que el creciente número de violaciones y delitos han sobrepasado las calificaciones jurídicas que tradicionalmente se han abordado en el derecho internacional privado (DIPr), ya sea adaptando figuras nacionales de propiedad intelectual a los medios digitales o suscribiendo tratados internacionales que procuran ofrecer una salida homogénea a las inquietudes de los creadores ante los casi instantáneos daños y perjuicios que ocurren con la simple reproducción de sus obras en medios digitales (*upload*) y de la inmediata disposición en que los internautas tienen la facultad de conocer, reproducir, distribuir, comunicar, modificar y explotar dichos contenidos (*download*) a través de medios como lo son servidores *FTP*, correo electrónico, *WWW*, aplicaciones y un sinfín de herramientas tecnológicas que, en la mayoría de los casos, son creadas para percibir fines de mejoramiento de la difusión del patrimonio cultural.

[1] LIMÓN, Jaime. Obra versionada de la original *Explotación Digital de la Propiedad Intelectual*, publicado en México, Septiembre de 2015, a través de Foro Jurídico; disponible en https://www.foro-juridico.org.mx/explotacion-digital-de-la-propiedad-intelectual/

Sin embargo, no es permisible en nuestra labor jurídica abordar interpretaciones paranoicas o hipótesis apocalípticas respecto del futuro de la propiedad intelectual en el ámbito digital, al contrario es nuestra encomienda generacional el ofrecer nuevas rutas de proceso hermenéutico de los cuerpos normativos autorales y adaptarlos a las uecesidades que hoy nos ocupan, portando decorosamente, la consigna académica de impedir que los hechos reales superen la cantidad de hipótesis jurídicas y por tanto que pudieren transformar en obsoleto el estudio del fascinante mundo de la propiedad intelectual. A saber de la artista británica Mycelia, no es posible avanzar mucho musicalmente, sin toparte con la tecnología.[2]

Uno de los principales obstáculos que enfrenta la vigilancia de la propiedad intelectual en la telaraña informática, es la pluralidad de sistemas en que se rigen los Estados, por un lado el sistema de protección económico y despersonalizado en que se basa el *Copyright* frente a aquel que defiende el carácter personalísimo de cada una de las creaciones en materia de derechos de autor, otorgando un valor meritorio a los derechos morales frente a los derechos patrimoniales.

Esta duplicidad no sólo afecta desde el punto de vista doctrinal el estudio de las "obras digitales",[3] sino que tiene un resultado práctico, en las varias complicaciones al momento para procesal y procesal, en que el autor que presume una violación en su perjuicio, debe elegir el derecho aplicable y sobre el cual solicite la protección y reparación de los daños ocasiones por el ilegal actuar de terceros, muchas veces desconocidos al disfrazar su actuar con el anonimato que ofrece el ciberespacio; así las cosas, el infractor puede descargar una obra que se encuentra en un servidor en Colombia, desde su equipo de cómputo en México y, posteriormente, modificar la obra, para "subir" (*upload*) de nuevo dicho contenido, a una página web con servidor en Estados Unidos de América.

Bajo tal supuesto, es lógico complicar el panorama normativo que deberá aplicarse al caso concreto, pues ¿qué tribunales serían los competentes para resarcir el daño?, ¿qué tribunal podría ejercer una medida cautelar efectiva? En caso de obtener

[2] JEWELL, Catherine. "Mycelia: una nueva configuración del panorama musical". División de comunicaciones de la OMPI. *OMPI Revista*. Abril de 2016. Visible a través del vínculo http://www.wipo.int/export/sites/www/wipo_magazine/es/pdf/2016/wipo_pub_121_2016_02.pdf el 02 de diciembre de 2017.

[3] Conforme lo refiere la Maestra Lydia Esteve González, en su obra "Aspectos internacionales de las infracciones de derechos de autor en Internet", Editorial Comares, Granada 2006; no se pueden abandonar todas las figuras preexistentes de derechos de autor, ni de propiedad intelectual, sino que se deben rescatar aquellas que, en el entorno digital, permitan una adecuada aplicación. Así las cosas, es correcto hablar de obra digital como la idea original materializada y tangible, sin que el concepto de traducción material impida la correcta apreciación del concepto de "obra", ya que, tal como también lo reconoce la profesora y directora de la Universidad de Alicante, el que la idea original exista en el mundo digital y se publique en Internet, resulta la figura que, por equiparación, nos permite comprender la figura de las obras en el entorno digital.

una sentencia favorable, ¿dicho tribunal tendría facultades para ejecutar la sentencia en el Estado o Estados, sin afectar la soberanía y autonomía de otras naciones, de forma efectiva?

Una de las probables salidas que ofrecen los autores modernos[4] es comenzar a resolver el rompecabezas de DIPr, bajo el criterio de flexibilizar los conceptos que tradicionalmente se respetan, para lograr una mejor adecuación con lo ocurrido en el entorno digital. Sin embargo, dicho criterio nos invitaría a calificar cualquier mínima expresión de originalidad y de sello personalísimo, como una idea susceptible de protección bajo las reglas del Convenio de Berna (Tema aparte sería la calificación marcaria que podría ofrecer el Convenio de París); esto es, que expresiones en correos electrónicos, comentarios en Youtube sobre un video popular, un tweet lanzado con perspicacia y que haya alcanzado sus mejores puntos de influencia como un *trendy topic*; inclusive un simplista comentario en un portal de opinión en Facebook podría alcanzar el calificativo de idea original y, por ende, de obra.

Dicho de otra forma, la "originalidad" reduciría sus estándares y rigidez para permitir que cualquier idea que navegue en la red de redes, pudiere alcanzar el calificativo de obra. Tal como analizaremos más adelante en el desarrollo de la presente obra, existen principios que limitan el grado de flexibilización de la "originalidad"; como si fuere aquél, la goma que mantiene unida la teoría tradicional de protección de derechos de autor, en el ciberespacio y las redes sociales (Léase parágrafo VII.2 de *Abogado Digital)*.

En términos de dicha flexibilización es imprescindible no forzar la adaptación de figuras jurídicas que no encuentren aplicación analógica en el entorno digital. Al hablar de la concepción subjetiva de derechos de autor, siempre se destaca la existencia de los Derechos Morales como aquellas prerrogativas que son inherentes al autor, por el simple hecho de crear una obra original y plasmarla en un medio tangible y de fácil reproducción. Estos Derechos Morales adquieren diversos nombres, denominaciones, inclusive la cantidad de prerrogativas consideradas como morales varían de una legislación a otra, sin embargo, son fundamentales: 1) Paternidad, 2) Divulgación, 3) Oposición, 4) Retiro y, 5) Integridad. En la praxis de la navegación autoral, se ha puesto en evidencia que la figura de la Divulgación y del Retiro, adquieren una naturaleza diferente a aquella bajo la cual han sido concebidos tradicionalmente, en primer lugar, toda vez que la divulgación no ocurre con la formalidad que aparece en el sistema tradicional de derechos de autor, ya que ésta viene aparejada de Derechos Patrimoniales de comunicación, reproducción, distribución y en general, a la puesta a disposición para cualquier tipo de persona que tenga acceso a Internet, impidiendo que el autor controle la forma en que se realiza esa exposición de su idea original y que elimina el carácter inédito de la misma; a su vez, la posibilidad de retirar una obra que ha ingresado a Internet mediante el uso de servicio de

[4] Autores como Lydia Esteve, Calvo Caravaca, A.L. y Carrascosa González, J.

WWW, correo electrónico o redes sociales resulta prácticamente imposible de sustraerse de la telaraña informática, no sólo complicando de forma evidente el ejercicio del Derecho Moral de Retiro que se defiende en el sistema tradicional de derechos de autor (subjetiva), sino complicando, en la mayor cantidad de hipótesis procesales, a la correcta aplicación de medidas cautelares solicitadas u ordenadas por Tribunales de un Estado en su propio territorio y máxime, cuando se trata de Tribunales que pretenden hacer valer dichas medidas en Estados cuya soberanía no les corresponde, independientemente de las facultades que pudieren adquirir por el principio de *lex loci protectionis*. Ahora bien, por lo que refiere a la clasificación de los Derechos Patrimoniales desde el punto de vista subjetivista, estos son tan diversos como los supuestos que las legislaciones nacionales han decidido abordar en apego al Convenio de Berna, empero, en este caso ocupa nuestra especial atención el derecho patrimonial de exportación-importación. Lo anterior, ya que la red de redes tiene entre sus características principales, que ésta carece de muros territoriales que permitan calificar la distinción de la Nación a la que pertenecen[5] y tal como se expuso con anterioridad, el autor digital difícilmente puede controlar el destino de su obra una vez que ésta ha ingresado en la red de redes, permitiendo el acceso de la obra digital, no sólo en el país que corresponde al domicilio del autor digital, no sólo del servidor al que pertenece el portal, FTP o conexión *Peer to Peer* que es utilizada por el creador (*Internet Service Provider*) , sino que ésta se encuentra a disposición de cualquier ser humano con la posibilidad de tener acceso a Internet.

Todo lo anterior no resta importancia a las preguntas que formulamos en párrafos anteriores, ya que la doctrina internacional ha resuelto que como límite jurisdiccional y criterio de competencia entre Tribunales Internacionales, se puede aplicar como regla general el Convenio de Berna/París para vigilar y perseguir las infracciones o delitos, mientras que Convenios de carácter volitivo, como lo es el Convenio de Roma, permiten contar con un mecanismo de solución de coutroversias desde el DIPr, originado por contratos; ello, siempre y cuando las partes no hubiesen sometido la jurisdicción del acuerdo de voluntades a una circunscripción de su preferencia, ya sea por razón de domicilio (*lex forum)* o por el beneficio jurídico que ello implica; hipótesis que resulta más difusa, al oponerse cualquier pugna sobre las directrices de las redes sociales que pretenden subsumir cualquier controversia a la jurisdicción de su conveniencia, lo que podría provocar la indefensión total de la víctima.

[5] Es importante destacar la distinción existente la anti territorialidad a la que se atañe Internet, pues a pesar de que esta fue creada por Estados Unidos, la misma no le pertenece a dicho Estado, así como las Olimpiadas no le pertenecen a Grecia. Ello, independientemente de que sea posible determinar con cierto nivel de convicción la procedencia de ciertos portales o servidores mediante los sufijos "ue, mx, co, us, etcétera". Muller, M, "Who Own The Internet? Ownership as a Legal Basis for American Control of Internet", Prop. Media & Ent, Volumen 15, 2005.

Ya expuesta la pluralidad sistemática (sistema subjetivo u objetivo), las Cortes Internacionales han sido congruentes en que uno de los conceptos que vale la pena rescatar del sistema tradicional es el de Integridad de la Obra Digital. En este sentido, la figura tradicional de derecho de autor, otorga la prerrogativa personalísima al autor de la idea original de modificar su obra y a terceros, siempre que exista el consentimiento expreso del titular del Derecho moral.

En el entorno digital dicha figura no pierde la fortaleza bajo la cual está consagrada, al contrario, el Convenio de Berna, Convenio de Roma y el Reglamento de Bruselas son consistentes en mantener el rigor sobre las sanciones a que se hacen acreedores aquéllos que modifican una obra, sin autorización del autor y sin incurrir en algunos de los casos de excepción previstos por dichos cuerpos Internacionales (en el sistema objetivo lo conocemos como *fair use* bajo el Acta 107), cuyas limitaciones las encontramos, por ejemplo, en la alteración de las obras tradicionales o digitales, para compartir la idea original –en la medida de la adaptación posible- con terceros con capacidades diferentes o de percepción disminuida.

Sin embargo y tal como lo expusimos con anterioridad, los autores modernos defienden la idea de la flexibilización jurídica de un *numerus clausus* de conceptos, entre ellos, el de integridad *versus* modificación de la obra. Lo anterior, bajo la noción esencial del funcionamiento tradicional de Internet y los protocolos de transferencia de datos bajo los cuales opera; lo anterior adquiere sentido, toda vez que la obra tradicional al ser ingresada al entorno digital transforma su naturaleza, en primera instancia, para ser fragmentada y enviada a través del ciberespacio en paquetes que pueden ser enviados mediante un protocolo de paquetería que modifica la obra digital en código binario.

Este proceso de desfragmentación no sólo implica la modificación de la obra, sino la reproducción temporal de la obra digital aún ininteligible para el humano, creando copias *ex novo* para el proceso de digitalización de la obra, procedimiento que se multiplica cuando la obra, adicionalmente, es enviada a algún destinatario de correo electrónico, en cuyo caso la obra "original" digital se encuentra en dos momentos (o más) a la vez, en el correo electrónico origen, en la *World Wide Web* y en el correo electrónico destino. En este ejercicio de reproducción, el criterio internacional ha determinado que las copias temporales que los protocolos requieren para la desfragmentación y de nuevo, fragmentación de los paquetes en la web, no significan una variación económica significativa que pudiere generar un perjuicio a los beneficios que pudiere obtener el autor de la idea original bajo su normal explotación. [6]

Por otro lado, la policía cibernética y organizaciones como la Corte de Bruselas y la Organización Mundial de la Propiedad Industrial han determinado que existen prácticas de navegación que no sólo atentan contra la propiedad intelectual, sino

[6] Dentro del proceso de copiado temporal, también se engloba aquellas que realiza el ordenador a través de la memoria RAM (*Read Access Memory*)

contra la información confidencial y los límites de fondo que el autor digital hubiese esperado de sus ideas originales; estas prácticas consisten en utilizar fragmentos de otro portal dentro de la *WWW* o redireccionar dicho contenido a través de una página web sin obtener la autorización requerida por el titular, ya que es una falacia entre los internautas que, todo lo que se encuentra en la red de redes, es gratis y utilizable.

En primer lugar, tenemos el *framing* que consiste en utilizar impresiones de pantalla de otros portales sin reconocer la titularidad de los autores, así, el infractor recurre a esta práctica ante la necesidad de citar información para manuales, blogs y más comúnmente, en redes sociales al compartir imágenes que simplemente se han descargado para volverse a cargar en un tweet o comentario en *Facebook*. Por otro lado, tenemos el *linking* que es utilizado en mayor parte por reporteros o curadores de información que reutilizan la información que se encuentra en la web, le agregan el sello personalísimo de crónica bajo el cual fueron contratados, pero en el cuerpo del documento utilizan hipervínculos que permiten direccionar el contenido de la página hacia otro portal, impidiendo que el internauta reconozca los límites de paternidad, partiendo del supuesto que ahora se encuentra en otro *layout* del mismo autor.

En este último caso, el *linking* constituye un campo de estudio peculiar, ya que si bien la práctica de agregar hipervínculos de navegación debe cumplir con las reglas de autorización como si se tratase de una cita en el sistema tradicional de derechos de autor,[7] independientemente, de si dicho vínculo direccionará al internauta a la página de origen o ésta permitirá la navegación a un subportal dentro de aquella, no menos cierto lo es, que la redacción del texto que permita el *hiper enlance* puede ser una idea original que *per se* adquiera derechos de protección autoral, debiendo realizar la ligera distinción entre lo que pertenece a uno y otro autor. La necesidad de la comprensión de dichas figuras radica en la posibilidad de determinar la responsabilidad principal del infractor y la subsidiaria o secundaria, del ISP que no retire el contenido protegido de sus portales; en este caso, resulta en algo trascendente que la *praxis* internacional ha logrado identificar el grado de responsabilidad de los proveedores del servicio de Internet *versus* la responsabilidad de los infractores. Lo anterior, independientemente de las consecuencias jurídicas que ocurran en derecho marcario.

Conforme lo que se ha expuesto hasta ahora, debemos poner de relieve la importancia de la más grande cuestión dentro del estudio de la información en el ámbito digital: ¿Requerimos de nuevas reglas para proteger las obras digitales en el *ciberespacio*? Aparentemente, todo implica un análisis minucioso sobre cada una de las

[7] En la práctica, se reconoce que el *linking* es la figura que mejor se adapta al ámbito digital y que tiene su similar en el derecho de cita, del sistema tradicional de protección. Por lo que el *linking*, como el derecho de cita, también debe cumplir ciertas reglas para su utilización, como lo son: 1) citar la fuente, 2) fecha y hora de consulta y 3) permitir que el internauta reconozca la diferencia entre el cuerpo del texto y la reproducción parcial de la que se trata, por tanto, permitiendo la distinción de autores en el documento; siempre y cuando dicho *linking* se practique sin fines de lucro, en caso contrario, se requiere de la autorización del titular conforme las reglas del sistema tradicional.

figuras de derecho que actualmente existen, sin embargo, la tendencia que debemos seguir radica en adaptar los conceptos jurídicos que otorguen un mejor beneficio de protección a la obra digital y a los autores digitales, flexibilizando aquéllos que, por su naturaleza, requieran de un estudio más laxo en el entorno digital. Así las cosas, podríamos estar en la época que requiere de la creación de nuevos conceptos de Derechos Morales y Patrimoniales (concepción subjetiva) y en la fortaleza del *Digital Copyleft* (concepción objetiva). Un claro ejemplo de ello, es la inadecuada apreciación de los derechos patrimoniales de reproducción y comunicación, en el ámbito digital dada la imposibilidad material de distinguir dichas figuras respecto del derecho patrimonial de explotación digital, dado que el proceso de *upload* inmediatamente implica la aceptación del autor de reproducir y comunicar su obra, ya que, tal como se narró anteriormente, el proceso de carga en la red de redes implica la creación de un sinnúmero de copias que son permisibles dentro del proceso del protocolo (*TCP/IP)*, iniciando el proceso de reproducción bajo la consigna de comunicación web, asimismo, la comunicación de la obra digital es automática al momento en que el autor digital agota su prerrogativa del derecho moral de Divulgación.

En este sentido, la explotación digital bien puede formar parte del derecho patrimonial de mayor trascendencia en el entorno digital y que el sistema americano de *copyright* lo sostenga como el pináculo de retribución económica autoral y como centro de estudio para la mayor cantidad de licencias digitales que se otorgan en el *ciberespacio*, resulta lógico bajo la tendencia que exigen los negocios jurídicos actuales. Bajo esta dinámica se torna necesario la creación de mecanismos jurídicos que distingan los usos legítimos de obras digitales y aquéllos que, por el perjuicio económico que provocan a ésta, no pueden ser considerados dentro de la familia del *fair use* (concepción objetiva) o *excepciones* (concepción subjetiva).

Para determinar tales hipótesis las Cortes y Tratados Internacionales han establecido los criterios aplicables para determinar la presencia de usos permitidos por la ley nacional o los cuerpos normativos internaciones:

i. El sistema de protección *copyright* prevé que los usos legales (*fair use*) se determinarán casuísticamente, conforme lo establece el criterio *common law*; sin embargo, esta dinámica se estudiará en término de las demandas de los autores digitales ante los Tribunales Nacionales, es decir, a *posteriori* de la conducta que pudiere resultar infractora y generar un daño en la esfera de la propiedad intelectual
ii. La familia que defiende la concepción subjetiva, se sujetan a las reglas previstas en el Convenio de Berna, bajo la fórmula *Three Step Test:*[8]

[8] Convenio de Berna, artículo 9.2, consultado en línea a través del portal http://www.wipo.org el 17 de abril de 2015

1. Que la conducta se encuentre prevista en el sistema tradicional de excepciones del derecho de autor
2. Que la conducta no afecte el normal beneficio económico que puede obtener el autor de la obra (similar a la hipótesis de *fair use* citada con anterioridad, mediante la cual se permite realizar copias autorizadas por los procesos del protocolo *TCP/IP*), es decir, que realizando dichas conductas no se detienen los beneficios económicos que podría recibir el autor digital.
3. Que la conducta no depare un perjuicio injustificado e indeterminado al patrimonio del autor. A este último examen contenido en el Convenio de Berna, se le conoce también como el "examen económico de Berna", toda vez que regula las excepciones respecto de las cuales no se requiere autorización del autor, únicamente desde el punto de vista de los derechos patrimoniales, sin detenerse a realizar un estricto examen de fondo, sobre los derechos morales.

Después de la breve exposición del comportamiento de la propiedad intelectual en la telaraña digital, hemos tratado de aproximar al lector a las inquietudes que se abordaron inicialmente, además, de defender la postura de la creación de nuevas figuras de derechos de autor cuando el caso lo amerite o realizar el trabajo de deconstrucción de conceptos, para adaptar figuras jurídicas de antaño al nuevo entorno digital.

Una de las grandes incógnitas que no hemos abordado totalmente, es la referente a la inquietud sobre la competencia de los Tribunales Nacionales e Internacionales para resolver sobre demandas derivadas de infracciones y delitos o de desacuerdos derivados de contratos. Si bien, ya se aproximó ligeramente a la solución que nos brindan los cuerpos normativos internacionales, como lo es el Convenio de Berna (vigila infracciones y comisión de delitos) y el Convenio de Roma (vigila el cumplimiento de las obligaciones contraídas con razón de la cesión de derechos o licencias en materia de derechos de autor), debemos aproximar nuestro estudio al principio que se ha citado con anterioridad conocido en la *praxis* jurídica como *lex loci protectionis*, fundamento teórico, que beneficia la protección de la propiedad intelectual bajo la consigna de la aplicación de las normas que, de fondo, resuelvan el conflicto en el lugar en que ocurrió la infracción o se cometió el delito, evitando conflictos respecto de la ubicación del sujeto, sin embargo, la tradición internacional ha acuñado el término de *ciberdomicilio* a través del cual, ha sido posible determinar la posición que geográficamente conviene al autor que ha sufrido un menoscabo en su patrimonio; rescatando a nuestro parecer, dos principios que en derecho internacional y en derechos humanos han realizado su tarea: *pro persona* y la *interpretación conforme*; bajo los cuales ha sido posible justificar el derecho aplicable de fondo y, por tanto, las reglas del procedimiento y la competencia del juez que resolverá sobre el asunto concreto.

El *ciberdomicilio* existe como el parámetro de medición bajo el cual las partes y el juez que se estime competente, podrá determinar si el derecho que se invoca es aplicable o no; lo anterior, ya que como se ha explicado con anterioridad, los cuerpos normativos nacionales no cuentan con homogeneidad, por lo que es posible que no en todos los Estados se protejan los mismos derechos de autor, ni mucho menos, que se protejan con los mismos alcances; así las cosas, una violación que puede estar ocurriendo en estos momentos en Estados Unidos, puede ser considerada de una manera completamente diferente para un Tribunal en España en el que se practica el derecho a través de la concepción subjetiva o, bien, de un Tribunal en China, cuyos cuerpos normativos carecen del rigor —a mi parecer— que exigen las nuevas tendencias de creación digital.

Por un lado, el sistema americano ha adoptado el examen de *personal jurisdiction*, bajo el cual, el juez al que se solicita ejerza su jurisdicción y competencia, debe analizar si en el caso concreto, cualquier decisión precautoria, perentoria o de fondo tendrá una aplicación práctica en el mundo material, es decir, el examen del juzgador consistirá en analizar los efectos jurídicos que puede llegar a tener una sentencia emitida en su circunscripción; además, estudia si las partes involucradas y el hecho que se estima infractor tiene una relación general o específica (contacto mínimo) tanto con la legislación aplicable, como con los tribunales cuya justicia se solicita; además, implica prejuzgar sobre la naturaleza de la infracción o conducta cometida y si ésta tiene una injerencia mayor en su circunscripción o en la de otro Estado soberano, así las cosas, cuando los daños o perjuicios son cometidos todos ellos en un solo Estado se habla de *general personal jurisdiction*, mientras que, en el supuesto en que dicha conducta tiene una traducción material secundaria como resultado de un indebido actuar en otras regiones y cuyas consecuencias económicas son inferiores que en otros sectores territoriales, estamos en presencia de *specific personal jurisdiction*. Verbigracia, si colocamos la hipótesis bajo la cual un tercero descarga (*download*) y modifica sin autorización la fotografía de un autor en Verona, Italia, para subirla (*upload*) en un diario local en Chile como parte de uno de sus artículos como "curador de información", la cual tendrá su hospedaje cibernético gracias al servicio que otorga un prestador en México; estamos en presencia de una violación de derechos de autor (bajo la concepción subjetiva), no sólo en el aspecto patrimonial, sino moral, al momento en que el curador Chileno, se ostenta como propietario de la obra original digital; conducta que de forma evidente puede tener repercusiones legales en México, Italia y Chile, si es que sólo se usa la concepción tradicional de domicilio.

Sin embargo, supongamos que gracias a dicho artículo, el autor chileno adquiere renombre en la Costa Oeste de los Estados Unidos y es invitado a impartir una serie de conferencias sobre las cuales recibe una remuneración evidente y adquiere renombre a costa de la creación original del autor italiano, ¿complicado? Sí, si comenzamos a agregar todas las hipótesis que podrían ocurrir en realidad, sin

embargo, el límite lo han colocado los propios organismos internacionales bajo el concepto del *ciberdomicilio*, bajo el cual, el autor tiene la prerrogativa de solicitar la protección del Estado en la que estime que obtendrá un mejor beneficio, concede el Tribunal de causa, la posibilidad de determinar si la sentencia que dicte tendrá los efectos deseados bajo el principio de una correcta aplicación de la *Tutela* Judicial *Efectiva*.

Así las cosas, el autor digital podría solicitar la reparación del daño, la detención de la conducta infractora y hacer valer en una sola vía e instancia, el interés jurídico que pudo haber hecho valer en cualquier parte del mundo, delimitando así, el espacio geográfico sobre el cual se puede hacer valer efectivamente el interés jurídico bajo la noción de la competencia otorgada por el *ciberdomicilio*. Por lo tanto, en nuestro ejemplo anterior, sería mucho más práctico que el autor italiano, hiciera valer su interés jurídico mediante una acción en los Tribunales chilenos, de tal suerte que las medidas precautorias tendrían una más pronta y efectiva ejecución, inclusive, la ejecución de una posible sentencia sobre los bienes del autor plagiario, en caso de estimar procedente el pago de daños y perjuicios a favor del autor digital.

Empero, todo lo anterior no implica que el creador de la idea original carezca de interés jurídico para hacer valer un derecho en México, Italia o Estados Unidos, sin embargo, bajo los criterios antes expuestos se advierte la competencia a favor de los juzgadores andinos.

Conforme la exposición anterior, es inconcuso que nos encontramos en un momento único jurídicamente hablando, en el que tenemos en nuestras manos la facultad y posibilidad real de construir nuevas figuras de derecho cibernético que no sólo regulen la propiedad intelectual en el ciberespacio, sino que de a poco, transformen otras ramas del Derecho hasta comprender la imperante necesidad de crear una nueva línea de estudio a través del Derecho Informático como una nueva visión, una nueva óptica bajo la cual es posible construir nuevos conceptos en beneficios de las herramientas cibernéticas con que contamos hoy en día y evitar que la realidad social supere nuestros grandes cuerpos normativos.

Entonces, es ineludible afirmar que la propiedad intelectual se encuentra a salvo, "hospedada" en la máxima red de redes jamás construida por el hombre, sin embargo, su casi autónomo crecimiento no puede invitarnos a abandonar el estudio de su protección, muy en cambio, debe consagrar la creación de nuevas leyendas jurídicas en el ciberespacio.

La filosofía de I Ching supone un universo regido por el principio del cambio y la relación dialéctica entre los opuestos, en la que la única realidad existente en el ser, es el cambio; bajo ese supuesto, hoy en día debemos aceptar que existen un cúmulo de figuras jurídicas en el ámbito de la propiedad intelectual que fueron creadas para otorgar equilibrio a las creaciones dentro del sistema tradicional pero que, hoy en día, nos exigen apoyar su transformación y seguir su rumbo de crecimiento en el *ciberespacio,* para transformarlas en el nuevo *sistema digital de protección intelectual.*

Sobre el particular, invocaré cuatro normas que resultan fundamentales para el estudio de los Derechos de autor en el ámbito digital.

V. 1 *Digital Millennium Copyright Act*

Documento legal que se acuñó en octubre de 1998 por la oficina de Derechos de Autor de los Estados Unidos de América, es el resultado de la aplicación y cumplimiento de 2 tratados internacionales administrados por la Organización Mundial de la Propiedad Intelectual: 1) Tratado de Derechos de Autor de la OMPI y 2) Tratado de la OMPI para protección de presentaciones y fonogramas.

El texto oficial se encuentra disponible a través de la página oficial de la Organización Mundial de la Propiedad Intelectual[9] y refleja las pautas mínimas de su implementación y ajustes indispensables a los tratados de la OMPI. Sobre el particular, destaca lo siguiente:

- Prohibición de aplicar medidas tecnológicas que impidan la cousulta de las obras en medios tradicionales, asimismo, se castiga cualquier acto tendiente a desencriptar o encriptar una obra protegida por la oficina de Derechos de Autor.

  - La prohibición a que hace referencia este apartado, así como la encriptación referida, serán considerados lícitas cuando de ello dependa la protección de la personalidad o infornación que permita identificar datos personales sensibles de terceros.

- Medidas eu contra de los dispositivos análogos, 18 meses después de la entrada en vigor de la *DMCA*, se dictó que sería prohibitivo el producir, importar u ofrecer públicamente cualquier obra que se encuentre disponible en formato VHS, 8mm o Beta. De esta forma, la medida pretende eliminar cualquier dispositivo análogo que impida la divulgación de las obras a través del ámbito digital.
- La sección 1203 refleja lo que hemos expuesto con anterioridad, pues faculta a la persona que estime violaciones en sus derechos de autor, para iniciar cualquier acción de naturaleza civil, en la corte y distrito competente de los Estados Unidos de América. Tal como lo refleja la Ley Federal del Derecho de Autor (México), el numeral (3) de la sección que nos ocupa, determina indemnizaciones mínimas por violaciones contenidas en las sección 1201, por lo

[9] LEGISLATIVE HISTORY. *Digital Millennium Copyright Act.* Public Law 105-304. 20 de octubre de 1998. Visible el 14 de agosto de 2018 a través del vínculo http://www.wipo.int/wipolex/es/text.jsp?file_id=337359

que no existirá reparación inferior a los 200 dólares o superior a los 2500 dólares, por cada acto, dispositivo, producto, componente, oferta o presentación del servicio, en consideración justa del Tribunal; por su lado, en tratándose de violaciones relativas a la sección 1202, la suma de la indemnización no podrá ser inferior a 2500 dólares o superior a los 25, 000 dólares, por acto.

- A diferencia de otros cuerpos normativos, la *DMCA* es precisa en los límites de responsabilidad civil y penal, sin embargo, destaca la responsabilidad de los proveedores de servicio, sobre todo, en aquellos casos en que aquéllos vinculen sus portales con sitios que promuevan violaciones en materia de derechos de autor; salvo que estos no tengan conocimiento de la ilegalidad del sitio vinculado. En ese mismo tenor, no se podrá responsabilizar al proveedor de servicio que elimine, baje o deshabilite el acceso a material que se encuentra *sub judice* en materia de derechos de autor.
- A diferencia de las excepciones tradicionales del sistema objetivo de derechos de autor, la sección 117 del título 17 del Código de los Estados Unidos, ahora permite la posibilidad de realizar copias de seguridad o respaldo, sobre todo en caso de reparaciones y mantenimiento de equipos de cómputo, a todo el software que hubiere instalado sobre dicho equipo.

V. 2 Tratado de la OMPI sobre Derecho de Autor

Tal como lo refiere la propia Organización en su sitio oficial[10], este Tratado es un arreglo particular adoptado en virtud del Convenio de Berna que trata de la protección de las obras y los derechos de sus autores en el entorno digital. Adicionalmente, el arreglo se ocupa de estudiar figuras destacas en la protección autoral como lo son los programas de computadora y las compilaciones de datos (bases de datos).

Este texto entraría en vigor el 6 de marzo de 2002, seis años después de su concepción en diciembre de 1996. Conforme lo anterior, es imperativo recordar a mi lector que cualquier artículo de dicho Tratado se debe interpretar y leer armónicamente con el Convenio de Berna que antes hemos referido; sin embargo, para efectos de la presente obra, vale la pena destacar las siguientes precisiones normativas:

- Los artículos 4 y 5 definen a los programas de cómputo y bases de datos, desde el punto de vista de los derechos de autor. En el caso del primero, recuerda la importancia de estudiar el software desde la perspectiva de las obras literarias, en tanto que el quinto precepto, delimita el ámbito de protección de una base

[10] OMPI. *Tratado de la OMPI sobre Derecho de Autor.* Adoptado en Ginebra el 20 de diciembre de 1996. Visible el 14 de agosto de 2018 a través del vínculo http://www.wipo.int/wipolex/es/treaties/text.jsp?file_id=295158

de datos, únicamente a la parte original de la misma y no los datos personales o derechos de terceros, que podrían contenerse en las mismas

- Si bien es cierto, el derecho de alquiler es una fórmula del derecho de autor tradicional, el artículo 7° realiza precisiones sobre la "renta" de programas de ordenador, obras cinematográficas y obras incorporadas en fonogramas. Sobre el particular, prescribe la facultad del autor para autorizar el alquiler comercial al público del original o de los ejemplares de sus obras.
- Además del reconocimiento de fijación en medios tradicionales, el artículo 8° reconoce la facultad de los autores para comunicar al público, su obra, a través de medios alámbricos o inalámbricos, siempre que este canal permita un debido ejercicio del Derecho Moral de Divulgación que estudiamos con anterioridad.

V. 3 Music Modernization Act (MMA)

El pasado septiembre de 2018, el Senado de Estados Unidos de América aprobó por unanimidad el proyecto que pretende actualizar el sistema de licencias de música para su adaptación al panorama digital.[11] En términos generales, el proyecto normativo tiene como finalidad generar equidad en el ejercicio del derecho de divulgación de los autores y su posibilidad de obtener regalías, independientemente de la modalidad que las plataformas empleen para explotar las obras. De este esfuerzo legislativo destacan las siguientes 4 dimensiones:

- ***Mechanical Licensing Collective:*** será el organismo que emitirá las licencias mecánicas (automatizadas) para la transmisión de la música en el entorno digital. A pesar que no se confirmó el proceso tecnológico que se emplearía para ello, se estima que el organismo creará una base de datos que identifique a los titulares de derechos de las obras, lo que permitiría una transparente y eficaz vía de retribución autoral. Sin duda, ello parece emular el exitoso modelo que emplea Youtube, a través de la herramienta Content ID y Facebook, a través de Audible Magic, que se estudiarán más adelante en la presente Obra.
- **Libre autodeterminación de tarifas**: en términos de la sección 115 de la *Copyrigh Act*, dicta que los topes máximos y mínimos en el pago de regalías se fijaran por *Copyright Royalty Board (CRB)*, un organismo gubernamental responsable de aplicar estándares que no reflejan el valor del mercado. Con la reforma que propone la MMA, se substituye dicho estándar y se propone que

[11] LIEU, Ted. *Overview of the MMA*. Estados Unidos de América, Septiembre de 2018. Congresista del 33ª Distrito de California. Visto el 21 de octubre de 2018 a través del vínculo https://lieu.house.gov/sites/lieu.house.gov/files/Overview%20of%20the%20Music%20Modernization%20Act.pdf

la consideración de la corte sobre la condiciones del libre mercado en la determinación del pago de regalías.

- **El enfoque de la "rueda"/ turno:** bajo la MMA, un juez de distrito en el Distrito Sur de Nueva York sería asignado aleatoriamente desde la rueda de los jueces de distrito para disputas de fijación de tarifas. El enfoque de la "rueda" permitiría a *Broadcast Music Inc. (BMI)* y a la Sociedad Americana de Compositores, Autores y Editores (*American Society of Composers, Authors and Publishers/ ASCAP)*, así como a los licenciatarios, comparecer ante cualquier juez en el Distrito Sur de Nueva York de forma rotativa, en lugar de ser asignado a un solo juez, con el propósito de resolver conflictos de ajuste de la tasa. Este enfoque de "rueda" asegura que el juez valorará los medios de convicción y analizará los hechos de cada caso en particular, sin impresiones derivadas de casos anteriores
- **Ecosistemas digitales como evidencia**: la MMA pretende garantizar el pago directo a productores y compositores, al derogar la sección 114 de la *Copyright Act*, al permitir ofrecer pruebas sobre el comportamiento de sus obras en todas las facetas del ecosistema digital musical. Ello permitiría que los jueces consideren cada obra y autor en particular, para obtener tarifas/ regalías más justas para la comunicación pública de las obras musicales, lo que incluye la fijación que realizan los Productores de fonogramas.

El proyecto tiene un sabor dulce amargo en el proceso legislativo de los Estados Unidos de América, en tanto que organizaciones como *Grammy's Awards, Billboard, Rolling Stones Magazine*, la *Recording Industry Association of America (RIAA)* y la *National Music Publisher's Association)*, han acogido de buena manera la implementación de esta norma, otras como *Black Group* y la estación de radio *Sirius XM*[12], afirman que la presentación de más leyes autorales digitales, no substituye los mecanismos que la cibersociedad implementó y, en su caso, no demuestran éxito alguno, sobre todo en la fijación de fonogramas antes de 1972.

La oposición que presentó la MMA no prosperó y se espera que pronto obtenga la firma presidencial.

V. 4 T-MEC. United States- Mexico- Canada Agreement (USMCA)

Con la firme intención americana de abandonar el Tratado de Libre Comercio de América del Norte (TLCAN o *NAFTA* por sus siglas en inglés), el presidente Donald

[12] SUÁREZ MAGALLANES, Amanda. *El senado de EEUU aprueba por unanimidad la Music Modernization Act.* España, 24 de septiembre de 2018. Instituto de Derecho de Autor. Derechos PI, Legislación, Legislación internacional. Visto el 21 de octubre de 2018 a través del vínculo http://www.institutoautor.org/es-ES/SitePages/EstaPasandoDetalleActualidad.aspx?i=2176&s=1

Trump sujetó a consideración del gobierno canadiense y mexicano, la firma de un nuevo tratado que permitiera condiciones equitativas de comercio y cambiar las condiciones que les regían desde 1994.

En ese tenor, el proyecto de Tratado que se compone de 34 capítulos y un preámbulo, permite reconocer nuevas condiciones entre los gobiernos de América del Norte. En particular, me enfocaré en el apartado *19 Digital Trade* y *20 Intellectual Property:*

- ***Digital Trade:***[13] el capítulo 19 del T-MEC, pretende reconocer el crecimiento y oportunidades del comercio digital. Asimismo, desea generar las condiciones de confidencialidad suficientes a favor de los consumidores y evitar barreras innecesarias en el consumo electrónico. De tal suerte, el USMCA obliga a los Estados contratantes a:

  - No gravar o generar cargos fiscales de importación y exportación de productos digitales que se transmiten de forma electrónica. Sin embargo, cada Estado será libre de fijar impuestos a productos electrónicos de forma interna.
  - No discriminar los productos digitales creados, producidos, editados, contratados o comisiones en otro territorio de los Estados miembro, mediante condiciones menos favorables de mercado. Esto aplica también si el **autor, intérprete, productor, inventor o titular** es un ciudadano de otro Estado miembro, en cuyo caso, la protección a su producto digital impedirá que su obra se trate en condiciones de desigualdad.
  - Mantener un **marco legal *ad hoc* a la Ley Modelo de Comercio Electrónico (UNCITRAL) de 1996.** En ese tenor, los Estados miembros evitarán regulaciones innecesarias para las transacciones electrónicas y permitirán la participación ciudadana en la implementación de dicho marco legal (Sobre el particular, sugiero lectura al parágrafo *VIII.1.2 Precedentes sobre la aplicación de la Ley Modelo UNCITRAL* dentro de la presente Obra).
  - No negar validez a un documento por haberse firmado de forma electrónica. En ese tenor, los Estados miembro se obligan a eliminar medidas que prohíban a los contratantes celebrar el acto por medios electrónicos y fijar los mecanismos apropiados de autenticación, asimismo, a no requerir a los contratantes el perfeccionar sus actos ante autoridades administrativas o judiciales en afán de lograr la autenticación de firmas electrónicas.

[13] OFFICE OF THE UNITED STATES TRADE REPRESENTANTIVE. *United States-Mexico-Canada Agreement Agreement (USMCA).* Estados Unidos de América, Septiembre de 2018. Executive Office of the President. Resource Center. Visto el 21 de octubre de 2018 a través del vínculo https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/19%20Digital%20Trade.pdf

- Mantener transparencia y medidas efectivas para proteger al consumidor de fraudes y actividades engañosas en el ambiente digital.
- Mantener un marco legal que garantice la protección de datos personales de los usuarios del comercio electrónico. Se reconocen los principios clave de la protección: *i)* Límites en la obtención, *ii)* Voluntad, *iii)* Calidad de los datos, *iv)* Propósito en la recolección, *v)* Limitación en el uso, *vi)* Medidas de seguridad, *vii)* Transparencia, *viii)* Participación individual, *ix)* Responsabilidad.
- Aceptar trámites administrativos mediante el envío de documentos electrónicos y que estos se consideren como el equivalente legal de la versión impresa.
- No prohibir o restringir la transferencia transfronteriza de información.
- Reconocer las amenazas de Ciberseguridad que afectan la fiabilidad del comercio electrónico. Por ello, los Estados miembro se obligan a construir entidades nacionales capaces de responder a incidentes de Ciberseguridad. De esta forma, los Estados reconocen que estas amenazas no se resolverán con la regulación de las amenazas, sino que el combate efectivo, es incentivar a las empresas en la implementación de estándares de Ciberseguridad para proteger la identidad de sus empleados y clientes, en contra de riesgos de Ciberseguridad.
- No solicitará acceso al código fuente, como condición para permitir la importación, distribución, venta o uso del Software en alguno de los territorios de los Estados miembro.
- Fortalecer la política *Open Government Data* como un mecanismo para facilitar el acceso público a información que permita una mejor práctica comercial.

- ***Intellectual Property Rights:***[14] el capítulo 20 del T-MEC pretende fortalecer la protección de los derechos de propiedad intelectual, con la intención de promover la innovación, transferencia y diseminación de tecnológica, para el beneficio mutuo de los creadores y los usuarios del conocimiento tecnológico, en consecuencia, beneficiaría a la sociedad en las condiciones económicas, al permitir un correcto balance entre derechos y obligaciones.

[14] OFFICE OF THE UNITED STATES TRADE REPRESENTANTIVE. *United States-Mexico-Canada Agreement Agreement (USMCA) Chapter 20 Intellectual Property Rights.* Estados Unidos de América, Septiembre de 2018. Executive Office of the President. Resource Center. Visto el 21 de octubre de 2018 a través del vínculo https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/20%20Intellectual%20Property.pdf

- Cada Estado deberá realizar los mejores esfuerzos para incorporar el registro de marcas no tradicionales, así como marcas colectivas y de certificación a la legislación local.
- En afán de generar una relación de Transparencia entre los ciudadanos y los Estados miembro, cada gobierno deberá:

  » **Contar con un sistema electróuico para la solicitud y renovación de registros de Marcas**
  » **Publicar los requisitos para solicitud de registros de forma electrónica y, en su caso, publicar la base de datos sobre solicitndes de registro y marcas efectivamente registradas.**

- Cada Estado deberá contar con **un sistema para el control de nombres de dominio y generar un proceso para la resolución de conflictos.** Sobre el particular, el T-MEC recoge el principio de acreditación de la "mala fe" del contrario, como un elemento indispensable para la solicitud.
- Los Estados miembros permitirán el bloqueo tecnológico de las obras, siempre que se acredite o existan elementos razonables sobre la probabilidad de violación de las mismas. En términos generales las ***Technological Protection Measures (TPM's)*** se consideran ilegales, sin embargo, los gobiernos reconocen la necesidad de establecer excepciones a la regla, en los casos de:

  » Necesidad para evitar la aplicación de ingeniería en reversa que se pudiere obtener de un programa de cómputo.
  » Requerir la inclusión de un componente con la intención de prevenir el acceso a contenido inapropiado para menores de edad.
  » El uso de tecnología, dispositivos o componentes que, en el curso normal de su operación, controle el acceso a obras protegidas, interpretaciones, fonogramas, derechos conexos o derechos relacionados con derechos de autor: ***Effective Techonological Measure.***

- Cada Estado tipificará como delito, la conducta de crear, modificar, exportar, importar, vender, o distribuir un dispositivo o sistema, tangible o intangible, que tenga por objetivo decodificar una señal ***encriptada***, de cable o satelital, sin la autorización del titular. Las penas también se aplicarían respecto de aquéllos que reciban dicha señal o bien, que la distribuyan de forma ilegal.
- Cada Estado regulará los mecanismos de reparación para los titulares de derechos por violaciones y promulgará por el establecimiento de puertos seguros (***Safe Harbors***) por lo que refiere a la prestación de los servicios en Internet:

- Se establecerá el marco legal adecuado para incentivar que los Proveedores de Servicio de Internet (***Internet Services Providers)*** cooperen con los titulares de derechos de autor, para la detección de almacenamiento o transmisión no autorizada de obras protegidas.
- Eliminar condiciones legales que generen responsabilidad monetaria a cargo de los Proveedores de Servicio de Internet, que sean consecuencia de infracciones que estos no controlen.

Sobre el último análisis, es importante señalar al lector, que el presente Tratado aún se encuentra en negociación y pendiente de ratificación por los Estados que podrían ser miembros del mismo.

VI
CAPÍTULO

Programas de cómputo y sistemas de licenciamiento

En el universo de creaciones que brinda la cibersociedad, se erige una figura en lo particular, que permitió la consolidación de grandes empresas millonarias a nivel internacional. El ejemplo de Microsoft, líder mundial de creación de programas de cómputo, con ingresos aproximados en los $77 550 millones de dólares tan sólo en el 2013, debió esa impactante cantidad al margen del 84% sobre sus ventas totales; Oracle ingresó $29.7 mil millones de dólares e IBM la cantidad de $29.1 mil millones de dólares; esto sólo en el mercado de venta de software sin contemplar ganancias por mercadeo o hardware; a esta lista se podrían sumar especialistas como Hewlett-Packard, EMC2 y SAP —el gigante del software multinacional con sede en Alemania—, todos ellos que superaron la cantidad de 6 mil millones de dólares. Su crecimiento económico no sólo ocurre en su campo, sino que a nivel internacional ha permitido que su poder político y monetario los refleje dentro de las empresas más poderosas del mundo; en ese mismo año, según la lista *Forbes*, coloca a General Electric (lugar cuatro de la lista global), Apple (lugar 15), Samsung Electronics (Número 20), IBM (Lugar 34), Microsoft (Lugar 41) y Oracle (en el lugar 112);[1] este

[1] *FORBES México*. "Las 20 empresas tecnológicas más importantes del mundo". Forbes Staff. Portada. Agosto 18 de 2013. Puede consultar el listado completo en el vínculo https://www.forbes.com.mx/las-20-empresas-tecnologicas-mas-importantes-del-mundo/ visto el 14 de noviembre de 2017.

listado merece grandes actualizaciones, sin embargo, destaca la premisa fundamental del presente capítulo, pues determina la cantidad de bienes digitales que circulan en la red, gracias a las únicas y novedosas formas jurídicas que existen hoy en día.

En gran medida, las empresas que he invocado al presente texto deben su fortaleza al sistema de licenciamiento no exclusivo y temporal que otorgan a los usuarios de sus plataformas, no sólo para uso doméstico, sino comercial. Empero, el ciberespacio se ha consagrado como el rey de la creación de nuevos modelos de negocio —y con ello nuevos esquemas jurídicos— que obliga a los empresarios a adaptar sus modelos en persecución de mantener las ganancias millonarias que los colocan en la cúspide comercial.[2]

El presente capítulo tendrá por objeto detallar a los programas de cómputo desde la semántica[3] y cómo es que se componen los negocios jurídicos detrás de los mismos; posteriormente analizaremos la base jurídica internacional (Tratado de la OMPI sobre Derechos de Autor) y nacional (en apego a lo prescrito por la Ley Federal del Derecho de Autor); finalmente, aterrizaremos estos elementos en los tipos más usuales de transmisión de derechos patrimoniales digitales, es decir, código abierto, el polémico software libre (en específico, sobre el proyecto GNU) y *Creative Commons*.

Debemos entender por *programa de cómputo/ordenador* o *software* a la información en forma de programas informáticos que permiten a una computadora encargarse de ciertas funciones.[4] A su vez, el Glosario de la OMPI define el programa de ordenador (computación) como "un conjunto de instrucciones que, cuando se incorpora a un soporte legible por máquina, puede hacer que una máquina con capacidad para el tratamiento de la información indique, realice o consiga una función, una tarea o resultados determinados".

Al conjunto de programas que permiten la debida integración de los mismos dentro de un ordenador, se le conoce como Sistema Operativo. De forma regular, el sistema operativo se compone de software que pertenece al mismo desarrollador o bien a terceros autorizados a crear programas sobre su misma base y lenguaje. El lenguaje es un conjunto de vocablos, sintaxis y reglas semánticas que definen los programas de computador; el texto que se redacta con un lenguaje en particular, que una vez finalizado incluye las instrucciones que deberá realizar la computadora, según la sintaxis del lenguaje que se ocupó.

---

[2] Sugiero la lectura del texto *Cómo negociar licencias tecnológicas*, publicado por la Organización Mundial de la Propiedad Intelectual con el número 9035, a través del vínculo http://www.wipo.int/export/sites/www/ip-development/es/strategies/pdf/publication_903.pdf visto el 16 de noviembre de 2017.

[3] Propongo un estudio semántico, debido a lo complejo e infructífero que podría resultar un estudio técnico especializado sobre la materia; ya que el mismo nos alejaría del objetivo central del presente capítulo.

[4] BLACK'S Law Dictionary. *Software*. http://thelawdictionary.org/software/

El texto no siempre resulta legible para una persona de conocimientos mínimos sobre computación, pero resulta relevante que sea comprensible por los programadores y los equipos de cómputo para llegar a los fines deseados. Es decir, el software se compone de un código fuente que se programa con base en un lenguaje que permite a la computadora operar bajo un conjunto de instrucciones;[5] en tanto que un sistema operativo puede incluir distintos códigos fuente,[6] siempre opera sobre uno propio que organiza el funcionamiento de todo el equipo de cómputo.

El presidente del Departamento de Propiedad Intelectual y Tecnología de la Información del despacho Leonard, Street and Deinard (Minneápolis, Minnesota), Stephen Davidson, se refiere al código como un elemento necesario para que el computador pueda utilizar realmente un programa, de tal suerte, éste lo tiene que traducir del código fuente a un idioma informático que el computador pueda entender y ejecutar. Ese proceso de traducción se llama "compilación". A su vez, define al código fuente como el texto que los programadores introducen y modifican en el computador para producir programas que funcionen[7].

[5] CASAÑAS, María Elena. ¿Qué es el software libre? CASANAS. COM. AR. Puede consultar el texto íntegro a través del vínculo http://www.casanas.com.ar/attachments/Que_es_-_A_-_Conc_tecnicos.pdf Visto el 14 de noviembre de 2017.

[6] En términos de la empresa *SoftDoIt*, la programación es el área de la informática que se dedica a la creación de programas y también a la creación de su código fuente. Define a éste último de la siguiente maneras: "*El término código tiene diferentes usos y acepciones, la que nos ocupa en términos de software viene a decir que puede tratarse de una combinación de símbolos que cuenta con un cierto valor dentro de un sistema ya establecido con una representación de caracteres alfanuméricos que facilita la comunicación entre distintos dispositivos digitales. Este mismo término se usa para hacer referencia a otros elementos del software, como por ejemplo, el código fuente de una página web que está escrito en lenguaje de marcado HTML o en Javascript o en otros lenguajes de programación web y que serán ejecutados por el navegador para visualizar la página cuando es visitada.*

Un editor de texto creado específicamente para editar el código fuente de programas informáticos es el encargado de diseñar este código. Puede ser una aplicación independiente o bien, estar incluido en el entorno de desarrollo integrado de un programa. El resaltado de sintaxis, el autocompletar y pareo de llaves son algunas de las características diseñadas por los editores de código fuente para simplificar y acelerar la escritura. También proveen un modo certero de ejecutar un compilador, un intérprete, un depurador o cualquier otro programa que sea importante en el desarrollo de software.

Algunos editores de texto de código fuente verifican la sintaxis a medida que el programador escribe, avisando en el acto de los posibles errores sintácticos que puedan surgir. Otros editores de texto de código fuente comprimen el código, convirtiendo las palabras clave en tokens o componentes léxicos de un solo byte eliminando espacios en blanco y transformando los números a una combinación binaria. Algunos de los editores más conocidos son Adobe dreamweaver, Code Crusader IDE, Emacs entre otros muchos." SOFTDOIT. ¿Qué es el código fuente? Puede consultar el texto íntegro, a través del vínculo https://www.softwaredoit.es/definicion/definicion-codigo-fuente.html visto el 15 de noviembre de 2017

[7] DAVIDSON, Stephen J. *Estudio sobre los programas informáticos de código abierto para empresarios y abogados* Organización Mundial de Propiedad Intelectual. Estados Unidos, 2004. Puede consultar el texto íntegro, a través del vínculo http://www.wipo.int/sme/es/documents/opensource_software_primer.htm

El negocio detrás del software debe su riqueza a la posibilidad de explotar al máximo el potencial de los procesadores de nuestros equipos de cómputo, de esta forma, al adquirir hardware solemos poseer una versión simple del mismo, con un cerebro y procesador mínimo que permiten un adecuado funcionamiento, empero, el sacar el máximo provecho de uua computadora implica aumentar su capacidad y, en algunas casos, adquirir herramientas, virtuales, costosas que se integran gracias a las paqueterías del desarrollador, conjunto de software, aplicaciones (*apps* para el caso de los equipos móviles) o bien, dejar en manos de expertos el funcionamiento de nuestros equipos.

Este negocio ha sufrido diversas variaciones a lo largo de su historia desde el año 1940, cuando surgieron los primeros programas de cómputo, a un lado de los primeros ordenadores; fue hasta la década de 1980 cuando las computadoras llegaron a manos de las empresas y para finales de ésta, surgió la posibilidad de tener un ordenador de este tipo para uso doméstico. En este punto histórico, el poder económico del software creció y se transformó en un bien intangible de consumo básico para los seres humanos.

Con el progreso de la tecnología, paralelamente se lleva la carrera de mejores programas de cómputo que permitan mejores experiencias en la vida *online* e inclusive en la *off line*; vivencias que resultan costosas y fuera de cualquier canasta básica. Al principio del negocio jurídico que nos ocupa, se resolvió la transmisión de programas de cómputo a través de la venta del soporte material y otorgando la licencia de uso no exclusivo respecto del código fuente, es decir, se celebraba una operación tradicional de compra venta respecto del *Compact Disc* que contenía el código y se brindaba la facultad de uso del programa para uno o más ordenadores, según el tipo de licencia.

En caso que el usuario pretendiera vender el CD que contenía el lenguaje de programación (software) bajo la premisa de pretender transmitir la licencia, configuraba la hipótesis de fraude, pues éste enajenó el soporte electrónico sobre el que se fijó el programa de cómputo, no así transmitió los derechos de uso que se le otorgaron anteriormente en forma jurídica de licencia; máxime que la misma se brinda de forma no exclusiva y sin posibilidades de sub-licenciamiento a favor de terceros.

En caso que el propietario del soporte electrónico pretendiera obtener ganancia con las licencias disponibles, éste debía permitir ocupar alguna de las legamente adquiridas o, en su caso, recurrir a medidas ilegales en perjuicio de los intereses del desarrollador y del interés público que protege las creaciones susceptibles de regulación autoral; en el último escenario, no sólo el titular de la licencia cometía un delito, sino el tercero adquirente de buena o mala fe.

La separación *software* y *hardware* encontró una respuesta comercial razonable para futuras generaciones, por ejemplo, la compañía *Dell* celebró un contrato de coalición comercial con la empresa *Microsoft* para que todos los equipos que produjeran tuvieran instalada la paquetería *Windows Profesional, Windows XP o Windows*

Profesional X64 Edition; esto implicó para el consumidor la adquisición de un ordenador fabricado por la primer compañía (operación de compra-venta), y la obtención de una licencia sobre la activación del producto únicamente en la computadora obtenida y de forma puntual, indicaba que ésta no era objeto de venta, por lo que dictaba que únicamente podría transmitir el software a un tercero si éste lo hacía junto con el dispositivo que tiene la licencia incluida, sin posibilidad de conservar copia del software, incluida la autorizada por ley para seguridad. De forma textual, las condiciones bajo las cuales se adquirió el equipo de cómputo y su programa, son las siguientes:

> **Términos de Licencia del Software de Microsoft** [8]
> [...]
>
> 8. ALCANCE DE LA LICENCIA. El software se cede bajo licencia y no es objeto de venta. El presente contrato sólo le otorga algunos derechos de uso del software. El fabricante o instalador y Microsoft se reservan todos los demás derechos. A menos que la legislación aplicable le otorgue más derechos a pesar de esta limitación, usted sólo podrá utilizar el software tal como lo autoriza expresamente el presente contrato... Usted no podrá: eludir las limitaciones técnicas del software, · utilizar técnicas de ingeniería inversa, descompilar o desensamblar el software, excepto y únicamente en la medida en que ello esté expresamente permitido por la ley a pesar de la presente limitación · usar componentes del software para ejecutar aplicaciones que no se ejecuten en el software; · hacer más copias del software de las que especifica este contrato o permite la legislación vigente a pesar de esta limitación, · hacer público el software para que otros lo copien, · alquilar, arrendar o ceder el software, o · utilizar el software para prestar servicios de alojamiento de software comercial.
>
> ...10. COPIA DE SEGURIDAD. Usted puede realizar una única copia de seguridad del soporte del software. Usted sólo podrá utilizarla para volver a instalar el software.[9]

[8] DELL. *Términos de licencia del software de Microsoft. Windows Vista Home Basic, Windoes Vista Home Premium, Windows Vista Ultimate.* Puede consultar las políticas íntegras, a través del vínculo http://www.dell.com/downloads/global/products/vostrodt/es/UseTerms_OEM_Vista_HomeBasicHomePremiumUltimate.pdf visto el 15 de noviembre de 2017.

[9] Este apartado atiende a la propia y especial naturaleza del bien intangible que nos ocupa. A saber, *The Digital Millennium, Copyright Act of 1998* determina la protección tecnológica y manejo de Copyright de sistemas, la cual detalla la sección 1201 (a) (1) (B)- (E) de la Copyright Act, y específica excepciones a reproducciones no autorizadas, entre ellas, las derivadas de un uso por protección ante perdida únicamente en caso de mantenimiento o reparación, siempre que no se realice ingeniera en reversa; a saber la *DMCA* prescribe: Reverse engineering (section 1201(f)). This exception permits circumvention, and the development of technological means for such circumvention, by a person who has lawfully obtained a right to use a copy of a computer program for the sole purpose of identifying and analyzing elements of the program

> ...12. SOFTWARE NO PARA REVENTA ("Not for Resale" o "NFR"). Usted no podrá vender el software identificado como "NPR", "NFR" o "No Para Reventa".
>
> ...15. TRANSFERENCIA A UN TERCERO. Sólo puede transferir el software directamente a un tercero junto con el dispositivo con licencia. No podrá conservar ninguna copia del software ni ninguna versión anterior. Antes de la transferencia permitida, el tercero deberá aceptar la aplicación de los términos del presente contrato a la transferencia y uso del software. La transferencia debe incluir la etiqueta de Certificado de Autenticidad.

Estas condiciones dejan clara la postura de dos grandes colosos de la tecnología, mismas que se reprodujeron por otros operadores y hasta hoy en día, permiten comprender gran parte de la operación comercial que ocurre entre el usuario y las desarrolladoras. Es decir, por un lado celebran una operación de enajenación respecto al hardware, en tanto que obtienen un licenciamiento puro sobre la titularidad del Programa de Cómputo.

No deseo obviar que la adquisición de la licencia únicamente ocurre respecto del Código Fuente que compone la totalidad del Programa de cómputo, ya que éste incluye otros elementos de propiedad intelectual que no serán abordados en el presente texto, tales como los elementos marcarios, avisos comerciales, características comerciales y en su caso, patentabilidad, propiedad industrial, cuya titularidad se reserva exclusivamente para el desarrollador. A destacar, las licencias que se otorgan como regla general incluyen las siguientes características:

1. Ilimitadas: a pesar de las restricciones jurídicas que pudieren existir en materia de derechos de autor, tanto en sistemas subjetivos como objetivos, la excepción a la regla ocurre en el universo de programas de cómputo, lo cual permite a los desarrolladores brindar licencias de uso ilimitados a los usuarios. La premisa comercial al respecto, parte de la idea que el código fuente cuenta con una **obsolescencia programada**[10] por lo que refiere a los dispositivos físicos

necessary to achieve interoperability with other programs, to the extent that such acts are permitted under copyright law. US COPYRRIGHT OFFICE SUMMARY. *The Digital Millenium Copyright Act of 1998.* Diciembre de 1998. Puede consultar el texto completo del Acta, a través del vínculo https://www.copyright.gov/legislation/dmca.pdf visto el 15 de noviembre de 2017.

[10] En propiedad industrial y derechos de consumidores, el concepto de obsolescencia programada es uno de los enemigos comerciales primordiales en perjuicio de los usuarios finales, sin embargo, constituye una herramienta comercial que permite a gran parte de los inventores y productores, mantener la circulación del bien creado y que la necesidad de consumo se mantenga; de tal suerte que los productores estiman una vida útil para sus insumos, en tanto que resulten benéficos para la sociedad, pero no ilimitados, en términos de continuar el flujo de consumo. La legislación ecuatoriana califica a la **obsolescencia programada** como "el conjunto de técnicas mediante las cuales un fabricante, importador o distribuidor de bienes, en la creación o a través de la modificación del producto, reduce deliberada

sobre los que se ejecuta, es decir, a pesar de poseer una licencia perpetua sobre un programa de cómputo, ello no implica que éste será útil *ad perpetuam*, sin la debida adquisición de las actualizaciones, parches y mejoras que surjan al respecto, siendo que, en la mayoría de los casos, quedan obsoletos después de cierto lapso.

2. Intransferibles: salvo pacto en contrario, el usuario final se encuentra limitado a la utilización de la licencia sólo para uso personal; en caso que licencias empresariales, se suele delimitar el número de licencias, fijar el tipo y cantidad de equipos de cómputo sobre los que se puede y debe instalar el programa y, en su caso, es el propio desarrollador quién instala el software en los dispositivos contratados, con fines de control y auditoría. Conforme se indicó con anterioridad, ello no impide que el licenciatario transmita la propiedad del soporte físico o electróuico que contiene el programa de cómputo, ya que siguen suerte diferentes y ramas de derecho diversas, sin embargo, la enajenación de un ordenador que contiene la licencia no implica, indudablemente, que se han cedido los derechos de autor adquiridos mediante licenciamiento, tal como se indicó en las condiciones que se reprodujeron anteriormente, dispuestas por Dell y Microsoft. En algunas condiciones comerciales, la transmisión del hardware que contiene la licencia, obliga al licenciatario a eliminar el software antes de la venta del equipo, lo que en muchos casos podría dejar éste inutilizable.
3. No Exclusivas: siempre que el desarrollo del programa de cómputo no se hubiese diseñado bajo la modalidad de obra por encargo, el autor (o la empresa desarrolladora) conservan los derechos patrimoniales suficientes para celebrar la cantidad de operaciones de licenciamiento que crea prudente, sobre la base tecnológica y humana, bajo las cuáles pueda brindar el soporte y mantenimiento respectivo. Es decir, la licencia que se adquiere como usuario final, no implica que otros usuarios no podrían adquirir el programa de cómputo en los mismos términos legales. En el caso de obras por encargo, el

e injustificadamente su duración con objeto de aumentar su tasa de reemplazo" [REPÚBLICA DEL ECUADOR. ASAMBLEA NACIONAL. *Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación*. Publicada el 01 de diciembre de 2016. Puede consultar el texto íntegro a través del vínculo http://www.wipo.int/wipolex/fr/text.jsp?file_id=439750]; por su lado, la "Ley General de los Derechos de las Usuarias y los Usuarios y de las Consumidoras y los Consumidores (sic)" de 4 de diciembre de 2013, del Estado Plurinacional de Bolivia contempla el concepto de ***obsolescencia programada*** como una preocupación de estado que generada necesidades impuestas y comprende la incidencia negativa sobre la sociedad [ASAMBLEA LEGISLATIVA PLURINACIONAL DE BOLIVIA. *Ley General de los Derechos de las Usuarias y los Usuarios y de las Consumidoras y los Consumidores.* Ley número 453 de 4 de diciembre de 2013, publicada por el Presidente Constitucional Evo Morales. Puede consultar el texto íntegro a través del vínculo http://www.wipo.int/edocs/lexdocs/laws/es/bo/bo044es.pdf]; sólo en el caso de la legislación ecuatoriana se determinan sanciones y, en su caso, bloqueos comerciales temporales para los productores que incurran en conductas que atenten contra derechos de usuarios y consumidores.

licenciamiento se suele otorgar de forma exclusiva para evitar consideraciones de competencia desleal y el código fuente pertenece al solicitante, salvo pacto en contrario.

4. Remuneradas: en el sistema subjetivo de protección de derechos de autor, el pago de regalía se consagra como una facultad irrenunciable, en tanto que sistemas que respetan la línea interpretativa del *copyright* consideran esta facultad transigible. Por lo que refiere al licenciamiento puro, se suele comprender que la regalía forma parte integral del monto que se paga al momento de la adquisición del soporte físico o electrónico que contiene el código fuente. Es difícil que el documento o acto jurídico de referencia incluya la distinción o conceptos precisos, sin embargo, para fines fiscales es prudente destacar el concepto de pago: *a)* Adquisición de software, *b)* Licenciamiento de software, o *c)* Licenciamiento de versiones del software [mantenimiento]; ya que suelen tener efectos contables diversos.
5. Soporte y Mantenimiento: por soporte se comprende la obligación del proveedor, prestador o desarrollador a favor del usuario, para obtener asesoría para el debido uso e implementación de la licencia adquirida. Al respecto, éste se suele brindar vía electrónica o telefónica, según el tipo de licencia adquirida; en el caso empresarial, el soporte puede ocurrir de forma presencial y con niveles de servicios claros que permitan medir la efectividad con la que se obtiene la atención del licenciante. A su vez, el mantenimiento implica la actualización del software que se adquiere; salvo casos extraordinarios, éste se pacta de forma general en la adquisición de la licencia y el pago de las versiones ya se incluye dentro del monto erogado por concepto de "regalía"; para licencias empresariales, este mantenimiento podría tener un costo adicional, debido a lo complejo o personalizado que llega a ser el mismo.
6. Código Cerrado: no se permite al acceso, modificación, divulgación no autorizada del lenguaje y sintaxis que conforman el programa de cómputo *a contrariu sensu* de los programas de código abierto que se estudiarán más adelante. En este tipo de licenciamiento, sólo el programador y la empresa desarrolladora conocen el texto original.

A la estructura de licenciamiento que describimos con anterioridad, se le podría considerar un debido ejercicio del *Derecho de Alquiler* a que refiere el artículo 7 del Tratado de la OMPI sobre Derechos de Autor. En tal precepto, se faculta a los autores de programas de ordenador para autorizar el alquiler comercial al público del original o de los ejemplares de sus obras. Este derecho debe seguirse del pago irrenunciable de una regalía tal como se indicó anteriormente, al menos en el caso mexicano. Al respecto, me permito invocar los precedentes emitidos por nuestra Suprema Corte de Justicia a nivel de Jurisprudencia (criterio obligatorio), mismos que de tenor literal dictan:

DERECHO A PERCIBIR REGALÍAS POR LA COMUNICACIÓN O TRANSMISIÓN PÚBLICA DE UNA OBRA, CONTENIDO EN EL ARTÍCULO 26 BIS DE LA LEY FEDERAL DEL DERECHO DE AUTOR. SU CONCEPTO.

Existen dos tipos de derechos dentro de la materia autoral: los morales, que permiten al autor realizar ciertas acciones para conservar el vínculo personal con su obra, y los de contenido económico o patrimoniales (lato sensu), que permiten al autor o al titular derivado obtener recompensas económicas por la utilización de la obra por terceros; asimismo, estos últimos pueden clasificarse en dos subtipos: 1) derechos de explotación o patrimoniales (en estricto sentido), y 2) otros derechos, dentro de los que se encuentran los de simple remuneración, como el de regalías, previsto en el artículo 26 bis de la Ley Federal del Derecho de Autor, el cual constituye un incentivo económico de carácter irrenunciable, garantizado y previsto por el Estado en favor del autor de la obra o su causahabiente, que está constituido por un determinado porcentaje a cargo de quien comunica o transmite públicamente la obra por cualquier medio, de lo cual deriva que tal derecho sea distiuto de las regalías mencionadas en los artículos 8o. y 9o. del Reglamento de la Ley Federal del Derecho de Autor, que se refieren, por ejemplo, a contraprestaciones contractuales que el adquirente del derecho de explotación paga al autor como parte del importe de la transmisión de dicho derecho estipulado en el contrato respectivo.[11]

DERECHO A PERCIBIR REGALÍAS POR LA COMUNICACIÓN O TRANSMISIÓN PÚBLICA DE UNA OBRA POR CUALQUIER MEDIO, CONTENIDO EN EL ARTÍCULO 26 BIS DE LA LEY FEDERAL DEL DERECHO DE AUTOR. ES TRANSMISIBLE A TERCEROS EN VIDA DEL AUTOR.

El citado precepto legal, al establecer que el **derecho** a **percibir** una regalía por la comunicación o transmisión pública de una obra por cualquier medio **es de carácter irrenunciable**, debe interpretarse en el sentido que su autor está imposibilitado para repudiar el ejercicio de tal **derecho** mediante cualquier tipo de acto jurídico que tienda a producir esos efectos, lo que no implica que tenga prohibido trausmitirlo en vida, pues en este último caso ha sido su voluntad ejercerlo y beneficiarse de los frutos derivados de la correspondiente transmisión. De ese modo, el autor, una vez que

[11] Suprema Corte de Justicia de la Nación. *Derecho a Percibir Regalías por la comunicación o transmisión pública de una obra, contenido en el artículo 26 bis de la Ley Federal del Derecho de Autor. Su concepto.* Semanario Judicial de la Federación y su Gaceta. Diciembre de 2007. Tesis P./J. 102/2007, novena época, Jurisprudencia. Puede consultar la misma a través del vínculo https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=derecho%2520a%2520percibir%2520regalias&Dominio=Rubro,Texto&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=7&Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas=6,1,2,50,7&ID=170786&Hit=1&IDs=170786,170785,170622,176157,176479,176476,177991&tipoTesis=&Semanario=0&tabla=&Referencia=&Tema= visto el 15 de noviembre de 2017.

el **derecho** referido ha entrado a formar parte de su patrimonio, está facultado para transmitirlo a través de cualquiera de las formas establecidas legalmente para ello, por un lado, porque el legislador no previó en el artículo 26 bis de la Ley Federal del **Derecho** de Autor que dicho **derecho** sea intransmisible, lo que no podría modificarse vía interpretativa y, por otro, porque los principios que sustentan el **derecho** a la libertad contractual y la autonomía de la voluntad impiden al intérprete suponer que la intransmisibilidad del **derecho** puede beneficiar aún más a los autores, considerando que ello constituye una apreciación subjetiva que corresponde al ámbito de libertad decisoria que compete al autor en cada caso concreto. Por tanto, el autor podrá transmitir en vida a un tercero su **derecho** a **percibir regalías**, siempre que celebre un acto jurídico en el que indubitablemente exprese su voluntad en ese sentido."[12]

[El énfasis es añadido]

VI. 1 Consideraciones Jurídicas

En el año 1996, la Organización Mundial de Propiedad Intelectual determinó que el Convenio de Berna concebido en 1886 —y su enmienda del 28 de septiembre de 1979— resultaba insuficiente para controlar el flujo de creaciones intelectuales, en particular las originales de fijación digital o bien, que dependían de Internet para lograr el ejercicio de los derechos patrimoniales consagrados por las mismas.

Así la Asamblea de miembros determinaron un arreglo particular adoptado en virtud del Convenio de Berna,[13] al que llamaron Tratado de la OMPI sobre Derechos de Autor (WTC por sus siglas en inglés), éste tiene por objeto la protección de: *i)* los programas de computadora, con independencia de su forma o modo de expresión y, *ii)* las compilaciones de datos y otros materiales ("bases de datos"). Finalmente, el 6 de marzo de 2002 entró el vigor el texto del Tratado que nos rige hasta nuestros días.

[12] Suprema Corte de Justicia de la Nación. *Derecho a percibir regalías por la comunicación o transmisión pública de una obra por cualquier medio, contenido en el artículo 26 bis de la ley federal del derecho de autor. Es transmisible a terceros en vida del autor.* Semanario Judicial de la Federación y su Gaceta. Diciembre de 2007. Tesis P./J. 103/2007, novena época, Jurisprudencia. México. Puede consultar el criterio así como la ejecutoria, a través del vínculo https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=derecho%2520a%2520percibir%2520regalias&Dominio=Rubro,Texto&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=7&Epp=20&Desde=-100&Hasta=-100&Index=0&InstanciasSeleccionadas=6,1,2,50,7&ID=170785&Hit=2&IDs=170786,170785,170622,176157,176479,176476,177991&tipoTesis=&Semanario=0&tabla=&Referencia=&Tema= visto el 15 de noviembre de 2017

[13] El artículo 20 del Convenio de Berna, permite el Arreglo entre distintos países contratantes, que tengan como base metódica dicho Convenio.

Éste brinda protección a los programas de ordenador y compilaciones de datos, en sus artículos cuarto y quinto, respectivamente:

> Artículo 4. Programas de ordenador
> Los programas de ordeuador están protegidos como obras literarias en el marco de lo dispuesto en el Artículo 2 del Convenio de Berna. Dicha protección se aplica a los programas de ordenador, cualquiera que sea su modo o forma de expresión.
>
> Artículo 5 Compilaciones de datos (bases de datos)
> Las compilaciones de datos o de otros materiales, en cualqnier forma, que por razones de la selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, están protegidas como tales. Esa protección no abarca los datos o materiales en sí mismos y se entiende sin perjuicio de cualquier derecho de autor que subsista respecto de los datos o materiales contenidos en la compilación.

A saber de la OMPI, si definimos el *software* como un conjunto de instrucciones de computadora que producen un resultado determinado, estas se expresan inicialmente en código fuente, es decir, líneas de instrucciones en lenguaje de computadora. Puesto que el código fuente se expresa de forma escrita, resulta lógico pensar que el software puede ser protegido por el derecho de autor como obra literaria. Así, por ejemplo, el artículo 4 del Tratado de la OMPI sobre Derecho de Autor (WCT), el artículo 10 del Acuerdo sobre los ADPIC de la Organización Mundial del Comercio y el artículo 1 de la Directiva (91/250/CEE) del Consejo Europeo sobre la protección jurídica de programas de ordenador equiparan el software con las obras literarias, protegidas por el derecho de autor.[14]

En ese mismo tenor, el Acuerdo 114 expedido por el Secretario de Educación Pública el 8 de octubre de 1984 en el *Diario Oficial de la Federación*, reconoce que los programas de computación constituyen obras producidas por autores en términos de la Ley Federal del Derecho de Autor de 1956. En consecuencia de lo anterior, a partir del 17 de julio de 1991, se publicó la reforma a dicha Ley, que no sólo permitía el registro de tales obras ante el Instituto Nacional de Derecho de Autor, sino que fijaba un apartado legal determinado para los programas de cómputo, la cual de tenor literal prescribe:

Capítulo IV De los Programas de Computación y las Bases de Datos

[14] GUADAMUZ GONZÁLEZ, Andrés. OMPI. "Propiedad Intelectual y Software". *Revista de la OMPI*. Diciembre de 2008. Puede consultar el texto íntegro a través del vínculo http://www.wipo.int/wipo_magazine/es/2008/06/article_0006.html visto el 15 de noviembre de 2017

Artículo 101.- Se entiende por programa de computación la expresión original en cualquier forma, lenguaje o código, de un conjunto de instrucciones que, con una secuencia, estructura y organización determinada, tiene como propósito que una computadora o dispositivo realice una tarea o función específica.

Artículo 102.- Los programas de computación se protegen en los mismos términos que las obras literarias. Dicha protección se extiende tanto a los programas operativos como a los programas aplicativos, ya sea en forma de código fuente o de código objeto. Se exceptúan aquellos programas de cómputo que tengan por objeto causar efectos nocivos a otros programas o equipos.

[...]

Artículo 105.- El usuario legítimo de un programa de computación podrá realizar el número de copias que le autorice la licencia concedida por el titular de los derechos de autor, o una sola copia de dicho programa siempre y cuando:

I. Sea indispeusable para la utilización del programa, o
II. Sea destinada exclusivamente como resguardo para sustituir la copia legítimamente adquirida, cuando ésta no pueda utilizarse por daño o pérdida. La copia de respaldo deberá ser destruida cuando cese el derecho del usuario para utilizar el programa de computación.

[...]

Artículo 107.- Las bases de datos o de otros materiales legibles por medio de máquinas o en otra forma, que por razones de selección y disposición de su contenido constituyan creaciones intelectuales, quedarán protegidas como compilaciones. Dicha protección no se extenderá a los datos y materiales en sí mismos.

Artículo 108.- Las bases de datos que no sean originales quedan, sin embargo, protegidas en su uso exclusivo por quien las haya elaborado, durante un lapso de 5 años.

[...][15]

Dichos preceptos en materia de derechos de autor, fijan las condiciones jurídicas que servirán para la comprensión de los programas de cómputo, siendo la más aproximada la figura autoral de "obras literarias". Sin embargo, algunos estudiosos de la materia consideran que no es prudente colocar a los programas de cómputo dentro de esta categoría por su naturaleza tan diversa y única, adicionalmente, consideran que un software incluye más elementos de protección que sólo el Código Fuente; esto es, no basta proteger el código objeto, sino que existen algunos elementos marcarios, de secreto industrial y, en su caso patentables que pierden el foco de atención jurídica si limitamos el estudio del *software* al universo de derechos de autor.

[15] CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. *Ley Federal del Derecho de Autor.* Última reforma del 13 de enero de 2016. Publicada el 24 de diciembre de 1996. Visto el 15 de noviembre de 2017 a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/122_130116.pdf

Es decir, está bien sentado que el código fuente, o el elemento literario y textual del software no puede patentarse, pero si el software produce algún tipo de efecto en el mismo sentido en que lo hace una invención, deberá alcanzar la protección que se brinda en propiedad industrial según el cuerpo normativo aplicable.

Los precedentes más claros al respecto, se encuentran en países como Australia, Brasil, India y Japón, que respetan una apertura legislativa a favor de la patentabilidad de algunos programas de cómputo, siempre que sus características lo destaquen del resto, por lo que refiere a su aplicación y mejoramiento de la técnica informática; a su vez, la Oficina Europea de Patentes ha concedido un gran número de patentes a invenciones aplicadas por computadora; según algunas estimaciones, hasta 2003 se habían concedido 30 000 patentes. Solamente en 2007, la Oficina Europea de Patentes concedió 8 981 patentes correspondientes a la clase "cómputo".[16]

Esta corriente parecería cobrar fuerza entre los estudiosos de la materia, tal como lo sugiere el Doctor Julio Téllez en su obra "La Protección Jurídica de los Programas de Computación", en la que reconoce que una fórmula híbrida de protección podría resultar más idónea, derivado de la amalgama de disposiciones emanadas del derecho patentario y autoral;[17] resultado de la misma, la Organización Mundial de la Propiedad Intelectual propuso (1971) el Sistema Internacional de depósito y registro de programas, lo que culminó con la publicación de dichas disposiciones en el año 1978, a través del cual se permitiría a los países contratantes y sus autores/creadores, el registro de programas de cómputo que no contengan secretos industriales y que estos sean de acceso directo al público, para evitar posibles infracciones. Eventualmente el sistema propuesto fracasaría, no sólo por lo complejo del mismo, sino por la renuencia de los países en adoptar un sistema híbrido de protección, contra sistemas autorales y de derecho patentario, particularizados.

Conforme las anteriores consideraciones, es prudente indicar al lector que la creación de un programa de cómputo y la titularidad de sus derechos corresponderá primigeniamente a las personas físicas; siempre que estemos sobre la base jurídica de un sistema que respete la protección *subjetiva autoral*, es decir, los derechos patrimoniales sobre cualquier programa de cómputo pertenecerán a su autor, hasta la celebración del acuerdo respectivo o, en su caso, la existencia de una relación laboral con la empresa desarrolladora que invite a una figura implícita de cesión de derechos de explotación.

[16] GUADAMUZ GONZÁLEZ, Andrés. OMPI. "Propiedad Intelectual y Software". *Revista de la OMPI*. Diciembre de 2008. Puede consultar el texto íntegro a través del vínculo http://www.wipo.int/wipo_magazine/es/2008/06/article_0006.html visto el 15 de noviembre de 2017

[17] TÉLLEZ, Julio. *La protección jurídica de los programas de cómputo*. Universidad Nacional Autónoma de México. México, 1989. Segunda edición. Puede consultar el texto íntegro, a través del vínculo https://biblio.juridicas.unam.mx/bjv/detalle-libro/871-la-proteccion-juridica-de-los-programas-de-computacion-2a-ed visto el 24 de noviembre de 2017 y disponible en la biblioteca jurídica virtual de la UNAM (México).

La regla general para la cesión de este tipo de derechos, encuentra su forma jurídica en el licenciamiento, tanto en el sistema *objetivo* como en el *subjetivo,* es un formulario legal y autorizado para la celebración de licencias onerosas y temporales, sin embargo, es recurrente que el modelo comercial que se siga implique licenciamiento ilimitado e intransferible, siendo éste el único caso de excepción a la regla general de la Ley Federal de Derecho de Autor (México), la cual consiste en fijar como plazo máximo legal el de 15 años para la cesión de cualquier derecho patrimonial. Estas consideraciones cambiarán si estamos en presencia del sistema *copyright* y de ser procedente, cualquier trámite de patentabilidad.

VI. 2 Código Abierto/ Open Source

En palabras de Stephen Davidson, los programas informáticos de código abierto son parte del ecosistema de los programas que ofrece a los programadores y usuarios una forma alternativa de desarrollador y distribuir sus creaciones. A saber del abogado que cito, se distingue al programa de código abierto de otras posibilidades de acceso como lo pueden ser programas informáticos del dominio público, programas de libre distribución y compartidos, así como el que se estudió en la primera parte del presente capítulo: programas informáticos comerciales y privados; inclusive se distingue al *open* source de la posibilidad de adquirir programa que aún no está disponible en el mercado pero de los que se habla (*vaporware*).[18]

Sin embargo, me parece que la ambigüedad con la que el experto de la OMPI define a este tipo de mecanismo de distribución dirige al usuario a creer que es exactamente lo mismo "código abierto/ *open source*" y "software libre/ *free software*", cuando sólo son parecidos en lo accidental, pero no lo son en lo fundamental. Un programa informático de código abierto permite a los usuarios conocer el lenguaje de programación y texto utilizado para lograr que un ordenador ejecute tales instrucciones; esto permite a programadores y usuarios conocer el elemento fundamental de protección en materia de derechos de autor –lo que hasta ahora los Tratados Internaciones y Legislaciones locales consideran "obra literaria"-, sin embargo, ello no implica que el acceso a tal elemento medular de protección será gratuito, siendo que ésta última condición es imperativa para la filosofía que sigue el software libre.

Como referiré más adelante, la adquisición de un software libre no necesariamente implica el acceso a las entrañas de la programación, su código, pero si su

[18] DAVIDSON, Stephen J. *Estudio sobre los programas informáticos de código abierto para empresarios y abogados* Organización Mundial de Propiedad Intelectual. Estados Unidos, 2004. Puede consultar el texto íntegro, a través del vínculo http://www.wipo.int/sme/es/documents/opensource_software_primer.htm

gratuidad, en tanto que la adquisición del licenciamiento de un código abierto puede ser oneroso o gratuito y, permitir o no modificaciones a la obra. Los programas de cómputo denominados *open source* sólo garantizan el acceso al código fuente como único requisito para el cumplimiento de sus fines que se resumen en lograr que el mundo empresarial se interese por los programas libres, en lugar de las soluciones privativas, con base en poner un mayor énfasis en la accesibilidad del código fuente y evitando otros elementos menos pragmáticos de tipo filosófico y moral.

En términos generales, el movimiento de código abierto surge como una ramificación al universo de software libre *(free software)*, en el entendimiento que la flexibilización absoluta y la ruptura de diversas reglas fundamentales para la protección en materia de propiedad intelectual, no eran aceptadas por los empresarios y sus compañías desarrolladoras. En un principio, el movimiento en comento siguió la filosofía de Stallman, sin embargo, en el año 1998 encontró una corriente propia y cuatro de sus defensores: John 'Maddog' Hall, Larry Augustin, Eric S. Raymond y Bruce Perens fundaron la Open Source Initiative (OSI). En palabras del propio Robert Stallman, entiende al *open source* como:

> [...] una «campaña de marketing para el software libre», con el objetivo de atraer a los ejecutivos de las empresas enfatizando los beneficios prácticos sin mencionar conceptos de lo que es correcto e incorrecto —y que quizá los empresarios no deseaban oír.
>
> El código abierto es una metodología de programación, el software libre es un movimiento social. Para el movimiento del software libre, el software libre es un imperativo ético, respeto esencial por la libertad de los usuarios. En cambio la filosofía del código abierto plantea las cuestiones en términos de cómo «mejorar» el software, en sentido meramente práctico. Sostiene que el software privativo no es una solución óptima para los problemas prácticos que hay que resolver. En la mayoría de los casos, cuando se discute sobre «código abierto» no se toma en consideración el bien y el mal sino únicamente la popularidad y el éxito.[19]

Hasta este punto, parece un debate de moralidad la diferencia entre ambos conceptos, sin embargo, los efectos jurídicos entre ambos constituyen el punto medular de nuestro estudio. Antes de pronunciarme al respecto, invocaré las condiciones que la *OSI* delimita para considerar que un software es *open source:*

[19] STALLMAN, Richard. *Por qué el código abierto pierde de vista lo esencial del software libre.* El sistema operativo GNU. Patrocinado por Free Software Foundation. Última actualización 11 de octubre de 2017. Visto el 16 de noviembre a través del vínculo https://www.gnu.org/philosophy/open-source-misses-the-point.es.html El texto original en inglés se intitula *Why Open Source misses the point of Free Software.*

Definición de Código Abierto

Introducción
El código abierto no sólo significa acceso al código fuente. Los términos de distribución del software de código abierto deben cumplir con los siguientes criterios:

1. Redistribución gratuita
La licencia no debe restringir a ninguna parte de vender o regalar el software como un componente de una distribución agregada de software que contiene programas de varias fuentes diferentes. La licencia no requerirá pago de regalía u otra tarifa por tal venta.[20]

2. Código fuente
El programa debe incluir el código fuente y debe permitir la distribución en el código fuente y en el formulario compilado. Cuando alguna forma de producto no se distribuye con el código fuente, debe haber un medio bien publicitado para obtener el código fuente por un costo razonable no superior al de reproducción, preferiblemente descargando a través de Internet sin cargo. **El código fuente debe ser la forma preferida en que un programador modificará el programa**. Código fuente deliberadamente ofuscado no está permitido. No se permiten formularios intermedios, como la salida de un preprocesador o un traductor.

3. Trabajos derivados
La licencia debe permitir modificaciones y trabajos derivados, y debe permitir que se distribuyan bajo los mismos términos que la licencia del software original.

4. Integridad del código fuente del autor
La licencia puede restringir la distribución del código fuente en forma modificada sólo si la licencia permite la distribución de "archivos de parche" con el código fuente con el fin de modificar el programa en tiempo de compilación. La licencia debe permitir explícitamente la distribución de software creado a partir de código fuente, modificado. La licencia puede requerir que las obras derivadas lleven un nombre o número de versión diferente del software original.

5. No discriminación contra personas o grupos
La licencia no debe discriminar a ninguna persona o grupo de personas.

[20] Es importante que el lector no confunda esta condición con la ausencia total de pago de regalía, ya que esta excepción, únicamente resulta aplicable por concepto de la segunda venta, en tanto que la primera operación respeta la obligatoriedad de pago de regalías del sistema subjetivo de protección de derechos de autor.

6. No discriminación contra campos de esfuerzo
La licencia no debe restringir a nadie el uso del programa en un campo específico de esfuerzo. Por ejemplo, puede no restringir el uso del programa en un negocio, o ser utilizado para investigación genética.

7. Distribución de la licencia
Los derechos adjuntos al programa deben aplicarse a todos aquéllos a los que se redistribuye el programa sin la necesidad de la ejecución de una licencia adicional por esas partes.

8. La licencia no debe ser específica de un producto
Los derechos adjuntos al programa no deben depender de que el programa sea parte de una distribución de software en particular. Si el programa se extrae de esa distribución y se usa o distribuye dentro de los términos de la licencia del programa, todas las partes a quienes se redistribuye el programa deben tener los mismos derechos que los otorgados junto con la distribución de software original.

9. La licencia no debe restringir otro software
La licencia no debe imponer restricciones sobre otro software que se distribuye junto con el software licenciado. Por ejemplo, la licencia no debe insistir en que todos los demás programas distribuidos en el mismo medio deben ser software de código abierto.

10. La licencia debe ser neutra desde el punto de vista tecnológico
Ninguna disposición de la licencia puede basarse en ninguna tecnología individual o estilo de interfaz.[21]
[El énfasis es añadido]

En términos jurídicos, podría resultar crítica la postura que adopta la OSI bajo su sistema de licenciamiento, sin embargo, la flexibilización que proponen respeta condiciones fundamentales para los sistemas más proteccionistas en materia de derechos de autor, verbigracia: *i)* Obliga al pago de una primera regalía, y *ii)* Permite creación de obras derivadas, siempre que se señale la obra original y su autor. Tales reglas precisan que el licenciamiento de un software bajo esta modalidad debe permitir el acceso al código fuente —código abierto— sin limitación alguna o alteración fraudulenta en perjuicio del usuario.

Esta mecánica invita a los usuarios y probables inversionistas a conocer la complejidad del software que han adquirido, que pretenderán modificar y, en algunos

[21] Traducción LIMÓN, Jaime. Puede consultar el texto original en inglés a través de OPEN SOURCE INIATIVE. *The Open Source Definition*. 22 de marzo de 2007. https://opensource.org/osd visto el 16 de noviembre de 2017.

casos, la compañía autora del programa de cómputo en que invertirán, en afán de lograr mejores resultados colaborativos. De las reglas expuestas, es inconcuso que éstas no coinciden con la filosofía del software libre, al menos por lo que hace a la obtención de regalías y la intención mercadológica que existe detrás de la corriente *open source*; empero, se destacada que ninguna de ellas parece atentar *a prima facie* contra derechos de autor consagrados, sobre todo en la esfera de los derechos morales (paternidad, integridad, divulgación), aunque no existen reglas particulares en el derecho positivo que nos permitan mayores referencias jurídicas, al respecto.

VI. 3 Software Libre

A diferencia de lo expuesto por Stephen Davidson, no se puede considerar al código abierto como variante del software libre, ni mucho menos al tipo de licenciamiento *i)* Licencia pública general (GPL) y *ii)* la Licencia pública general reducida (LGPL) —ambas propuestas por la Free Software Foundation— un resultado invariable del acceso abierto al código, ya que tal como se dejó claro en líneas atrás, el software libre / *Free Software* tiene como filosofía esencial la ausencia de pago de regalías a favor de cualquier programador (autor), a su vez, el acceso al código fuente no es una condición *sine qua non* para la celebración de este tipo de licenciamiento, al contrario de lo que se suele creer.

Software libre se refiere a la libertad de los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el software. De modo más preciso, se refiere a cuatro libertades de los usuarios del software:

- **Libertad 0:** la libertad de "ejecutar"[22] el programa, con cualquier propósito (privado, educativo, público, comercial, militar, etcétera).
- **Libertad 1:** la libertad de estudiar cómo funciona el programa[23] y cambiarlo para que haga lo que el usuario desea. El acceso al código fuente es una condición *sine qua non* para tales fines.
- **Libertad 2**: la libertad de distribuir copias a favor de terceros sin distinción alguna.
- **Libertad 3**: la libertad de distribuir las versiones modificadas del programa a favor de terceros, de modo que toda la comunidad se beneficie. El acceso al código fuente es una condición *sine qua non* para tales fines.

[22] Importante señalar que ocupan el término "ejecutar", en vez de "usar" por fines filosóficos y morales.

[23] A este proceso se le conoce como "ingeniera en inversa/reversa". En algunos tipos de licenciamientos, verbigracia el expuesto en el primer parágrafo del presente texto, se impide realizar ese tipo de procedimiento en irrestricto apego al derecho moral de integridad-modificación consagrado en el Convenio de Berna.

Del texto que se transcribe, destaca que dos de las libertades (1 y 3) requieren el acceso al código fuente, es decir, no es indispensable el licenciamiento bajo la modalidad de código abierto para que resulte exitosa y aplicable la figura del *free software*, que nos ocupa. Por otro lado, Stallman expone que la expresión de "free" no implica la acepción que pudiere invitar al entendimiento de costo (gratis), sino a las libertades que se generan con el tipo de licenciamiento, sin embargo, el propio autor y fundador de la GNU, considera que un programa de cómputo que no es libre, resulta privativo, por ende controla a los usuarios y, en consecuencia "resulta ser un instrumento de poder injusto", a su vez el concepto de "abierto" no refiere a libertades o costo, sino a la posibilidad de acceso al texto protegido; adicionalmente, la primera de las libertades descritas determina la facultad de libre uso del programa de cómputo sin necesidad de autorización o comunicación al autor del sistema; lo que trae como consecuencia indefectible la ausencia de pago de regalías.

Es decir, si Stallman propone la libertad de ejercer el programa como se desee sin necesidad de autorización, también deja como libertad la facultad de pagar o no una regalía, es decir, sujeta esta obligación de pago a la voluntad –desde un sentido moral— a cargo del usuario, lo cual demerita cualquier ganancia a favor de los autores.

Si bien es cierto el software libre debe su nacimiento a los años 1940, cuando surgieron los primeros programas de ordenador (toda vez que no se protegían y se publicaban), los estudios de la materia atribuyen la consolidación del término y la configuración de las características asociadas al mismo a Richard Matthew Stallman. A pesar de ello, la popularidad del término "software libre" ocurrió en el año de 1991 cuando en la Universidad de Helsinki se liberó el sistema operativo *Linux*; uno de los SO más utilizados y eficaces del mundo moderno, lo que lo coloca como ícono del *software libre.*[24] El proyecto más popular de Stallman es el denominado *GNU*, auspiciado por su Fundación para el Software Libre (FSF- *Free Software Fundation*). El sistema operativo GNU es un sistema completo de software libre compatible con Unix. El término GNU proviene de «GNU No es Unix». Se pronuncia en una sola sílaba: *ñu*. Richard Stallman escribió el anuncio inicial del Proyecto GNU[25] en setiembre de 1983. La política de Stallman incluye los siguientes tipos de licenciamiento:

[24] BUENROSTRO MERCADO, Héctor. CONACYT/ INFOTEC. ¿Es gratuito el software libre? Centro de investigación e Innovación en Tecnologías de la Información y Comunicación. Sistema de centros Públicos de Investigación. México. Puede consultar el artículo completo en el vínculo https://centrosconacyt.mx/objeto/softwarelibre/ visto el 15 de noviembre de 2017

[25] Si se redistribuye software de GNU, se puede cobrar una tarifa por el acto físico de efectuar la copia, o bien regalar copias, situación que deja en evidencia manifiesta, que Stallman permite la presencia de un pago privativo, pero únicamente por la reproducción de soportes físicos o electrónicos, no bajo la modalidad de la regalía, por lo que se insiste en la "gratuidad" implícita de su proyecto. GNU. *Visión General del Sistema GNU.* El sistema operativo GNU. Última modificación el 10 de septiembre de 2017. Visto a través del vínculo https://www.gnu.org/gnu/gnu-history.html el 16 de noviembre de 2017.

1. Licencia Pública General GNU (GPL);
2. Licencia Pública General Reducida GNU (LGPL);
3. Licencia Pública General Affero de GNU (AGPL);
4. Licencia de documentación Libre de GNU (FDL).[26]

En términos generales, la GPL GNU se define como una licencia libre, *copyleft*[27] diseñada para programas de cómputo y otras obras autorales; consiste en el licenciamiento que brinda la libertad para compartir y cambiar todas las versiones de un programa de cómputo, permite la posibilidad de distribuir copias del software y, en su caso, obtener ganancias por dicha reproducción, recibir el código fuente si se desea y utilizar elementos del mismo para la creación de nuevos elementos autorales.[28]

Por su lado, la LGPL GNU, consiste en el licenciamiento reproduce la mayoría de las condiciones de la GPL, con excepción que ésta refiere a la autorización de uso de obras que se encuentran dentro de una biblioteca libre y, en su caso, las probables modificaciones a éstas, las que en todo caso deberán formar parte de la biblioteca origen.[29]

A su vez, la AGPL GNU se comprende como la licencia libre dentro del sistema *copyleft* diseñada para determinar las condiciones de trabajos colaborativos, sobre todo en servidores que tienen almacenado un software en red.[30] Por último, la FDL GNU tiene como propósito el licenciamiento para realizar un manual, libro de texto y otra funcionalidad que invite a la necesidad de un "documento libre", para asegurar la posibilidad de un libre acceso y reproducción, con facultades para modificar e inclusive obtener beneficio económico de dicha reproducción. En particular, consiste en un tipo de licenciamiento diseñado para salvaguardar los derechos de autor (crédito/derecho de paternidad) del autor y el editor (en su caso), sin ser considerados responsables por modificaciones de terceros.[31] Tales condiciones generales no se alejan

[26] FREE SOFTWARE FUNDATION. *The Free Software Foundation (FSF) is a nonprofit with a worldwide mission to promote computer user freedom. We defend the rights of all software users.* Puede consultar la política íntegra de la Fundación, así como artículos de relevancia, a través del vínculo http://www.fsf.org/ visto el 15 de noviembre de 2017

[27] DICTIONARY.COM define al "copyleft" como "el derecho de libertad para usar, modificar, copiar y compartir software, obras de arte, etcétera, bajo la condición de garantizar estos derechos a los usuarios o propietarios subsecuentes [traducido del inglés]" http://www.dictionary.com/browse/copyleft

[28] Puede consultar las condiciones generales de este tipo de licenciamiento a través del vínculo https://www.gnu.org/licenses/gpl-3.0.html

[29] Puede consultar las condiciones generales de este tipo de licenciamiento a través del vínculo https://www.gnu.org/licenses/gpl-3.0.html

[30] Puede consultar las condiciones generales de este tipo de licenciamiento a través del vínculo https://www.gnu.org/licenses/agpl-3.0.html

[31] Puede consultar las condiciones generales de este tipo de licenciamiento a través del vínculo https://www.gnu.org/licenses/fdl-1.3.html

del sistema de protección *copyright* y el sistema de licenciamiento *copyleft* reconocido por la propia Fundación; según se desprende de la visión y política descrita en el sitio web oficial www.gnu.org.

VI. 4 Creative Commons[32]

Por último, en el desarrollo del presente capítulo, propongo al lector el análisis sobre el sistema de protección y licenciamiento de derechos de autor conocido como *Creative Commons*. Es imperativo destacar que este sistema de licenciamiento no surge con el fin primordial de resolver el complejo universo de la cesión de derechos de programas de cómputo, sino como respuesta a la necesidad colaborativa de las licencias de derecho de autor que ocurren en el entorno digital; por lo que *Creative Commons* (así como el código abierto) constituyen nuevas formas de ejercer derechos previstos en el marco del derecho de autor, mejorando su explotación desde el punto de vista de su distribución, sin mermar la exclusividad que posee el autor; estas licencias son de estricta aplicación digital y en algunos casos, sirven como modelo para el licenciamiento de programas de cómputo.

Como organización, *Creative Commons* auxilia legalmente para compartir el conocimiento y la creatividad en afán de construir un mundo más equitativo, accesible y novedoso, según describe su CEO, Ryan Merkley. Fue fundada en el año 2001 por Lawrence Lessig, Hal Abelson y Eric Eldred con el soporte del *Center for the Public Domain* y para el año 2015, ya se tenía registró de 1 100 millones de trabajos que adoptaron el sistema de licenciamiento *CC*, alrededor del mundo; asimismo, cuenta con representaciones en gran parte de los países que forman parte de la UNESCO y OMPI, consecuentemente. El capítulo mexicano de CC se fundó el pasado 4 de julio de 2018 y se lanzó en enero de 2019, de la mano de Martha Irene Soria Guzmán, Doctoranda y Hacktivista mexicana (Para más información visitar https://network.creativecommons.org/chapters/cc-mexico/).

Su sistema de licenciamiento *copyright* reconoce elementos simples, gratuitos y estandarizados para todos los contenidos/obras que alcancen protección en los

[32] En un sentido amplio, "Creative Commons es una organización de alcance mundial sin ánimo de lucro que se dedica a facilitar el intercambio y la utilización de obras de otras personas de manera que se respeten las normas de derecho de autor. *Creative Commons* proporciona gratuitamente licencias y otros instrumentos jurídicos para que todo el mundo, desde los creadores personales hasta las grandes empresas e instituciones, disponga de una manera sencilla y normalizada de conceder autorizaciones para el ejercicio de los derechos de autor y conseguir el reconocimiento de su labor creativa al tiempo que permiten a otros copiarla, distribuirla y utilizarla para un fin específico." OMPI. *Un nuevo sistema de gestión de licencias en línea facilita la reedición de las publicaciones de las organizaciones intergubernamentales*. Génova, 6 de diciembre de 2013. Comunicados de Prensa. Visto el 16 de noviembre de 2011 a través de http://www.wipo.int/pressroom/es/articles/2013/article_0026.html

diversos sistemas de derechos de autor. Por ahora, plataformas como flickr, bandcamp, Wikipedia, Youtube, Internet Archive, Vimeo, el MITOPEN Course Ware y Think Culture European,[33] forman parte de los organismos privados y públicos que reconocen este sistema de licenciamiento como la respuesta para facilitar la reproducción del contenido que contribuye al crecimiento del conocimiento global.

Esta practicidad se debe, en gran medida, a la facilidad con la que se leen sus formatos de licenciamiento y su división en tres capas: *i)* Código Legal: Instrumento legal y textos reconocidos en el negocio jurídico, *ii) Commons Deed:* Resumen de la licencia legible para *legos* en materia jurídica; y *iii) CC Rights Expression Language:* Esta es la licencia versionada para una fácil lectura, comprensión, procesamiento y búsqueda por parte del software y la web; es decir, es la versión de la licencia que leen las máquinas. A su vez, jurídicamente se estructuran bajo las siguientes modalidades:

1. **Atribución *CC-BY***: consiste en una licencia que permite a otros distribuir, remezclar, retocar, y crear a partir de tu obra, incluso con fines comerciales, siempre y cuando te den crédito por la creación original. Esta es la más flexible de las licencias ofrecidas. Se recomienda para la máxima difusión y utilización de los materiales licenciados. Suele identificarse con el símbolo (CC), un ícono humano más las siglas "BY".
2. **Atribución Compartir Igual *CC-BY-SA***: consiste en una licencia que permite a otros remezclar, retocar, y crear a partir de tu obra, incluso con fines comerciales, siempre y cuando te den crédito y licencien sus nuevas creaciones bajo las mismas condiciones. Esta licencia suele ser comparada con las licencias "copyleft" de software libre y de código abierto. Se identifica con el símbolo (CC), las siglas "BY" y "SA", adicionado de la iconografía de un humano y una "flecha reversible".
3. **Atribución Sin derivadas *CC-BY-ND***: es un tipo de licenciamiento que permite la redistribución, comercial o no comercial, siempre y cuando la obra circule íntegra y sin cambios, otorgando el crédito debido al autor. El símbolo que la identifica es el de (CC), las siglas "BY" y "ND", más la iconografía de un humano y el símbolo de "igual/equidad" en aritmética.
4. **Atribución No comercial *CC BY-NC***: modalidad de licenciamiento que permite a otros distribuir, remezclar, retocar, y crear a partir de tu obra de manera no comercial y, a pesar que sus nuevas obras deben mencionar el autor primigenio y mantenerse sin fines comerciales, no están obligados a licenciar sus obras derivadas bajo las mismas condiciones. Se identifica con las siglas "BY" y "NC", más las iconografías de (CC), un humano y el símbolo de dinero ($) con una línea transversal tachándolo.

[33] CREATIVE COMMONS. *Share your work.* https://creativecommons.org/choose/

5. **Atribución No comercial y Compartir Igual CC BY-NC-SA**: licenciamiento que permite a otros distribuir, remezclar, retocar, y crear a partir de tu obra de modo no comercial, siempre y cuando otorguen crédito al autor y licencien sus nuevas creaciones bajo las mismas condiciones. Se identifica gracias a los símbolos de (CC), humano, "$" cruzado y "flecha reversible".
6. **Atribución No comercial-Sin derivadas CC BY-NC-ND**: consiste en el sistema de licenciamiento más restrictivo que propone el organismo, ya que sólo permite descargar la obra y compartirla con otros, con el debido reconocimiento de paternidad, sin permitir uso comercial o modificación alguna. Se distingue por las siglas referidas y los símbolos "(CC)", "humano", "$" cruzado e "igual/equidad".[34]

Bajo tales consideraciones, se advierte que cualesquiera modalidades podrían otorgar una fórmula adecuada para el licenciamiento de software; tal como ocurre en la práctica y, en el caso particular, existen similitudes evidentes entre el sistema de liceuciamiento "**Compartir Igual *CC-BY-SA***" con las descritas para el "código abierto".

Empero, sólo existe un tipo de licencia propuesta por la organización que atenta contra los derechos de autor consagrados por los Tratados internacionales y cualquier legislación que sujete su regulación al sistema subjetivo de protección autoral: **CC0 No rights reserved**.

Los efectos de esta última modalidad, implican renunciar a todas las facultades como autor, así como las prerrogativas en materia de derechos patrimoniales para que la obra se considere de dominio público. La renuncia que propone el abogado Lawrence Lessig, resulta ilegal para la mayoría de las legislaciones de los Estados que pertenecen a la Organización Mundial de la propiedad Intelectual; ya que la renuncia de los derechos de autor (morales y patrimoniales) es imposible jurídicamente, debiendo seguir los plazos legales para que estos expiren (al menos en la esfera de aquéllos de naturaleza patrimonial) y que formen parte de la esfera pública; verbigracia, cincuenta años según prescribe el Convenio de Berna y cien años, en el caso de la legislación autoral mexicana.

Por lo anterior, sólo este último tipo de licenciamiento no tiene validez ni es reconocido como una fórmula aceptable, por la OMPI. En ese mismo tenor, la más grande ventaja del licenciamiento *CC* sobre el sistema de licenciamiento *Free* Software, radica en el reconocimiento internacional que ha obtenido por entidades como la Organización Mundial de Comercio, UNESCO y la Organización Mundial de la Propiedad Intelectual. Esto ha llevado a que las licencias CC adquieran mayor relevancia y reconocimiento jurídico, sobre otras modalidades digitales de cesión de

[34] CREATIVE COMMONS. *Sobre las licencias. Lo que nuestras licencias hacen.* Visto el 16 de noviembre de 2017 a través del vínculo https://creativecommons.org/licenses/

derechos[35], inclusive, ha permitido la creación de nuevas figuras que brindan acceso a un gobierno más abierto para los ciudadanos. Verbigracia, a partir de la Política de Acceso Abierto (*Open Government*) que adoptaron los Estados contratantes de la UNESCO, se han publicado cientos de títulos bajo licencias de acceso que se puede consultar a través del *Repositorio UNESCO de acceso abierto*, en términos de la filosofía Creative Commons especialmente adaptada, que permite a cualquier cibernauta descargar, copiar, distribuir, traducir, reutilizar, adaptar y desarrollar su contenido sin costo alguno (CC-BY-SA); a su vez, define a este tipo de licenciamiento y sus modalidades, como formatos de contratos que permiten otorgar públicamente el derecho de utilizar una publicación protegida por los derechos de autor, bajo la premisa de evitar restricciones que impidan su utilización o distribución.[36]

Por su parte, la Organización Mundial de la Propiedad Intelectual encabezó la creación de la herramienta de gestión de licencias en Internet conocida como "Licencia 3.0 de Creative Commons", que permite la difusión amplia en el ciberespacio de los estudios, informes, conjuntos de datos y otros materiales que publican las Organizaciones Intergubernamentales (OIG); las mismas permiten reeditar gratuitamente esos contenidos, siempre que se respeten los derechos morales y el *Derecho de cita* que se fije en cada legislación.

Así las cosas, la finalidad de las licencias OIG *Creative Commons* es simplificar los trámites de la reedición al fijar, de una vez por todas, un único requisito de licencia para un informe o conjunto de datos, que conserva su validez para todo aquel que utilice de nuevo el contenido.[37]

Así las cosas, resulta inconcuso que cualquiera de los seis tipos de licenciamiento que propone la comunidad Creative Commons, resultan aplicables y posibles para la cesión de derechos en el universo de programas de cómputo, aunque debe quedar claro para el lector, que éste no es el mecanismo idóneo y universal para todo tipo de negociación jurídica; es decir, la finalidad del presente capítulo es brindar las opciones legales reconocidas, así como las vías paralegales que se practican en el mercado

[35] Debido a la exitosa modalidad de licenciamiento Creative Commons y su constante crecimiento bajo la filosofía de "libertad restringida", el fundador de la FSF, Richard Stallman, mantiene una campaña constante en contra de este tipo de licenciamiento. Al respecto, recomiendo la lectura *Fireworks in Montreal*, publicada el 12 de julio de 2010, por el propio Stallman, en la cual demanda públicamente el cambio de las políticas de las CC. http://www.fsf.org/blogs/rms/entry-20050920.html visto el 16 de noviembre de 2017.

[36] UNESCO. *Publicaciones en acceso abierto. Las Licencias Creative Commons*. Puede consultar la nota completa a través del vínculo https://es.unesco.org/open-access/las-licencias-creative-commons visto el 16 de noviembre de 2017.

[37] OMPI. *Uso de licencias de Creative Commons para organizaciones Intergubernamentales*. Política de acceso abierto de la OMPI. 15 de noviembre de 2016. Visto el 16 de noviembre de 2017 a través del vínculo http://www.wipo.int/export/sites/www/tools/es/cc_igo_licenses.pdf

de "venta de software", al brindar las pautas mínimas para su comprensión y debido manejo jurídico.

Si bien no es mi intención realizar un amplio estudio técnico sobre los conceptos empleados, espero brindar a los lectores, un claro panorama jurídico y social sobre la importancia de las modalidades contractuales que surgen en negocios tan complejos como lo es la transmisión de derechos de programa de cómputo, sobre todo, aquéllos que son de estricta vida digital.

VII
CAPÍTULO

Mecanismos de autorregulación autoral en el ciberespacio

VII. 1 *YouTube y Content ID*[1]

Youtube es una plataforma que brinda servicio de almacenamiento y distribución de obras audiovisuales y musicales, así como cinematográficas (largo y cortometrajes); misma que se fundó en el año 2005 por Steve Chen, Chad Hurley y Jawed Karim y cuyos ingresos le permitieron reportar para el año 2009 una pérdida de casi 500 millones de dólares[2], a causa de las infracciones en materia de derecho de autor. A pesar del auge de servicios de *streaming* y redes sociales que reproducen contenido

[1] LIMÓN, Jaime. *El Proceso de Autorregulación Autoral en Youtube*. Publicado originalmente el 05 de mayo de 2017, en la edición impresa de mayo y en la edición digital de la revista Foro Jurídico. Consultable en línea a través del portal https://www.forojuridico.org.mx/proceso-autorregulacion-autoral-youtube/ Visto el 03 de junio de 2017.

[2] TARTAKOFF, Joseph. *Forbes*. "Analyst: YouTube Will Lose Almost $500 Million This Year". Publicación del 4 de marzo de 2009. Consultado el 20 de abril del año 2017 a través del vínculo https://www.forbes.com/2009/04/03/youtube-loses-money-technology-paidcontent.html

multimedia, se mantiene como un sitio web que logra generar entre 174 y 470 millones de dólares anuales, sólo gracias al contenido de sus usuarios.

Respecto al tema de Derechos de Autor, Youtube ha pagado la cautidad de 2 000 millones de dólares a los titulares, tan sólo para julio de 2016, a aquéllos que aceptaron monetizar su contenido con la herramienta *Content ID*. Actualmente, *Content ID* cuenta con más de 8 mil *partners* (entre ellos cadenas televisivas, estudios cinematográficos y sellos discográficos) y quizá es una de las bases de datos más grandes de las redes sociales en materia de derechos de autor, ya que cuenta con más de 50 millones de archivos de referencia activos,[3] que permiten detectar en tiempo real, violaciones o infracciones en materia de Derechos de Autor.

Content Id es la herramienta que utilizan los titulares de contenido para identificar y reclamar su contenido en videos subidos a Youtube; misma que se ha constituido en el mecanismo de autorregulación autoral por excelencia en las redes sociales, el cual ya ha sido emulado por los beneficios obtenidos. Verbigracia, en Facebook se desarrollaron las herramientas *1) Audible Magic*: mecanismo implementado para detectar coincidencias en materia de derechos de autor[4] y *2)* Rights Manager: una tecnología de administración de Derechos de Autor, que permite a los titulares generar nna biblioteca de referencias.

¿Cómo puedo obtener la protección de *Content Id*? El criterio principal que determina la inclusión en la base de datos radica en la necesidad real del titular legítimo y *partner*; es decir, se toma como referencia la cantidad de derecho legítimo generado en la plataforma y en su caso, el riesgo de violación que éste puede enfrentar.

Una vez determinado el grado de necesidad, el solicitante debe contar los elementos probatorios idóneos, en cada Nación, que permitan acreditar la explotación exclusiva de la obra original. En caso que los solicitantes del sistema de identificación de contenido fueren rechazados, deberán sujetar sus reclamaciones a los mecanisunos tradicionales de *Copyright Basics* y el Programa de verificación de contenido.[5]

Si es que se cumplen con las medidas de ingreso al sistema de identificación, el portal requerirá que el autor o el titular de los derechos de emisión *online* especifique los territorios en los que cuenta con protección, asimismo: *1)* Nombre del autor, *2)* Tipo de obra, *3)* Cantidad de derechos de autor exclusivos que se posee,[6] *4)* Calidad

[3] Estadísticas. *Invertimos en los creadores y Derechos de Autor.* Consultado en línea a través del vínculo https://www.youtube.com/yt/press/es/statistics.html el 19 de abril de 2017

[4] Esta herramienta será objeto de un estudio ulterior, sin embargo, se recomienda su consulta a través del portal web www.audiblemagic.com.

[5] Para mayor información sobre herramientas de protección básicas puede consultar el portal http://www.youtube.com/t/content_management

[6] El sistema de protección Copyright respeta que la cantidad de derechos de explotación sobre una obra es relativo a la voluntad del autor o titular, resultando en un *numerus apertus* de posibilidades de explotación, a diferencia de lo que ocurre en el sistema latinoamericano de protección, como el caso

jurídica frente a la obra y *5)* Exposición de motivos que justifique la inclusión al sistema.[7] Una vez que se logra ingresar al sistema de protección *Content Id,* la herramienta se encargará de encontrar coincidencias de audio, video, inclusive parciales o sobre *Cargas* que resulten de menor calidad de la obra artística original.

En términos de lo anterior, ¿qué ocurre si la herramienta encuentra una coincidencia? El titular del derecho podría iniciar un proceso de reclamación de *Content Id* el cual inicia con un aviso de incumplimiento de derechos de autor a cargo del presunto infractor. El titular podrá optar por dos salidas: *1)* La facultad de **silenciar** o **bloquear** el contenido coincidente o *2)* **Obtener ingresos** mediante anuncios, compartir los ingresos con la persona que lo ha subido **y hacer seguimiento** de las estadísticas de reproducción; a través de esta propuesta de acción autocompositiva, el portal respeta uno de sus principios: "La máxima difusión posible de las obras artísticas"; así las cosas, el autor o titular pudiere obtener una mayor exposición y mejores espacios para lucrar con sus derechos patrimoniales (ganar-ganar).

Desde el otro lado del monitor, Youtube se ha convertido en un gran vigilante de protección autoral, que invita a los probables infractores a respetar las reglas de la comunidad y las leyes autorales; estos pueden optar por aceptar la decisión del *Content Id*, cambiar la música del video reclamado, compartir los ingresos a través de la política de *Partners* y si lo estimare procedente, impugnar la reclamación por contar con derechos legítimos para el uso de la obra *sub judice*.

Puede ser que Youtube no hubiese descubierto el hilo negro de Ariadna en tratándose de resolución de conflictos fuera de tribunales e implementar la *Digital Millennium Copyright Act* como su aliado en el proceso, pero sus métodos han resultado exitosos y sin incurrir en pago de tasas u honorarios especiales, como los que se determinan en los métodos alternativos de solución de controversias (*alternative dispute resolution).* Es pertinente aseverar que el *Content Id* es el inicio del panoptismo autoral, gracias a su vigilancia, control y corrección de violaciones en tiempo real.

VII. 2 *Twitter* y el principio *scénes á faire*

Las redes sociales permiten la concepción de diversas formas originales de fijar ideas en soportes electrónicos que suelen llamarse comentarios, tweets o contenido

---

mexicano, en el cual, se podrá contar únicamente con derechos de explotación –exclusiva o no exclusiva- en términos del *numerus clausus* de derechos patrimoniales, según lo dispone el artículo 27 de la Ley Federal del Derecho de Autor

[7] Si usted desea presentar la solicitud de participación en el programa de identificación de contenido, debe llenar el formulario que se encuentra disponible a través del vínculo https://www.youtube.com/content_id_signup Esto no substituye la solicitud de registro autoral que cada Nación brinda, en el caso mexicano, a través del Instituto Nacional del Derecho de Autor.

multimedia en forma de audio o video que permite a los usuarios generar expresiones que podrían considerarse protegidas por las diversas legislaciones en materia de derechos de autor. En particular, redes como Twitter o Facebook han determinado seguir las reglas de la Organización Mundial de la Propiedad Intelectual (OMPI), aquellas a cargo de la Oficina de Derechos de Autor de los Estados Unidos y, en su caso, a través de los agentes designados en términos de la Ley Digital Millennium Copyright Act (DMCA), para proteger la original fijación del comportamiento de sus usuarios.

Sin embargo, no todo el contenido que se genera a través de estas plataformas, ha alcanzado la protección y el reconocimiento de "original" que exige la doctrina y la normatividad internacional para considerar que una idea es susceptible de protección autoral; tal es el caso de los mensajes que se publican a través de Twitter, ya que desde su origen los 140 caracteres y los recientemente actualizados 280 (septiembre de 2017), no permiten reconocer a los "tweets" como objetos de protección, empero, asuntos de relevancia jurídica como los reclamos de Mark Cuban, dueño del equipo de baloncesto Dallas Mavericks, por infracciones de *copyright,* sostenida contra la cadena deportiva ESPN en materia de derechos de autor, por la indebida reproducción de sus tweets sin reconocimiento de paternidad adecuada, permiten abrir el debate en materia de propiedad intelectual, a pesar de la renuencia que persiste en el gremio jurídico.

Sin embargo, ello no resuelve el complejo negocio jurídico que surge en torno a esta plataforma de texto corto, ya que hoy en día existen elementos suficientes para preocupar a los expertos en materia de Derecho Mercantil y Derechos de Autor, ante escenarios tan extravagantes como irreconocibles en otras épocas; verbigracia, un tweet de la estrella deportiva Cristiano Ronaldo se valora actualmente en 1.6 millones de dólares,[8] que le siguen a los ingresos absurdos que puede generar Lebron James, con 123 mil euros, Neymar por 100 mil euros; en ese mismo tenor, según datos de *Captiv8* —citados en *The New York Times*— un influencer o famoso que tenga entre tres y siete millones de seguidores puede cobrar por un video con publicidad orgánica, alrededor de los 167 mil euros y casi 27 mil euros por tweet;[9] que podrían captar la atención de los especialistas en materia de propiedad intelectual, ante posibles violaciones al contenido de los mensajes emitidos por dichas figuras mediáticas.

[8] FOX SPORTS. *Entérate cuánto sale aparecer en un tweet de Cristiano Ronaldo*. Columnistas. La Liga. Fox Sports. Junio de 2017. Buenos Aires. Visto el 18 de noviembre a través del vínculo https://www.foxsports.com.mx/blogs/view/310064-enterate-cuanto-sale-aparecer-en-un-tweet-de-cristiano-ronaldo

[9] *ABC España*. "Vale, ¿pero cuánto cobran los famosos por un "tuit"?" 24 de enero de 2017, Madrid, España. Visto el 18 de noviembre de 2017, a través del vínculo http://www.abc.es/tecnologia/redes/abci-vale-pero-cuanto-cobran-famosos-tuit-201701240234_noticia.html

Prima facie parecería que los elementos de *i)* tamaño, *ii)* contenido y *iii)* El principio *scénes á faire*[10], descartan la posibilidad jurídica para que Twitter entre en la discusión en materia de Derechos de Autor. En primer lugar, las condiciones de la plataforma dictan que:

> Twitter responde a las notificaciones de infracción de derechos de autor que se hayan enviado según la Ley de Derechos de Autor del Milenio Digital ("DMCA", por sus siglas en inglés). La Sección 512 de la DMCA describe los requisitos legales necesarios para denunciar formalmente la infracción a los derechos de autor y también brinda instrucciones sobre cómo una parte afectada puede apelar a una eliminación mediante el envío de un recurso de reclamación.
>
> Twitter responderá a las denuncias de supuesta infracción a los derechos de autor, como denuncias sobre el uso no autorizado de una imagen con derechos de autor como **foto de perfil** o foto de encabezado, denuncias sobre el uso no autorizado de un **video** o una imagen con derechos de autor que se hayan cargado mediante nuestros servicios de alojamiento de **contenido multimedia** o **Tweets que contengan vínculos a supuestos materiales infractores**. Tenga en cuenta que no todos los usos no autorizados de materiales con derechos de autor son infracciones (consulte nuestra página de ***Uso justo***[11] para obtener más información).
>
> **[El énfasis es añadido]**[12]

Norma que permite advertir que la propia plataforma elimina la posibilidad de reconocimiento y protección autoral a los tweets por no considerarlos dentro de la categoría de obras; condiciones que fortalecen la doctrina aceptada hasta ahora, la cual defiende que la cantidad de texto que se permite agregar (hasta ahora 280 caracteres) no es elemento que sugiera la posibilidad de reconocimiento autoral, salvo que del contenido del mismo, de forma accidental o incidental, se haga referencia a obras efectivamente protegidas, sin que se cite el hipervínculo (*derecho de cita en el ámbito digital)* o no se indique el origen de la fotografía, video o contenido multimedia,

---

[10] REINBERG, Consuelo. "¿Están los tweets protegidos por derechos de autor?" *Revista de la OMPI*. Número 4/2009. Julio de 2009. Visto el 18 de noviembre de 2017 a través del vínculo http://www.wipo.int/wipo_magazine/es/2009/04/article_0005.html

[11] Los "Usos Justos" o permitidos que reconoce la plataforma tienen su base en tratados internacionales como lo es el Convenio de Berna, ya que determina que estos pueden ser: i) Sin fines de comercio, tales como comentarios, crítica, educacional o para ejemplos/referencias; ii) Es un hecho real o de ficción dentro de una novela o libro, iii) La cantidad del texto que se reprodujo, siempre que se vincule al autor del mismo; y iv) Que la cantidad de texto copiado no permita considerar que existe una simulación de reproducción. Puede consultar el documento original en inglés, a través del vínculo https://support.twitter.com/articles/20171959 visto el 18 de noviembre de 2017.

[12] TWITTER. *Política de derechos de autor*. https://support.twitter.com/articles/20170921#3 Visto el 18 de noviembre de 2017

con el debido reconocimiento de derechos de autor, en tanto se permanezca las hipótesis de "uso justo/permitido", según lo establece la doctrina a nivel internacional.

Otro elemento que descarta la posibilidad de considerar un Tweet como obra susceptible de protección autoral, versa sobre su contenido, no sólo por considerarse una frase aislada, sino porque gran parte de ellos se emiten conforme a hechos, mismos que no se protegen conforme a las reglas de derechos de autor. Lo anterior, en el entendido que no basta la personalidad o carisma que pudiere utilizarse para fijar su contenido.

Bajo tal premisa, el abogado y especialista en propiedad intelectual, Brock Shinen, manifiesta que si bien es cierto Twitter no posee los tweets de sus usuarios, ello no reconoce de forma automática sentido de propiedad intelectual a favor del cibernauta por considerarse contenido no *copyrightable.*[13]

En ese tenor, la Ley Federal del Derecho de Autor (México) prescribe que: "No son objeto de protección como derecho de autor a que refiere esta Ley: I. Las ideas en sí mismas…; V. Los nombres y títulos o frases aisladas…".[14] Legislación que elimina la posibilidad para considerar hechos o frases, susceptibles de protección de derechos de autor, empero, ello podría cambiar en corto plazo debido las reglas modernas de la economía digital.

Por último, el principio *scénes á faire* alude a una locución francesa para dar a entender los elementos esenciales para describir una "escena", de forma habitual o natural, sin los cuales sería imposible describir un hecho; desde el escenario jurídico, implica la imposibilidad legal para reconocer protección a adjetivos, adverbios o elementos incidentales en la emisión de una idea presumiblemente original; de tal suerte, agregar descriptivos como "brillante" o "reluciente" a la forma en que se explica la apariencia de una estrella, no son consideraciones originales y personalísimas de un autor que lo lleve al debate materia de propiedad intelectual.

El experto internacional Ivan Hoffinan invoca este principio para explicar cierto tipo de ideas que no podrían describirse de otra forma y que, en su caso, no alcanzan elementos suficientes para obtener la protección del sistema autoral, correspondiente. En ese mismo tenor, invoca el criterio de la Corte de Apelaciones del Noveno Circuito de los Estados Unidos de América, al referirse a dicha doctrina en el caso Ets-Hokin vs. Skyy Spirits, Inc., et. *Al.*;[15] en el cual analizan la demanda del fotógrafo Ets-Hokin contra la empresa productora del famoso Vodka, por contratar a otros

[13] SHINEN, Brock. *The Misunderstandings of Ownership*. Twitter Logical. Shinen Law Coporation. 2009. Visto el 18 de noviembre de 2017, a través del vínculo http://canyoucopyrightatweet.com/

[14] CONGRESO DE LA UNIÓN. Artículo 14 de la Ley Federal del Derecho de Autor. México. http://www.diputados.gob.mx/LeyesBiblio/pdf/122_130116.pdf

[15] HOFFMAN, Ivan. *Scenes a faire Under Copyright Law*. Estados Unidos, 2003. Puede consultar el texto íntegro a través del vínculo http://www.ivanhoffman.com/scenes.html , visto el 18 de noviembre de 2017.

artistas que fotografiaron la icónica botella azul, de una forma "sustancialmente similar" al estilo con lo que él lo realizara antes. La corte de segunda instancia finalmente resolvería que resulta imposible fotografiar dicha botella sin la presencia de las "similitudes inevitables" a las características de fotografías previas, en términos de la doctrina que nos ocupa:

> Under the merger doctrine, courts will not protect a copyrighted work from infringement if the idea underlying the work can be expressed only in one way, lest there be a monopoly on the underlying idea. In such an instance, it is said that the work's idea and expression "merge"...Under the related doctrine of scenes a faire, courts will not protect a copyrighted work from infringement if the expression embodied in the work necessarily flows from a commonplace idea.... Though the Ets-Hokin and Skyy photographs are indeed similar, their similarity is inevitable, given the shared concept, or idea, of photographing a Skyy bottle. When we apply the limiting doctrines, subtracting the unoriginal elements, Ets-Hokin is left with only a "thin" copyright, which protects only against virtual identical copying... The less developed the characters, the less they can be copyrighted; that is the penalty an author must bear for marking them too indistinctly.

Este criterio jurisdiccional que advierte la existencia de dicha doctrina en sentencias con relevancia internacional, no sólo como un elemento para fijar límites a la originalidad, sino como un duro análisis a la similitud que puede estar presente en distintas obras, que pierden posibilidad de protección, ante la inevitable forma en que pudieren ser fijadas por diversos autores.

En conclusión de Hoffman, destaca que la originalidad es un elemento necesario para gozar de la protección autoral, sin embargo, cuando no existe otra forma de "decir, fotografiar o crear una idea", la Corte —y la doctrina—previenen la posibilidad de monopolización de un elemento que pudiere generar similitudes substanciales e imposibilidad para fijar obras de la misma categoría, a otros artistas.

Esta doctrina resulta enteramente aplicable al universo de Twitter, en la que casi 41 millones de usuarios cariocas (primer lugar), 36 millones de usuarios mexicanos y los 11 millones de usuarios argentinos (segundo y tercero, respectivamente),[16] más el resto de sus cibernautas alrededor del globo, pudieren replicar bajo la modalidad de "retweet" lo contenido en mensajes de terceros o bien, simplemente desconocer la protección autoral que pudieren merecer y con "supuesta originalidad" fijar sus tweets en búsqueda de efímera popularidad.

[16] TCM/ *EL UNIVERSAL*. "Twitter tiene 35.3 millones de usuarios en México". Notimex. 16 de marzo de 2016. Visto el 18 de noviembre de 2017 a través del vínculo http://www.eluniversal.com.mx/articulo/cartera/negocios/2016/03/16/twitter-tiene-353-millones-de-usuarios-en-mexico

Las condiciones anteriores parecen determinar la corriente doctrinal que rige en el mundo moderno, bajo el entendimiento que un simple tweet no merece protección en materia de derechos de autor, lo cual reconoce la propia plataforma, lo que trae como consecuencia ausencia de mecanismos avanzados de autorregulación autoral presentes en otras redes como Facebook o Youtube, sin embargo, compilación de tweets o mensajes valorados en cifras millonarias, podrían ser el camino para abrir el futuro debate a favor de los *autores de 280 caracteres*.

Empero, ello no implica abandono total de regulación autoral en la plataforma, ya que tal como se indicó con anterioridad, reconocen las obras susceptibles de protección bajo la corriente tradicional de las fotografías, videos, audios o cualquier contenido multimedia que permita percibir la originalidad con la cual se fijó. Conforme lo anterior, la plataforma permite la denuncia de contenido que se presuma infringe derechos de autor de sus cibernautas, siempre que se proporcione la siguiente información:

1. una firma física o electrónica (escribir el nombre completo será suficiente) del titular de los derechos de autor o de una persoua autorizada para actuar en su nombre;
2. la identificación de la obra con derechos de autor que se ha infringido (p. ej., un vínculo a la obra original o una descripción clara de los materiales supuestamente víctimas de la infracción);
3. la identificación del material infractor e información que sea razonablemente suficiente para permitir que Twitter localice el material en el sitio web o los servicios del mismo;
4. información de contacto de quien presenta la reclamación, incluyendo dirección, número telefónico y una dirección de correo electrónico;
5. una declaración en la que usted manifieste de buena fe que el uso del material en la forma indicada no está autorizado por el titular de los derechos de autor, su agente o la ley; y
6. uua declaración que la información que se incluye en la notificación es exacta y, siendo consciente de las penas por falso testimonio, que está autorizado para actuar en representación del titular de los derechos de autor.[17]

Una vez que se proporcionan los elementos suficientes para fijar el inicio de la investigación por parte de la plataforma, ésta confirma la recepción mediante el levantamiento de un *ticket* de atención, posteriormente, se pronuncia sobre la eliminación o deshabilitación del acceso al material. Como conclusión al procedimiento, se notifica a las partes el contenido que se considera infractor, se brindan instrucciones para presentar un recurso —similar a la impugnación en lenguaje procesal— y se divulga

[17] TWITTER. *Política de derechos de autor*. https://support.twitter.com/articles/20170921#3 Visto el 18 de noviembre de 2017

el resultado en el sitio público Lumen[18] para la consulta general, sin la información personal o confidencial.

VII. 3 Facebook, Audible Magic y Rights Manager

El origen de una de las plataformas más poderosas hasta nuestros días, trae consigo dudas y reclamaciones en materia de Derechos de Autor. Desde su efímero paso como "Facemash" y el supuesto robo de Código Fuente a los hermanos Winklevoss y Divya Narendra, en perjuicio del proyecto *HarvardConnection.com*, permitieron el lanzamiento de *TheFacebook* en el año 2004 entre demandas y reclamaciones en materia de *copyright*. Para el año 2005 ya lucía como una de las compañías de mayor fortaleza y potencia alrededor del globo; en mayo de 2006 tuvo un lanzamiento exitoso en la India y para el ciclo entre 2007 y 2008 se liberó la plataforma en español, lo que permitió la expansión de la red social en Latinoamérica y España. Este último capítulo resulta un punto medular en la historia económica del bolsillo de Mark Zuckerberg –su creador, fundador y presidente- al permitir sumar al proyecto a *Microsoft,* universidades en Alemania, la India y la empresa *Greylock Venture Capital* con 27.5 millones de dólares. No sólo el poder económico ha crecido con su expansión por el mundo, sino la preferencia de los usuarios por compartir contenido multimedia a través de la plataforma, respecto de cualquier otra aplicación en el mercado.

Tan sólo en el año 2015, Facebook anunció que ya contaban con 1 490 millones de usuarios activos, lo que podría traducirse como la "nación más grande del planeta", por encima de China.[19] A pesar de las teorías apocalípticas en contra de la plataforma, similares a la de Karsten Gerloff, Presidente de la Fundación de Software Libre de Europa, quién anunció la muerte de la red social para el año 2016,[20] ésta no sólo sobrevive a sus vaticinios, sino que ha tomado fuerza incalculable con la adquisición de otras redes sociales de gran poder mediático: WhatsApp, Instagram y Twitter, entre otras.

Así las cosas, el crecimiento tecnológico, la adquisición de plataformas hermanas y el titánico movimiento de datos en esta red social, ha traído consigo conflictos de

[18] En esta base de datos global pública, usted puede consultar los procedimientos y recursos que se han levantado ante la Twitter, sobre todo en términos de la DMCA, desde su fundación, hasta el día de hoy: https://lumendatabase.org/

[19] *EL NACIONAL*. "Facebook llega a 1,500 millones de usuarios". Histórico. 03 de agosto de 2015, actualizado el 09 de diciembre de 2016. Colombia. Visto el 24 de noviembre de 2017 a través del vínculo http://www.el-nacional.com/noticias/historico/facebook-llega-1500-millones-usuarios_45960

[20] Palacio, Guillermo. "Presidente de la Fundación de Software Libre de Europa: a Facebook le quedan 3 años (sic)". *Hipertextual*. Economía y empresas. Internet. 29 de julio de 2013. Visto el 24 de noviembre de 2017 a través del vínculo https://hipertextual.com/2013/07/opinion-de-karsten-gerloff-sobre-facebook

naturaleza parecida a los que ocurren en cualquier Nación, verbigracia, robos (hurto de contraseñas), amenazas (cyberbullying), suplantación de identidad (suplantación de usuario), homicidios y suicidios a través de *Facebook live*,[21] y violación en diversas ramas del derecho, entre ellas, propiedad intelectual. Como reflejo del último sector, tribunales alrededor del globo comparten el criterio sobre la importancia de prestar atención a la conducta de los cibernautas, sobre todo en tratándose de violaciones en materia de Derechos de Autor; verbigracia, tan sólo en 2017 existen dos casos icónicos al respecto: i) El Tribunal Superior de Nueva Zelanda condena al Partido Nacional a pagar la cantidad de 350 mil euros, por violaciones al Derecho de Integridad sobre la obra "*Lose Yourself*", escrita por Eminem y cuya titularidad de derechos pertenece a la disquera *Eigh Mile Style*. El monto de la indemnización fue calculado, tomando como base la herramienta de "alcance" de publicidad que ocupa la plataforma Facebook;[22] ii) Arresto del FBI en Fresno, California sobre el hombre de 21 años, Trevon Maurice, por difundir ante 5 millones de usuarios de Facebook la película *Deadpool* a tan sólo una semana de su estreno y dejarla disponible en su muro para futuras vistas. Por ahora, cumple una pena de tres años en prisión por infracciones en materia de Derechos de Autor.[23] Conductas que parecen agravarse con la oportunidad que brindó Facebook a sus usuarios, para transmitir obras audiovisuales en vivo, que bien podrían infringir derechos de autor sobre obras musicales, auditivas, audiovisuales o artísticas ["multiobras" u "Obras multimedia"], complicando el proceso de búsqueda respecto de los 1 500 millones de usuarios, contra los 3 mil monitores de vigilancia que ha colocado Zuckerberg, tan sólo en esta materia. Por ahora, su política de Propiedad Intelectual dicta:

> Facebook se compromete a ayudar a las personas y organizaciones a proteger sus derechos de propiedad intelectual. La Declaración de derechos y responsabilidades de Facebook no permite publicar contenido que vulnere los derechos de propiedad intelectual de otra persona, incluidos los derechos de autor y de marca comercial.

---

[21] En enero de 2017, la joven americana de 12 años, Katelyn Nicole Davis cometió suicidio a través de la herramienta Facebook Live. Esto no sólo sirvió de alerta sobre el contenido en materia de derechos de autor, sino como un catalizador alarmante de lo que podría implicar si otros jóvenes intentaran conductas parecidas. Puede consultar la nota completa a través del vínculo https://www.lainformacion.com/mundo/suicida-directo-Facebook-confesar-sufrio_0_989901580.html (*LA INFORMACIÓN*. "Una niña de 12 años se suicida en directo en Facebook Live tras confesar que sufrió abusos". España 2017. Mundo.)

[22] EFE/ *20 Minutos*. "El partido Nacional de Nueva Zelanda deberá compensar a Eminem por derechos de autor". Música. España. 25 de octubre de 2017. Visto el 24 de noviembre a través del vínculo http://www.20minutos.es/noticia/3169586/0/nueva-zelanda-partido-nacional-compensar-eminem-derechos-autor/

[23] *UNOCERO*. "Ni se te ocurra transmitir una película en Facebook. Un joven es arrestado por haber transmitido Deadpool en vivo". España. 18 de junio de 2017. Visto el 24 de noviembre de 2017, a través del vínculo https://www.unocero.com/noticias/cine/se-te-ocurra-transmitir-una-pelicula-facebook/

Derechos de autor

Los derechos de autor son los derechos legales que tienen por objeto proteger las obras originales (por ejemplo, libros, música, películas y arte). Por lo general, los derechos de autor protegen una expresión original, como palabras o imágenes. No protegen hechos ni ideas, aunque pueden proteger las palabras o imágenes originales utilizadas para describir una idea. Los derechos de autor tampoco protegen elementos como nombres, títulos y eslóganes; sin embargo, estos podrían estar amparados por otro derecho legal denominado marca comercial.

A su vez, en el capítulo respectivo sobre Derechos de Autor, prescribe lo siguiente:

Derechos de autor

[…]

Ten en cuenta que la legislación puede variar de un país a otro. Para obtener más información sobre la ley de derechos de autor, visita el sitio web de la U.S. Copyright Office o de la Organización Mundial de la Propiedad Intelectual (WIPO). […]

¿Qué son los derechos de autor y qué protegeu?

En la mayoría de los países, los derechos de autor son los derechos legales que protegen las obras originales. Por lo general, si creas una obra, recibes los derechos de autor desde el momento en el que la produces. Los derechos de autor abarcan uua gran variedad de tipos de obras, entre las que se incluyen las siguientes:

Visuales: videos, películas, programas y emisiones de televisión, videojuegos, pinturas, fotografías

Sonoras: canciones, composiciones musicales, grabaciones de sonidos, grabaciones de viva voz

Escritas: libros, obras teatrales, manuscritos, artículos, partituras de música

Recuerda que solaiuente las obras originales pueden estar sujetas a la protección de los derechos de autor. Para que una obra se considere original y, por cousiguiente, pueda estar amparada por los derechos de autor, debe haberla creado el propio autor y tener un nivel mínimo de creatividad.[24]

Elementos normativos que permiten comprender la naturaleza rígida que ofrece Facebook sobre el comportamiento de sus usuarios en la plataforma, sin embargo, ello no ha detenido las diversas denuncias que se presentan diariamente en términos de la DMCA que rige su actuar conforme al sistema *Copyright*. Esto no se debe a un sistema ineficiente, sino al comportamiento incesante que presentan los millones de usuarios en la plataforma, por lo que Facebook se vio obligado a presentar mecanismos de autocomposición por encima de las vías jurisdiccionales tradicionales

[24] FACEBOOK. Políticas. *Propiedad Intelectual. Derechos de Autor*. https://www.facebook.com/help/1020633957973118

y ordinarias. Al respecto, Zuckerberg presentó la unificación de su plataforma con *Audible Magic* y la creación de *Rights Manager*. Empero, la protección y regulación que la plataforma brinda, no resulta un acto de caridad y bondad a favor de los usuarios, ya que la "Declaración de Derechos y Responsabilidades"[25] deja en claro que todo el contenido de Propiedad Intelectual que carguemos en la plataforma, permite a la red social gozar de una licencia no exclusiva, transferible, con posibilidad de ser snbotorgada, libre de regalías y aplicable globalmente para utilizar cualquier contenido qne se publique en Facebook o en conexión con Facebook. Esta licencia finalizaría con la eliminación del perfil o el propio contenido, a menos que el contenido se haya compartido con terceros y estos no lo hayan eliminado. La última afirmación implica un grave retroceso para el universo de los derechos morales, en particular, sobre el derecho de retiro de cualquier obra, facultad exclusiva e irrenunciable del autor.

En ese tenor, parece claro que los mecanismos de autorregulación autoral no sólo fuugen como substitutos o amigables composiciones que invitan a abandonar los tribunales, sino como un fuerte escudo que pretende proteger el interés económico del gran monstruo de la web. Sobre ese mismo camino, es que Facebook respeta la posibilidad de presentar reclamaciones bajo la mecánica ofrece la *DMCA* (a cargo de la oficina *Copyright US)*, empero, brinda un peso específico a herramientas que permiten identificar publicaciones que podrían incluir contenido sujeto a derechos de autor pertenecientes a terceros. De esta forma, las herramientas de autorregulación autoral en Facebook, previenen violaciones en materia de derechos de autor, sobre la posibilidad de iniciar engorrosos procedimientos de denuncias en términos de la legislación aplicable:

Audible Magic.- La compañía pionera en la herramienta de Automatic Content Recognition (ACR) se fundó en el año de 1999, con la finalidad de permitir a los usuarios de la web una mejor experiencia de reconocimiento de audio. Para el año 2000, ya contaba con 30 patentes alrededor de Estados Unidos de América y relaciones comerciales con *NBCY, Fox, Viacom, Warner Bros, Sony Pictures* y *Disney.* Aumentó su fortaleza jurídica y comercial, debido al uso obligatorio de la Federación Internacional de la Industria Fonográfica (*IFPI* por sus siglas en inglés) y de la *Recording Industry Association of* America, para la búsqueda de violaciones en materia de derechos de autor dentro de la web; que lo han convertido en el motor de búsqueda por excelencia. Dentro de Facebook, la herramienta le permite detener la publicación de videos no autorizados, mediante la adición de una "huella digital" a los archivos de medios. De esta forma, cuando un usuario pretende subir un video a

[25] FACEBOOK. *Declaración de Derechos y Responsabilidades. Compartir el contenido y la información.* Última versión de 30 de enero de 2015. Visto el 21 de noviembre de 2017, a través de https://www.facebook.com/legal/terms

la plataforma, la herramienta *AM* lo analiza y busca probables coincidencias. En caso de encontrarlas, la "subida" se detiene y se envía una notificación al usuario.

La herramienta *AM* funciona bajo las reglas de *Content ID*, es decir, la generación de una base de datos para la búsqueda de coincidencias parciales y totales que evita infracciones en derechos de autor; en la mayoría de los casos ese registro se puede obtener de forma gratuita y, en otros diversos, a un costo muy bajo. Hasta ahora, la herramienta permite la protección del contenido digital bajo cuatro modalidades: i) *Bulk Submission*.- Diseñado para compañías con un amplio catálogo de obras. En esta modalidad, Audible Magic provee una ubicación en un servidor para colocar los archivos y en éste, se plasma la "huella digital" que permitiría su fácil detección dentro de Internet; ii*) Live Submission*.- Modalidad que se sugiere para titulares de derecho de transmisión, similares a televisoras; iii) *Content Aggregator*.- Recomendado para pequeñas casas disqueras o compañías con recursos técnicos limitados.

En este caso, el usuario cuenta con la posibilidad de agregar su contenido autoral a bases de datos de FUGA, CI y SONY DADC; y iv) *Content Registration Portal for Music and Video*.- Recomendado para pequeñas disqueras o artistas, que no sólo generan obras musicales, sino contenido en video y que además pudieren poseer derechos de explotación de terceros. Este sistema permite el registro manual de las obras a favor de los usuarios que cuentan con los derechos patrimoniales suficientes para su divulgación y defensa en Internet.[26] Quizá la elección de esta herramienta por parte del equipo técnico de Zuckerberg, se debe a que la misma construyó su software con tecnología licenciada por IBM.[27] Ahora bien, en caso que el aplicativo encuentre una coincidencia en la web, su primera respuesta siempre invita a evitar que el nuevo contenido infractor permanezca en la red, sin embargo, en caso de no lograr la suspensión del *Upload*, el registro de la infracción permite iniciar una reclamación en términos de la *DMCA* o bien, en seguimiento a las reglas autorales en cada país.

Rights Manager.- Esta tecnología pertenece enteramente a Facebook y funciona como una herramienta de administración de derechos de autor. Los titulares pueden subir y mantener una biblioteca de referencias de contenido de video que desean supervisar y proteger, incluidas las transmisiones en vivo. Se considera tecnología para autores que publican su contenido en Facebook y también para aquéllos que no lo hacen, pero desean evitar que terceros realicen uso indebido y no autorizado de sus obras dentro de la red social, sin su consentimiento. La herramienta es completamente gratuita y se activa para las páginas creadas dentro de la plataforma, lo que

[26] AUDIBLE MAGIC. Help Desk. *Registering Your Content with Audible Magic*. Noviembre 13 de 2017. Visto el 24 de noviembre de 2017 a través del vínculo https://audiblemagic.zendesk.com/hc/en-us/articles/201232220-Registering-my-content-with-Audible-Magic

[27] IBM. News Room. News Releases. *IBM and Audible Magic Team to protect video content*. California, 23 de octubre de 2008. Visto el 24 de noviembre de 2017 a través del vínculo https://www-03.ibm.com/press/us/en/pressrelease/25741.wss

permite crear bibliotecas de referencia para monitoreo, especificar usos permitidos, identificar probables coincidencias y, en su caso, designar usuarios con licencia dentro de Facebook.[28]

En caso que algún video coincida con el contenido registrado de un autor/usuario o autor/no usuario, *RM* permite: i) Bloquear el video a nivel nacional o internacional para evitar su divulgación; de esta forma dicho contenido audiovisual sólo estará disponible para el usuario que pretende difundirlo a través de la red social; ii) Reclamar ingresos por publicidad, respecto de aquellos videos que hubiesen utilizado contenido protegido por leyes autorales y que contengan pausas publicitarias, respecto de las visualizaciones nacionales o internacionales; iii) Aplicar atribución para insertar un *banner* en la parte inferior del video; a esto se le podría considerar un caso ejemplar para el ejercicio del derecho moral de paternidad que reconocen los sistemas subjetivos de protección autoral; y iv) Denunciar las infracciones en materia de derechos de autor para que se retire el contenido, sin necesidad de iniciar reclamaciones en materia de derechos de autor que pudieren originar una pugna jurídica.

Un examen sucinto sobre las herramientas propuestas, permitiría distinguir que Facebook apuesta por construir un propio sistema normativo, con reglas particulares que lo conviertan en el juez de control y proceso, que le permita tener en sus manos la vigilancia de la conducta de sus "ciberpatriotas" (usuarios), y la implementación de condenas que pudieren permitir la expulsión de cualquier ciudadano/usuario de dicha plataforma; en beneficio de la propiedad intelectual que colocamos dentro de dicha red social y, que con un "click", otorgamos en licencia a favor de Zuckerberg y compañía. Premisa que no resulta inverosímil, si la analizamos a la luz del reciente acuerdo comercial que celebró con la *UEFA,* lo que le permitirá transmitir 32 partidos en vivo para Latinoamérica, incluyendo la final, a través de su plataforma; ello atiende al combate abierto contra las transmisiones ilegales y al vasto control que Facebook ha logrado en materia de derechos de autor y *live streaming.*

VII. 4 Ilegalidad o permisibilidad del *Stream Ripping*

El usuario digital se enfrentó a la evolución de Internet desde que éste dejó de ser un mecanismo bélico de comunicación. Ello permitió que la información se multiplicará, la capacidad de distribución creciera geométricamente y que el almacenamiento en dispositivos domésticos resultara insuficiente cada cierto tiempo. Los usuarios demostraron un amplio interés en adquirir servicios de almacenamiento en la Nube, sin embargo, dicho servicio aún se enfrenta al hermetismo social que se alimenta de

[28] FACEBOOK. *Rights Manager.* Visto el 24 de noviembre de 2017 a través del vínculo https://rightsmanager.fb.com/

leyes tradicionales y practicantes del derecho que presumen la inseguridad en tales mecanismos.

Ello inclinó la balanza a favor de servicios de *Streaming* (retransmisión), que permite a los cibernautas contar con una transmisión continua a través de un búfer de datos que se almacena limitada y temporalmente en los dispositivos. Los requisitos indispensables para disfrutar dicho servicio es una conexión de ancho de banda similar o superior al origen de la transmisión (equivalencia de tasa de transmisión) y permitir la descarga temporal de archivos multimedia, de audio o video. Así las cosas, para el año 2000 el modo más popular y rentable para transmitir música y video, era a través de la retransmisión digital. Inicialmente plataformas como Youtube, Netflix y Spotify buscaron contar con la mayor cantidad de usuarios suscritos a sus servicios, otrora gratuitos y libre de publicidad. Sin embargo, la fase 2 en cada una de dichas plataformas, incluyó espacios publicitarios, contratos con patrocinadores, *product placement* y cuentas *Premium* que prometen una mejor experiencia al disfrutar la navegación en dichas plataformas. Hasta este punto, el crecimiento del *Streaming* permitió que para el año 2012, el consumo número uno de obras musicales, audiovisuales y cinematográficas se diera no de la venta de soportes físicos en tiendas tradicionales, ni de acudir a las salas de cine a disfrutar una casual velada en compañía de palomitas, sino de suscripción a plataformas de retransmisión o consumo gratuito de aplicaciones, software y portales; quizá el cambio generacional y la preferencia que tienen nuevos sectores de consumidores, es la fórmula del éxito detrás de las plataformas antes mencionadas.[29]

A pesar del éxito que tiene el *Streaming* en nuestros días, parece insuficiente para un sector de cibernautas que consideran ociosa la falta de portabilidad de dichas obras musicales y audiovisuales, máxime que la aparición de las modalidades Premium en los portales de referencia, generó pobrísimas experiencias en el modo estándar o "visitante", entre anuncios obligatorios, bibliotecas digitales restringidas y consumo de datos (Internet portable) innecesarios; situación que no todos los internautas aceptaron de buena forma y, contrario a lo esperado, no sólo evitaron adquirir las cuentas Premium, sino que abandonaron dichas plataformas hacia *el lado oscuro*

[29] En el año 1998 Netflix ya comenzaba a generar propuestas de valor al mercado del *Streaming* en tratándose de obras cinematográficas y audiovisuales, lo cual hizo pensar que fue el factor principal para la desaparición de ofertas de rentas domésticas como *Blockbuster*, sin embargo, estudios financieros y de mercado han demostrado que el declive del gran coloso del video VHS y DVD, comenzó mucho antes, aproximadamente en el año de 1995. Para el año 2005 los números que reportaron Netflix y Blockbuster eran similares, sin embargo, desde 1998 hasta el 2012 la plataforma de *Streaming* contó con estabilidad financiera, comercial y posicionamiento líder en el mercado, en tanto que *Blockbuster* demostró pérdidas significativas, sobre todo en el año 2004 cuando reportó pérdidas de casi 1200 millones de dólares, frente a los números ganadores de Netflix, con sumas de 22 millones de dólares. Top Accounting Degrees. *Netflix Vs Blockbuster*. http://www.topaccountingdegrees.org/netflix-vs-blockbuster/ Consultado en línea el 24 de agosto de 2017.

de la fuerza. Así, plataformas como *Youtube-mp3, Mp3skull.com, Stream Ripper y* otros proveedores de servicio *Stream Ripping* brindaron a los usuarios una experiencia *ad hoc* a sus necesidades: portabilidad, interoperabilidad y manipulación en entre formatos, extensiones y calidad de las obras artísticas cuya distribución se conminó exclusivamente a portales legales. Inicialmente, el *Stream Ripping* permite al usuario tomar el URL de un portal legal -como Youtube-, copiarlo dentro del portal ilegal y descargarlo en la extensión que más se adecua a las necesidades y capacidad de almacenamiento del usuario, de esta forma adquiere un archivo ilegal y una reproducción no autorizada de la obra audiovisual, musical o cinematográfica para ser "consumida" en el dispositivo portátil o personal de su preferencia.

Empero, toda esta operación es ilegal a prima facie: i) toda vez que esto atenta contra el derecho moral de integridad, ya que la obra original que se ha cargado en el sitio legal, se mutila, transforma y modifica bajo el capricho del usuario; ii) viola el derecho moral de divulgación, ya que el autor cuenta con la prerrogativa de decir las modalidades, plataformas y características con las que se da a conocer su obra, siempre en beneficio de la difusión de su composición, lo cual no ocurre en la especie; por último, iii) atenta contra el autor o el titular de los derechos patrimoniales de distribución, reproducción, explotación y transmisión, lo que impide obtener el pago de regalías –irrenunciables- que por ley, uso y explotación le pertenecen a sus titulares.

¿Son legales los sitios de Stream Ripping?

La Oficina de Propiedad Intelectual del Reino Unido define a esto, como los servicios que "proporciona cualquier sitio, programa de cómputo o aplicación que provee a los usuarios la facultad de descargar contenido sin permiso, *por lo tanto ilegal*, desde un servicio de transmisión a cargo de terceros, para ser usado sin conexión".[30] Al parecer de quien escribe, el argumento es poco sólido para sostener la automática ilegalidad de dichas plataformas, ya que en términos de la fracción IV, del artículo 148 de la Ley Federal del Derecho de Autor (México), tenemos facultad de utilizar obras literarias artísticas y literarias ya divulgadas, asimismo, reproducirlas por una sola vez, y en un solo ejemplar, para uso personal y privado siempre que esto ocurra sin fines de lucro.

[30] INTELLECTUAL PROPERTY OFFICE & PRS for Music. *Stream-Rippin: How it works and its role in the UK music piracy ladscape.* Reino Unido. Julio de 2017. Consultado en línea el 25 de agosto a través del vínculo https://s3.amazonaws.com/documentos-ia/pdf/KANTAR_E_INCOPRO_STREAM-RIPPING_REPORT.pdf El texto original dicta: "…any site, software program or app which provides users with the ability to download content without permission, and therefore illegally, from a third-party Internet stream which can be used offline"

Por otro lado, el Convenio de Berna para la protección de las Obras Literarias y Artísticas (administrado por la Organización Mundial de la Propiedad Intelectual desde su concepción en París el 9 de septiembre de 1886 [más sus diversas enmiendas]), brinda la regla de los Tres pasos, a saber, los diversos 10 y 10 bis de dicho Tratado Internacional, permiten la libre utilización de la obra en algunos casos, siempre que: i) Se cite la fuente, ii) Sea con fines de ilustración o enseñanza y iii) Se mencione la fuente y el autor. Es decir, existen apartados normativos que podrían defender loablemente un argumento a favor de la existencia del *stream ripping*, sobre todo en tratándose de copias privadas y de uso personal con fines de enseñanza, crítica o periodismo.

A priori, las plataformas que señala el estudio británico únicamente brindan el mecanismo auxiliar para la comisión de la conducta del cibernauta que, *a posteriori*, podría generar la conducta ilícita o ilegal, siempre que no se realice en los términos de lo dispuesto en los preceptos antes invocados. Pero, ¿dichos ordenamientos son suficientes para defender el uso de estas plataformas? La respuesta parece ser no, toda vez que, si bien es cierto existen facultades para reproducir, por una sola vez y con uso personal ciertas obras artísticas, no menos cierto es que existen prerrogativas de orden moral que se ven afectadas con esta conducta (divulgación e integridad); no sólo por las modificaciones que sufre la obra protegida al ser víctima del proceso del *Stream ripping*, sino por la evidente alteración de la fuente de procedencia de la "copia" no autorizada que se produjo con dicha conducta.

Por otro lado, aquellas plataformas que brindan el servicio de *streaming ilícito* violan las políticas y términos de los sitios con la legítima titularidad de la biblioteca multimedia, asimismo, ofrecen espacios publicitarios debido al amplio tráfico de datos en sus portales, de tal suerte que se acredita el lucro indirecto de su actuar. De esta forma, es que se logra vincular y responsabilizar sobre las ilegales y no autorizadas reproducciones (retransmisiones) a los portales que ofrecen dicho servicio.

Criterios internacionales parecen sostener dicha postura. Tan sólo en enero de 2016, un juez federal de los Estados Unidos de América, condenó a *Mp3skull.onl* pagar la cantidad de 22 millones de dólares a favor de los autores y titulares de derechos patrimoniales por concepto de indemnización, adicional a la desaparición (*shut down*) del sitio para descarga libre e ilegal de música;[31] en septiembre de ese mismo año, compañías discográficas de Estados Unidos y Reino Unido hicieron lo propio en contra de Youtube-mp3.org.[32]

[31] KARP, Hannah. *Music Industry's Latest Piracy Threat: Stream Ripping*. The Wall Street Journal. Estados Unidos de América. Septiembre 12 de 2016. Puede consultarse el artículo completo –previo pago de suscripción-, a través del vínculo https://www.wsj.com/articles/music-industrys-latest-piracy-threat-stream-ripping-1473718919 visto el pasado 22 de agosto de 2017.

[32] Techbit. "Enfrenta Youtube.mp3 acciones legales a nivel internacional". *El Universal*. Septiembre de 2016, México. Pude consultar la nota completa a través de http://www.eluniversal.com.mx/articulo/

Para el Reino Unido la piratería digital se ha convertido en un tema relevante, que los llevó a solicitar el estudio citado párrafos anteriores, no sólo a su oficina de Propiedad Intelectual, sino a INCOPRO y KANTAR, lo que tuvo origen a un informe sobre el estado que guardan las obras y su explotación ilegal. Por ahora, se confirma que al menos el 57% de la población adulta usa servicios de transmisión ilegal y que el *stream ripping* constituye la principal causa de violaciones en materia de derechos de autor de aquel territorio, con el escandaloso número de 68.2%. Pronto la piratería digital rebasará ordenamientos como nuestra Ley Federal del Derecho de Autor, el Convenio de Berna y quizá, hasta la famosa *Digital Millennium Copyright Act;* ello hace prudente aseverar que debemos mirar hacia convenios sobre cibercriminalidad como el Convenio de Budapest, que brindan un panorama mejor preparado para enfrentar los retos de nuestro ciberespacio.

VII. 5 Solución de controversias entre Marcas y Nombres de Dominio

El 4 de junio de 2014, la Corporación de Asignación de Nombres y Números de Internet (en adelante "ICANN") liberó el dominio global ".futbol". Ahora las personas físicas o morales relacionadas con el mundo del soccer o interesadas en ser identificadas con una reputación digital vinculada al mundo del balón pie, son capaces de obtener un nombre de dominio que contenga su alias, denominación o referencia, más el sufijo ".futbol". Esto ocurrió en el marco del mundial de fútbol de Brasil 2014, organizado por la FIFA ™. Dentro de las selecciones que brindaron una actuación destacada en el certamen, se encontró la española, también conocida como "La Roja" y el mundo lloraba el retiro como seleccionado de Iker Casillas, uno de los grandes arqueros que ha defendido la casaca Ibérica. Derivado del lanzamiento del dominio global, el evento deportivo que ocurría y el impacto mediático que existió alrededor de la selección representativa de España, hubo unos cuantos "oportunistas" que compraron dominios como "Laroja.futbol" e "Ikercasillas.futbol".

Esto no sólo ocurrió con estas dos populares compras, sino que afectó a otros jugadores como "cristianoronaldo.futbol" y "lionelmessi.futbol"; todos ellos adquiridos por ilegítimos usuarios que esperaron con atención la oportunidad. A nivel de registro de marcas cada uno de estos exitosos futbolistas, así como las selecciones afiliadas a la Federación internacional, cuentan con una interesante lista de activos intangibles consistentes en los signos distintivos que, conforme a ley, los representan en el mercado, tanto de productos deportivos, ropa de moda y diversos contratos

techbit/2016/09/28/enfrenta-youtubemp3-acciones-legales-nivel-internacional visto el pasado 25 de agosto de 2017.

comerciales en los cuáles son utilizados para elevar las ventas de bienes o servicios;[33] sin embargo, la estrategia de estos deportistas así como las Federaciones nacionales no han ocupado su atención al complejo mundo de la adquisición de los nombres de dominio, que por su *propia y especial naturaleza* han generado un hueco legislativo con el que se enfrenta la propiedad industrial y que no en todos los sistemas jurídicos se ha sabido abordar de la mejor manera; tal como ocurre con el caso mexicano.

A diferencia del avance legislativo que han tenido otros países y uniones económicas como lo es la Unión Europea, en México no se ha determinado -en derecho positivo local- un concepto absoluto que permita calificar los nombres de dominio (en adelante DNS por sus siglas en inglés, *domain name system*) y darles una posición jerárquica respecto de los títulos de exclusividad que se otorgan en derecho marcario. Es decir, no contamos con un criterio que determine el derecho de preferencia del que goza un titular de marca respecto del uso exclusivo de su signo distintivo y la probable compra de un nombre de dominio que pudiere generar confusión entre el consumidor promedio que navega en la red de redes y que conoce el producto, bien o servicio fuera de Internet. Para empezar, hay que destacar que una **marca** es todo signo visible que distingue productos o servicios de otros de su misma especie o clase en el mercado,[34] sobre la cual, el Estado otorga un derecho de uso exclusivo mediante su registro ante la autoridad competente, en el caso mexicano ocurre ante el Instituto Mexicano de la Propiedad Industrial –registro con efectos constitutivos- siempre que se cumplan los requisitos de forma y fondo.

Por otro lado, la adquisición de un DNS brinda un derecho de propiedad que se adquiere por una operación comercial, que no genera exclusividad y que podría considerarse un **signo distintivo de facto.** Bien podría asumirse que los límites de los artículos 87 y 88 de nuestra Ley de Propiedad Industrial, pudieren permitir la explotación de una marca a nivel de DNS, sin embargo, existen 2 conductas en el ciberespacio que –a parecer del autor- complican el respeto del derecho marcario entre los internautas:

1. Impera el principio de *prior in tempore, potior in iure*.- La compra de espacios en la red y las distintas operaciones de compraventa y subasta que se ejecutan, genera una compleja tarea de regulación o concentrado de "directorios registrales" de DNS que pudiere impedir la violación a derechos morales de

[33] En el año 2016, una de las marcas deportivas mejor valoradas a nivel internacional es "Beckham ™" con un valor de 1,000 millones de dólares, después de que el exitoso futbolista se convirtiera en embajador benéfico de UNICEF. Este dato se aportó por analistas de ***London Business School***. ESTEVEZ, María. "El valor de la marca Beckham se dispara hasta los 1.000 millones de euros". *ABC*. Gente y estilo. Consulta en línea a través de http://www.abc.es/estilo/gente/abci-valor-marca-beckham-dispara-hasta-1000-millones-euros-201601140020_noticia.html

[34] Artículo 88 de la Ley de Propiedad Industrial. Consultada en línea el 21 de febrero de 2017 a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/ref/lpi.htm

propiedad industrial. La consultora española *ELZABURU* rescata de la práctica jurídica este principio y lo define como "***First come, first served".*** El primero que llega se queda con el nombre de dominio[35].

2. *Cybersquatting*/ Ciberocupación.- Según lo define la OMPI, en el Informe final sobre el *Proceso de la OMPI relativo a los nombres de dominio de Internet* se puede considerar como el "registro abusivo, deliberado y de mala fe de un nombre de dominio en violación de los derechos de marcas de producto y de servicio". En el universo de piratería digital, existen un grupo de cibernautas que ejecutan la conducta conocida como *warehousing* que "implica el registrar una colección de nombres de dominios con la intención de vender los registros a los titulares de las marcas".[36] El Director General Adjunto de la OMPI, Francis Gurry, afirmó que para 18 de febrero de 2005, la Organización resolvió el 80% de los casos de reclamación a favor del titular de la marca[37] conforme a la Política Uniforme de Solución de Controversias en materia de Nombres de Dominio (en adelante "Política Uniforme" o "UDRP/ *Uniform Dispute Resolution Policy*").

Derivado del Proceso de la OMPI anteriormente citado, se determinó que la ICANN –constituida el 18 de septiembre de 1998- sería administrada en adelante por la Organización Mundial de Propiedad Intelectual, y se pactó la Política Uniforme, misma que se ha adecuado para su debida ejecución en cada país; verbigracia, en México contamos con la Política de solución de controversias en materia de nombres de dominio para ".MX" (en adelante "LDRP.mx").[38] Con la colaboración entre diversas organizaciones, así como la construcción de aparatos normativos, parece ser que hemos encontrado la panacea de solución de conflictos entre titulares de marcas e ilegítimos propietarios de signos distintivos en forma de DNS, sin embargo, esto no resuelve el paradigma tradicionalista que pudiere permitir a las marcas abandonar, como caso de excepción, el principio de territorialidad en tratándose de su explotación digital.

[35] SAN MARTIN, José Ignacio. *Marcas y nombres de dominio: solución de controversias*. ELZABURU. Abril de 2016. Consulta en línea a través del vínculo http://www.oepm.es/export/sites/oepm/comun/documentos_relacionados/Ponencias/101_03_II_Jornadas_Sobre_Propiedad_Intelectual_e_Industrial.pdf

[36] WIPO Internet Domain Name Process. *La gestión de nombres y direcciones de Internet: cuestiones de Propiedad Intelectual* "Informe Final sobre el Proceso de la OMPI relativo a los Nombres de Dominio de Internet" de 30 de abril de 1999. Consultable en línea, a través de http://www.wipo.int/amc/es/processes/process1/report/finalreport.html Visible el día 21 de febrero de 2017.

[37] Puede consultar la nota íntegra a través del vínculo http://www.wipo.int/pressroom/es/prdocs/2005/wipo_upd_2005_239.html. Revisado el 19 de febrero de 2017

[38] Véase http://www.wipo.int/amc/es/domains/cctld/mx/ Consultado el 21 de febrero de 2012

Por lo que refiere a la aplicación de la LDRP.Mx –en ausencia de derecho positivo local- se encuentran casos recientes de éxito ante la OMPI, en los cuáles se resolvió la cesión de los derechos del DNS a favor del titular del registro marcario, tales como: i) TV Transmisiones de Chihuahua, S.A. de C.V. contra Javier Carrillo Ramírez por el uso de **izzipaquetes.com.mx**[39], ii) NIKE, Inc. & Nike Innovate C.V. contra Jesús Navarro Saracibar por el uso de **nike.mx**[40] y, iii) Licensing IP International S.A.R.L. contra Jesús Navarro Saracibar por el uso de **pornhub.com.mx, redtube.com.mx y youporno.com.mx**. En los últimos escenarios, el experto panelista de la OMPI tuvo por acreditada la mala fe con la cual se condujo "Jesús Navarro Saracibar/ el Titular", asimismo, tomó en consideración los diversos procesos sobre uso ilegítimo que se han presentado en contra del mismo, acreditando así, la conducta de *ciberocupación* en que ha incurrido el demandado. Tales aseveraciones, llevaron a que el titular transfiriera los DNS a favor del promovente, propietario legítimo de la marca.

A pesar de estos esfuerzos institucionales y normativos, aún se presentan escenarios sin respuesta absoluta que genera incertidumbre entre los usuarios al momento de pretender usar su marca en la web. En principio, es meritorio destacar que las resoluciones que emite el experto de la OMPI en términos de la Política Uniforme o la LDRP.Mx (léase "Política Uniforme Local"), sólo vincula a los agentes registradores que son miembros de la ICANN; es decir, por lo que refiere a los proveedores del servicio de generación de DNS y *hosting*, únicamente se puede exigir el cumplimiento vinculante respecto de aquellos prestadores que se encuentren dentro de los Estados miembros de la OMPI y que se encuentren dentro de la lista de entidades registradoras acreditadas por la ICANN.

A *contrariu sensu* las promociones interpuestas en contra de registradores que no cumplan con estas características –no pertenezcan a la ICANN-, no podrán ser llamadas a este proceso y, en caso de conseguirlo, la resolución emitida no les será vinculante. Por otro lado, la OMPI pone a disposición de los promoventes, una lista de expertos autorizados para emitir resoluciones que resuelvan este tipo de controversias, sin embargo, los aranceles por la intervención de estos oscila entre los 3200 y 5800 euros, lo que podría complicar el bolsillo de algunos solicitantes; empero, el recuperar un DNS estratégico para nuestra marca por este medio, puede presentar ahorros de hasta un 40%, respecto de cualquier negociación realizada sin el apoyo de la OMPI. Por último, hoy en día sólo es permisible llamar a este proceso de solución de controversias, cuando se considere que el titular ilegítimo adquirió el DNS con mala fe, la cual debe ser acreditada ante el experto que resuelve.

[39] Puede consultar la resolución completa a través del vínculo http://www.wipo.int/amc/en/domains/decisions/word/2016/dmx2016-0001.doc Acceso reciente el pasado 20 de febrero de 2017.

[40] Puede consultar la resolnción completa a través del vínculo http://www.wipo.int/amc/en/domains/decisions/word/2016/dmx2016-0002.doc Acceso reciente el pasado 20 de febrero de 2017.

Sin que resulte óbice a lo anterior, se sugieren respetar las siguientes conductas si es que se pretende comprar un nuevo DNS, previa su adquisición:

A) Revisar la presencia de la entidad registradora (*proveedor de servicio de hosting)* en el listado que publica ICANN a través del portal http://www.icann.org, que precisa los organismos acreditados y que sujetan su actuar a las reglas de OMPI.

B) Realizar una búsqueda del DNS cuyo registro se pretende, no sólo como signo distintivo que brinde exclusividad desde el universo de propiedad intelectual (V.gr. Marcanet), sino implementar una búsqueda previa a través del registrador o con la herramienta UWhois, consultable en línea en http://www.uwhois.com. Esto le permitirá conocer si un nombre de dominio ya ha sido registrado, que entidad registradora participó de la operación y, en el mejor de los casos: i) Fecha de registro, ii) Fecha de expiración y, iii) Titular del DNS.

C) Tal como se ha señalado con anterioridad, debe evitar prácticas de cybersquatting que coloquen a sus signos distintivos (marca y DNS) en una posición jurídica inestable que podría considerarse de mala fe y, por ende, generar sanciones administrativas y penales según la legislación territorialmente aplicable. Resulta meritorio afirmar que no sólo podría activar alguna hipótesis infractora en materia de propiedad industrial, sino que dicha conducta podría llevar a la reclamación de daños y perjuicios de titulares legítimos (legitimados).

   a. Verifique en el portal nacional de la entidad gubernamental registradora si el DNS cuya adquisición pretende, no cuenta con un signo distintivo similar o igual que pudiere generar conflictos y confusión al consumidor promedio. En México puede hacerse a través del portal http://marcanet.impi.gob.mx/marcanet/ y a nivel internacional, por medio del portal que administra la OMPI http://ecommerce.wipo.int/

D) Evitar DNS que incluyan en su construcción elementos que se pudieren considerar genéricos o, que de forma evidente, impliquen controversias por contener: i) elementos geográficos, ii) nombres de personas famosas, iii) acrónimos de organizaciones o empresas notoriamente conocidas.[41]

E) En caso de sufrir de ciberocupación/ocupación ilegítima buscar el proceso de autocomposición con el titular del DNS que pudiere aparecer en la búsqueda particular que se realice a través de UWhois. En caso de negativa o existencia de mala fe, acudir a la OMPI a ejercer derechos de preferencia, exclusividad y legitimidad conforme lo dicta la Política Uniforme de Solución de

[41] Se pueden encontrar las recomendaciones que realiza la OMPI a través del vínculo http://www.wipo.int/sme/es/e_commerce/domain_names.htm. Consultado en línea el 20 de febrero de 2017.

Controversias. De ahí la importancia de la contratación de entidades registradoras certificadas, como se indicó en el inciso A) anterior. Puede consultar el proceso íntegro en http://arbiter.wipo.int/domains/

El mundo deportivo nos ha abierto la puerta para esta breve intervención literaria, en la cual podemos citar casos de éxito como el ocurrido en el Caso D2015-1659, a través del cual el Club Atlético Madrid recuperó el nombre de dominio "atletico-madrid.com", después de su registro ilegítimo en el año 2000. Esta controversia se resolvió gracias a la aplicación de la UDRP ante la OMPI.

Así las cosas, se puede concluir que hoy en días existen mecanismos –internacionales- de solución de conflictos entre marcas y DNS, sin embargo, estos aún no resuelven de forma preventiva la protección de los derechos morales a favor de los titulares de registros marcarios. Por ahora, parecería que la OMPI nos ha otorgado mecanismos mínimos para emprender el *vuelo marcario* en el ámbito digital, así como Dédalo lo hiciere con Ícaro, sin embargo, por ahora parecería que nuestras *alas* (marcas), aún se pudieren derretir ante el intenso calor de la red.

VIII
CAPÍTULO

El valor jurídico del Clic

La dinámica social y la evolución del *Homo Videns* han llevado a los seres humanos a adaptar su comportamiento y rutinas bajo dos modalidades fundamentales: *online* y *off line*; sin embargo, gran parte del tiempo que un ciudadano moderno permanece despierto –me atrevería agregar "en vida"- lo invierte en la red de redes, lo que ha dotado de relevancia equitativa lo que acontece frente al computador, respecto de cualquier conducta que se ha estudiado desde una perspectiva tradicionalista.

Esta afirmación adquiere sentido si recuperamos los datos aportados por la Asociación de Internet MX, la cual afirma que los mexicanos pasan al menos 8 horas de su día frente a una computadora y conectados a la red, en ese mismo canal tecnológico, entre 2014 y 2015 el *e-commerce* reportó un crecimiento de 59% lo que implica un valor de 257 mil millones de pesos, y para el 2016 el valor de venta aumentó un 27% con la cantidad de 326 mil millones de pesos.[1] Según la firma *Vesta Corporation,* México es uno de los países que son líderes en el ámbito del comercio electrónico, por lo que resulta el escaparate perfecto para la implementación de protocolos para evitar fraudes, así como el escenario ideal para la proliferación de hackers.[2] Tom Byrnes y Daniel Lee, Director de Marketing y Vicepresidente de *e-commerce*

[1] LÓPEZ, Yair. "Las Empresas pierden hasta 10% de sus ventas por fraude electrónico". *CNN México*. Tecnología. Miércoles 19 de julio de 2017. Visto el 27 de noviembre de 2017 a través del vínculo http://mexico.cnn.com/tecnologia/2017/07/19/las-empresas-pierden-hasta-10-de-sus-ventas-por-fraude-electronico

[2] Según el Diccionario de Inglés de Oxford, se le puede definir como la persona que usa su habilidad con las computadoras para tratar de tener acceso no autorizado a los archivos informáticos. Oxford University Press. "hacker". Oxford Dictionaries, Oxford Dictionaries. 2010.

de Vesta, respectivamente, afirman que su empresa es la única en el mundo capaz de evitar que esos fraudes afecten a los consumidores de sus clientes, sin embargo, eso no evita que exista la aparición de nuevas conductas para perjudicar la credibilidad del comercio electrónico e impactar sus ventas en márgenes millonarios; verbigracia, gracias a delitos cometidos en Internet como robo de identidad [Phreaking (especialistas en mecanismos para vulnerar la seguridad de los sistemas telefónicos), amenazas [Fraudes en e-commerce (portales de subasta)], fraudes en línea (compras en tiendas virtuales), Clonación de tarjetas de crédito, robo de información [Carding (utilización ilegal de tarjetas de crédito)], traspasos ilegítimos [Phishing (correos falsos para robar datos de usuarios) y *Click-Bait* engañosos;[3] sitios como *Spotify* o *Netflx* presumen pérdidas desde el 8%, en tanto que existen pérdidas globales entre los 7 y 12% para aquellos proveedores que han aventurado su camino al contacto digital con sus clientes. Parecería entonces, que la confianza en los consumidores digitales no tiene obstáculo frente a las probables amenazas que existen en la web, ya que las pérdidas por las conductas antes descritas en la mayoría de los casos encuentran soluciones transparentes a través de la *Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (México),* empero, en opinión de expertos en la materia como Mario Reynoso (Director general de Gaudena.com) la solución no se encuentra en la estadística, sino en la mejora regulatoria de dichas conductas y de las empresas que hacen de su fin primordial el e-commerce.[4] Bajo ese intrincado camino, parecería que la respuesta se encuentra en establecer protocolos, normas oficiales y leyes suficientes para limitar el funcionamiento de las plataformas que operan a través del comercio electrónico. Tan sólo el 15 de noviembre de 2017, en México, el pleno de la Cámara de Diputados aprobó reformas a la Ley Federal de Protección al Consumidor, por las cuáles incorporó a dicha ley el artículo 76 BIS, para especificar que el proveedor que ofrezca, comercialice o venda bienes, productos o servicios utilizando medios electrónicos, ópticos o de cualquier otra tecnología deberá guiar su actuar a los términos de la Norma Mexicana que se expedirá para tal efecto; sin embargo, a parecer de quien emite el presente escrito, el mercado que en el 2017 representara más de 329,000 millones de pesos y 2% del Producto Interno Bruto,[5] no puede simplemente rendir honores a reglas jurídicas de nivel jerárquico

[3] CORELLA RAMÍREZ, David, et al. *Modalidades de Fraude en la compra-venta de artículos de aplicaciones electrónicas*. Universidad Autónoma del Estado de Hidalgo. Boletín ICEA Número 9. Disponible en línea a través del vínculo https://www.uaeh.edu.mx/scige/boletin/icea/n9/e1.html

[4] ESCAMILLA, Viridiana. "¿Quién pierde con los fraudes en e-commerce?" Portada. Emprendedores. *FORBES MÉXICO*. Agosto 1 de 2013. Disponible a través del vínculo https://www.forbes.com.mx/quien-pierde-con-los-fraudes-en-e-commerce/

[5] MONROY, Jorge. "Aprueban que SE emita NOM para regular ecommerce". *El Economista*. México. 15 de noviembre de 2017. Visto el 27 de noviembre de 2017 a través del vínculo https://www.eleconomista.com.mx/empresas/Aprueban-que-SE-emita-NOM-para-regular-ecommerce-20171115-0049.html

inferior como lo son las Normas Oficiales Mexicanas, a su vez, los Estados deberían optar por instituir y apoyar procesos de certificación de las empresas tales como *PCI y* cumplimiento de ordenamientos de virtual aplicación internacional como la Ley Sarbanes-Oxley. Estos estándares internacionales deben su existencia comercial a la especialización del blindaje corporativo para la protección de las operaciones que ocurren en el ámbito digital, no sólo por lo que refiere al negocio jurídico, sino a la protección de datos bancarios, contabilidad pública y datos personales. Hasta ahora, el nuevo siglo dicta una corriente sumamente legislativa, en la que los abogados pretenden insertar normas de derecho al complejo mundo de la web.

El objeto del presente capítulo será estudiar los casos legislativos más exitosos en materia de comercio electrónico, así como realizar las distinciones adecuadas respecto del contrato informático, electrónico y digital, así como el efecto de los novedosos *Click Wrap Agreements*. Seguido a ello, brindaré un breve análisis sobre criterios trascendentales que se han emitido en términos de la Ley Modelo Sobre Comercio Electrónico aprobada por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional; me referiré a los derechos de consumidor en la web y, por último, realizaré unas breves precisiones sobre las *criptomonedas*, desde el punto de vista jurídico.

VIII. 1 Comercio Electrónico

El 16 de diciembre de 1996 se celebró la 85ª edición plenaria de la Organización de las Naciones Unidas, en la cual se aprobó la resolución por la Asamblea General en la cual se incluye la base del informe emitido por Comisión de las Naciones Unidas para el Derecho Mercantil Internacional: 51/62 Ley Modelo[6] Sobre Comercio Electrónico aprobada para la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. En ésta se recordó el humilde origen de la Comisión -17 de diciembre de 1966- con la finalidad de fomentar la armonización y la unificación progresiva del derecho mercantil internacional, sobre todo, con la meta de colocar en similitud de condiciones a países en desarrollo en el campo del comercio internacional; esto pareció ser sencillo ante la homogeneidad internacional de las transacciones

[6] En términos de la Organización de las Naciones Unidas, el concepto "ley modelo" debe comprenderse bajo la siguiente acepción: "Las disposiciones de una ley modelo se preparan con el fin de ofrecer una pauta a los legisladores para que se planteen la posibilidad de incorporar la ley modelo a su derecho interno. Dado que los Estados que promulgan legislación basada en una ley modelo pueden actuar con toda flexibilidad y apartarse del texto de la misma…Para determinar la diferencia existente entre una ley modelo y un texto legislativo adoptado sin ajustarse totalmente a ella, habría que estudiar la legislación de cada Estado." CNUDMI. *Situación actual Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996).* Visto el 27 de noviembre a través del vínculo http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1996Model_status.html

comerciales que ocupan el intercambio electrónico de datos y otros medios de comunicación; al respecto, la Ley Modelo UNCITRAL responde a la necesidad de otorgar un valor jurídico a los registros computarizados que guardan actos de comercio, no sólo con fines procesales, sino con la intención de invitar a las naciones a reconocer la celebración de actos jurídicos que generan consecuencias de derecho, independientemente que estos no fueren celebrados con papel y tinta, tal como ocurría anteriormente.

Así las cosas, la ONU determinó la conveniencia de contar con un mecanismo internacional que permitiera la celebración del comercio electrónico y que éste fuere reconocido por los Estados en sus diversos sistemas jurídicos, sociales y económicos. En ese tenor, la Ley Modelo que nos ocupa no sólo tiene como misión el reconocer el valor jurídico del comercio electrónico y cada uno de los conceptos informáticos que se involucran en su celebración, sino provocar la modificación legislativa de las naciones frente a la creciente tendencia de actos digitales.

Casos de éxito que me gustaría invocar[7] son los ocurridos en países como Antigua y Barbuda, Bangladesh, Canadá, Colombia, Kuwait, Malí, México, Francia[8], España[9] y Estados Unidos de América[10], cuyos procesos legislativos han permitido la incorporación de los conceptos de la Ley UNCITRAL en beneficio de los negocios jurídicos electrónicos, al tomar como base de sus leyes la Ley de la ONU, así como los principios en que se basa. Actualmente, esta ley modelo cuenta con 150 países ratificantes, de los cuales, al menos 71 han adoptado sus normas de derecho a los principios contenidos en el marco legislativo multicitado. Sin embargo, ¿esto qué significa para el mundo *online*? Tal como señalé en el primer capítulo de la presente obra, el comportamiento de los usuarios muestra una clara tendencia a invertir gran parte de su tiempo despierto en la red de redes, ello tiene como consecuencia la generación de bienes y la obtención de servicios de carácter informático, que hasta

[7] Fuente: ONU/ Supra. Cit.

[8] Puede consultar la Ley 2000/230 de 13 de marzo 2000, por la que se reforma el Código Civil Francés en materia de prueba de las obligaciones, así como la reforma 2004/575 de 21 de julio de 2000, por la que se prescribe el poder vinculatorio de la firma digital. Puede consultar el texto íntegro a través del vínculo https://www.legifrance.gouv.fr/content/download/1966/13751/.../Code_41.pdf

[9] El 12 de julio de 2002, se publicó la Ley 34/2002 para regular los servicios de la sociedad de la información y comercio electrónico, por la jefatura del Estado. Puede consultar el texto íntegro de la ley a través del vínculo https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758 Visto el 29 de noviembre de 2017.

[10] Estados Unidos de América cuenta con la Ley de Transacciones Electrónicas, aprobada por Decreto en todos los Estados, en julio de 1999. Fuente: LÓPEZ VARAS, Mariana. *Regulación Jurídica de la Contratación Electrónica en el Código Civil Federal*. Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios. Primera Edición. México, Septiembre 2010. Puede consultar el texto íntegro a través del vínculo http://www.infoem.org.mx/sipoem/ipo_capacitacionComunicacion/pdf/pet_tesis_001_2009.pdf Visto el 29 de noviembre de 2017.

ahora, parecerían no estar enteramente regulados por las diversas legislaciones alrededor del mundo, lo cual también complica su estudio desde la semántica legislativa.

Desde un primer peldaño metodológico, se debe precisar que la legislación que invocamos, pretende regular el comportamiento de los usuarios en la capa superficial de la web, es decir: "Internet"[11]. Al respecto, la Conferencia de la Haya de Derecho Internacional privado, define a éste como "una red de redes de ordenadores, los cuales se encuentran interconectados entre sí por línea de telecomunicaciones, permitiendo de este modo llevar a cabo una serie de actividades (sic)". Se destaca de la anterior definición, que en dicha conferencia se utiliza por primera vez –al menos en un discurso jurídico- el término "actividad humana <<off-line>>".[12] Por su parte, la Corte Suprema de Justicia de los Estados Unidos lo define como "una red internacional de computadoras interconectadas, que permite comunicarse entre sí a decenas de millones de personas, así como acceder a una inmensa cantidad de información en todo el mundo"[13]. Por otro lado, la Ley Modelo prescribe su campo de aplicación a las actividades "comerciales", lo que a su vez nos pudiera brindar una apreciación sobre su significado:

> El término comercial deberá ser interpretado ampliamente de forma que abarque las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las operaciones siguientes: toda operación comercial de suministro o intercambio de bienes o servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; de factoraje ("factoring"); de arrendamiento de bienes de equipo con opción de compra ("leasing"); de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; de inversión; de financiación; de banca; de seguros; todo acuerdo de

[11] El Maestro Reyes Kraft define a Internet como un "canal mundial de telecomunicaciones informáticas…", además, califica tres características fundamentales de dicha red: "…consisten en que se trata de una red **distributiva** (no cuenta con un depósito central de información o de control, sino que está compuesto por una serie de computadoras host o anfitrionas que están interconectadas, cada una de las cuales puede ser *accesada* (sic) desde cualquier punto de la red en que el usuario de Internet se encuentre), **interoperable** (utiliza protocolos abiertos, de manera que distintos tipos de redes e infraestructura puedan ser enlazados, permitiendo la prestación de múltiples servicios a una diversidad de usuarios a través de la misma red. En este sentido, la interoperabilidad con la que cuenta Internet se debe al protocolo TPC/ IP, el cual define una estructura común para datos de Internet, así como para el enrutamiento de dichos datos a través de la red) y que funciona a través de **transferencias de paquetes de información** (mejor conocida como conmutación de paquetes, consistente en dividir la información que se transmite por la red en pequeñas partes o paquetes)." REYES KRAFT. Alfredo A. *La firma electrónica y las entidades de certificación.* Editorial Porrúa. México, 2003.

[12] Conferencia de la Haya de Derecho Internacional Privado, Electronic Commerce and International Jurisdiction – Ottawa, 28/2-1/3/00. Preliminary Document N° 12, Agosto de 2000.

[13] Jane Reno, Attorney General of the United States et al. appellans vs. American Civil Liberties Union, et al., sentencia del 26 de junio de 1997.

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 y marítima o por ferrocarril y carretera.[14]

Dicho concepto resulta consonante con lo prescrito por la legislación mexicana, a través de su Código Comercio, mismo que delimita que "comerciante" será todo aquel que haga del comercio su ocupación ordinaria, además, todos aquéllos que accidentalmente, con o sin establecimiento fijo realicen una operación de comercio. En ese mismo tenor, prescribe que se reputarán como actos de comercio:

Artículo 75.- La ley reputa actos de comercio: I.- Todas las adquisiciones, enajenaciones y alquileres verificados con propósito de especulación comercial, de mantenimientos, artículos, muebles o mercaderías, sea en estado natural, sea después de trabajados o labrados; II.- Las compras y ventas de bienes inmuebles, cuando se hagan con dicho propósito de especulación comercial; III.- Las compras y ventas de porciones, acciones y obligaciones de las sociedades mercantiles; IV.- Los contratos relativos y obligaciones del Estado u otros títulos de crédito corrientes en el comercio (sic); V.- Las empresas de abastecimientos y suministros; VI.- Las empresas de construcciones, y trabajos públicos y privados; VII.- Las empresas de fábricas y manufacturas; VIII.- Las empresas de trasportes de personas o cosas, por tierra o por agua; y las empresas de turismo; IX.- Las librerías, y las empresas editoriales y tipográficas; X. Las empresas de comisiones, de agencias, de oficinas de negocios comerciales, casas de empeño y establecimientos de ventas en pública almoneda; XI.- Las empresas de espectáculos públicos; XII.- Las operaciones de comisión mercantil; XIII.- Las operaciones de mediación de negocios mercantiles; XIV.- Las operaciones de bancos; XV.- Todos los contratos relativos al comercio marítimo y a la navegación interior y exterior; XVI.- Los contratos de seguros de toda especie; XVII.- Los depósitos por causa de comercio; XVIII.- Los depósitos en los almacenes generales y todas las operaciones hechas sobre los certificados de depósito y bonos de prenda librados por los mismos; XIX.- Los cheques, letras de cambio o remesas de dinero de una plaza a otra, entre toda clase de personas; XX.- Los vales u otros títulos a la orden o al portador, y las obligaciones de los comerciantes, a no ser que se pruebe que se derivan de una causa extraña al comercio; XXI.- Las obligaciones entre comerciantes y banqueros, si no son de naturaleza esencialmente civil; XXII.- Los contratos y obligaciones de los empleados de los comerciantes en lo que concierne al comercio del negociante que los tiene a su servicio; XXIII.- La enajenación que el propietario o el cultivador hagan de los productos de su finca o de su cultivo; XXIV. Las operaciones contenidas en la Ley General de Títulos

[14] CNUDMI. *Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996)*. Visto el 21 de noviembre de 2017 a través del vínculo https://documents-dds-ny.un.org/doc/UNDOC/GEN/N97/763/60/PDF/N9776360.pdf?OpenElement

> y Operaciones de Crédito; XXV.- Cualesquiera otros actos de naturaleza análoga a los expresados en este código.[15]

Es decir, la Ley Modelo UNCITRAL pretende invitar a la regulación de los actos de comercio que se celebren en Internet y que se precisan en cada una de las legislaciones locales. Para ello, es imperativo comprender el concepto de "mensaje de datos" como la unidad de medida más elemental que se origina en los actos electrónicos; a saber, la Ley Modelo lo define como "la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares."

Esto es, el mensaje de datos es el contenido, mientras que el continente podría ser un sistema de intercambio similar al correo electrónico, FAX, telegrama, telefax, SMS, inclusive WhatsApp o cualquier sistema de conversaciones (chat). Al respecto, la ONU y su Asamblea general son precisas, al definir en su artículo 5° que no podrá negarse efecto jurídico, validez o fuerza obligatoria a la información, por estar contenida en un mensaje de datos, ni podrá negársele a los archivos adjuntos o texto que vayan vinculados a dicho mensaje de datos (Artículo 6°). Procesalmente, inplica la necesidad de permitir los mecanismos jurisdiccionales suficientes para que los medios de convicción que se contengan en un medio electrónico se puedan ofrecer tal como ocurre con otras pruebas, sin colocar obstáculos procedimentales o de admisibilidad, inclusive, que no se presente el mensaje de datos "original", derivado de la naturaleza *sui generis* que presenta un mensaje de dicha naturaleza, siempre que cumpla con los principios pactados en el apartado 2) del artículo 9 de la propia ley, misma que de tenor literal dicta:

> Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.

Principios que serán estudiados más adelante en el capítulo respectivo, así como los mecanismos de conservación (**conservación forense**) que exige la Ley Modelo.

En términos de la legislación que se invoca, es prudente definir al **comercio electrónico** como el acto que involucra una operación ordinaria o accidentalmente comercial en las que se emplean medios electrónicos, ópticos o cualquier otra tecnología para el perfeccionamiento del acto jurídico, mediante la transmisión de un

[15] CONGRESO DE LA UNIÓN. MÉXICO. *Código de Comercio*. Texto publicado el 13 de diciembre de 1889, cuya última reforma ocurrió el 02 de mayo de 2017. Visto el 27 de noviembre de 2017 a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/3_020517.pdf

mensaje de datos. Por su lado, el Diccionario de Black, lo define como el negocio que se conduce sin la presencia de papel y con base en el uso de equipos electrónicos o digitales.[16]

Dicho concepto debe leerse con prudencia, ya que la acepción que propongo no pretende hacer referencia al objeto del negocio jurídico del que estemos hablando, ya que puede variar en atención de la calidad comercial que pudiere presentarse: i) informático, ii) electrónico o, iii) digital.

Hasta este punto, la legislación que hemos traído al presente texto, nos permite definir al comercio electrónico, sin embargo, ¿pueden celebrarse contratos electrónicos bajo dichas reglas? La respuesta es afirmativa y obvia, a estas alturas históricas y tecnológicas. Según lo prescribe el artículo 11 de la propia Ley Modelo, para que un contrato electrónico se forme y cuente con validez, las partes podrán expresar una oferta y aceptación por medio de un mensaje de datos, asimismo, no podrá negarse validez o fuerza obligatoria a dicho pacto de voluntades por haberse utilizado en su formación un mensaje de datos. Es decir, no podrá negarse formalidad a ningún convenio, ni a la manifestación de la voluntad de las partes por haberse realizado mediante mensaje de datos (artículo 13 Ley Modelo), siempre que se hubiese emitido por un sistema de información programado por el iniciador o en su nombre para que opere automáticamente o bien, por un presentante que pudiere manipular legítimamente dichas plataformas. En ese tenor, se advierte que el documento digital alcanzará validez y eficacia absoluta en tanto cumpla con los requisitos anteriores, sin que resulte necesaria la presencia de una firma. La figura de la "firma" como elemento de validez surge con el derecho moderno, sin embargo, en la antigua Roma –base de nuestro sistema jurídico- no era costumbre firmar los documentos; según señala Gabriel Andrés Cámpoli, la *manufirmatio* (ceremonia de validación del contenido de los documentos) permitía la participación de un fedatario para leer el documento, se desplegada sobre la mesa del funcionario y luego pasaba la mano abierta sobre el "pergamino" en actitud de jurar, posteriormente se escribía el nombre, o se colocaba un par de cruces[17]. Empero, la presencia de un elemento gráfico se adoptó como

[16] *Black's Law Dictionary. What is Electronic Commerce (e-commerce)?* Definición disponible a través del vínculo https://thelawdictionary.org/electronic-commerce-e-commerce/ Cuyo texto original indica: "What is ELECTRONIC COMMERCE (E-COMMERCE)? Business conducted without the exchange of paper based documents through the use of electronic and/or online devices. It includes activities such as procurement, order entry, transaction processing, payment, authentication and nonrepudiation, inventory control, order fulfillment, and customer support. The general public participates in ecommerce, almost unknowingly these days. Ecommerce devices include computers, telephones, fax machines, barcode readers, credit cards, automated teller machines (ATM) or other electronic appliances, whether or not using the Internet."

[17] CÁMPOLI, Gabriel Andrés. La Firma Electrónica en el Régimen Comercial Mexicano. Editorial Porrúa. México. 2004. pág. 3

medio de convicción para acreditar la existencia de consentimiento en el documento, sin que éste resulte indispensable o requisito *sine qua non* para la validez de un contrato.

Tratándose del comercio electrónico si bien es cierto que existen diversas legislaciones en materia de Firma Electrónica, incluyendo la Ley Modelo sobre el Uso de la Firma Electrónica que propone la CNUDMI, no menos cierto lo es, que el artículo 7 de la Ley Modelo que hemos estudiado hasta ahora, propone la eliminación de dicho concepto desde un punto de vista tradicional, en la cual se plasma un elemento gráfico sobre papel, ya que ello podría ser un riesgo para vincular la validez del mensaje de datos a la ratificación a través de dicho mecanismo anticuado de manifestación de la voluntad. Así las cosas, el artículo 7 de la Ley Modelo propone una salida alternativa a la presencia de la "firma" desde un punto de vista tradicional, siempre que se presenten dos condiciones substitutas: i) Se identifique el autor del mensaje de datos y ii) Se confirme que el autor consiente y aprueba el contenido del documento.

En ese tenor lo ha prescrito la legislación española, misma que en su Ley 34/2002 regula el comportamiento de los servicios de la sociedad de la información y de comercio electrónico, que en la parte conducente dicta:

> **[...] Artículo 24. Prueba de los contratos celebrados por vía electrónica.**
>
> 1. La prueba de la celebración de un contrato por vía electrónica y la de las obligaciones que tienen su origen en él se sujetará a las reglas generales del ordenamiento jurídico.
>
>   Cuando los contratos celebrados por vía electrónica estén firmados electrónicamente se estará a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
> 2. En todo caso, el soporte electrónico en que conste un contrato celebrado por vía electrónica será admisible en juicio como prueba documental.

En ese mismo tenor, el artículo 3° de la Ley 59/2003 define a la firma electrónica como "el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante". Preceptos normativos que resultan ilustrativos respecto al cumplimiento de la Ley Modelo, ya que son coincidentes con lo prescrito en el tratado internacional que hemos estudiado, ya que la firma electrónica no cuenta con una estructura rígida, sino un elemento flexible que sólo exige la identificación del iniciador y, en su caso, certeza razonable de la manifestación de la voluntad y, consentimiento.[18]

[18] El Doctor Juan Guadalupe Valencia Monge, nos recuerda que la forma de un contrato electrónico depende de la doctrina sobre el "consentimiento entre no presentes": i) Sistema de la declaración.- Se perfecciona el acto jurídico en el momento que el receptor declara la aceptación de una oferta; ii)

Tema diverso sería la certificación de dichas firmas, en cuyo caso intervienen autoridades o entidades registradoras que permiten la expedición de documentos informáticos que fortalecen el contenido de la firma electrónica, constituyendo una firma electrónica "avanzada" o "certificada". Según la propia legislación española, podríamos definir a un mecanismo a dicho elemento de autenticación como aquella que "permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control".[19]

En ese mismo tenor se ha concebido la Ley Modelo de la CNUDMI sobre Firmas Electrónicas, cuyo artículo 2° define a la firma electrónica como los datos consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, que pueden ser utilizados para identificar al firmante, en tanto que la certificación consiste en un método de confirmación del vínculo entre un firmante y los datos de creación de la firma.[20]

El caso mexicano resulta un paradigma en tratándose del estudio de la firma electrónica y la distinción que existe con la firma digital, el caso medular se presenta en el exitoso Juicio en Línea del Tribunal Federal de Justicia Administrativa, cuya legislación procesal indica que la firma electrónica avanzada –certificada- tendrá los mismos efectos legales que la firma autógrafa e idéntico valor probatorio[21], en tanto que el artículo 22 de los Lineamientos Técnicos y formales para la sustanciación del

Sistema de expedición.- el contrato se perfecciona cuando la aceptación se declara y se envía al oferente; iii) Sistema de recepción.- El acto se perfecciona cuando el oferente recibe la aceptación; y iv) Sistema de la información.- Para perfeccionar el acto se requiere la recepción de la expedición, aceptación y en su caso, que el oferente se dé por enterado de la misma. A parecer de quien emite el presente texto, el tercer nivel de perfeccionamiento resultaría suficiente para dotar e plena validez jurídica a un contrato electrónico. Puede consultar el texto que propine el Doctor Monge en: VALENCIA MONGE, Juan G. *Validez jurídica de los contratos por Internet.* Temas de derecho civil en homenaje al doctor Jorge Mario Magallón Ibarra. Editorial Porrúa. México, 2011. Visto el 29 de noviembre de 2017 a través del vínculo https://archivos.juridicas.unam.mx/www/bjv/libros/8/3861/20.pdf

[19] Ley 59/2003, de 19 de diciembre, de firma electrónica. Publicado en «BOE» núm. 304, de 20 de diciembre de 2003, páginas 45329 a 45343, España. Artículo 3°. Puede consultar el texto íntegro a través del vínculo https://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399

[20] Organización de las Naciones Unidas. *Artículo 2° de la Ley Modelo de la CNUDMI sobre Firmas Electrónicas*. Puede consultar el texto íntegro a través del vínculo http://www.uncitral.org/pdf/spanish/texts/electcom/ml-elecsig-s.pdf visto el 29 de noviembre de 2017.

[21] Congreso de la Unión. *Artículo 58-F de la Ley Federal de Procedimiento Contencioso Administrativo*. México. Última reforma publicada en el Diario Oficial de la Federación el 27 de enero de 2017. Puede consultar el texto íntegro a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPCA_270117.pdf visto el 29 de noviembre de 2017.

juicio en línea[22], distingue 3 requisitos para firmar resoluciones y actuaciones por parte de los Magistrados y Secretarios de Acuerdos: i) Huella digital, ii) Firma Digital y iii) Firma Electrónica Avanzada. De esta forma, se distingue la fuerza jurídica de la firma certificada frente a una firma digital simple, en tanto que la última acude como un elemento gráfico que afecta la *psique* de los particulares con la intención de permitir que viejas generaciones de abogados confíen en la resolución jurisdiccional en su poder, a pesar que la firma electrónica avanzada sea aquella que dote de verdadero poder jurídico a la decisión del Tribunal y la primera, no genere ningún efecto jurídico real.

Así las cosas, resulta adecuado afirmar que un contrato electrónico que cuente con elementos suficientes para acreditar la identidad de las partes, así como su contenido, tendrá por cierta la presencia de la firma digital, sin que sean necesarios mayores elementos de convicción, salvo aquéllos que expresamente requiere la ley, en cuyo caso será necesaria la presencia de una firma electrónica certificada/ avanzada. Empero, la Ley Modelo UNCITRAL reconoce el valor del contrato, con independencia que no cuente con una firma avanzada en tanto se respeten los principios cousagrados en el diverso artículo 7° multicitado, por lo que las legislaciones de los 151 Estados contratantes deberían ser coincidentes con dicha prescripción. Razonamientos jurídicos que podrían sostener la validez y eficacia de cualquier contrato comercial que tuviera su base en correo electrónico, un mensaje de texto (*SMS)* e inclusive aquéllos emitidos a través de redes sociales, toda vez que cada uno de ellos permite identificar debidamente a las partes firmantes e inclusive, cuenta con mecanismos de autenticación sobre el contenido de los mensajes de datos, al cuestionar a los usuarios sobre su voluntad en incógnitas parecidas a: "¿Está seguro de que desea enviar el mensaje?". Sin duda, los medios electrónicos y digitales resultan mecanismos idóneos para manifestar la voluntad comercial en tanto se respeten las reglas que hemos estudiado.

VIII.1.1 Contratos Informáticos, electrónicos y digitales

En palabras del Doctor Julio Téllez Valdés, un contrato informático es un "acuerdo de partes en virtud del cual se crean, conservan, modifican o extinguen obligaciones relativas a los sistemas, subsistemas o elementos destinados al tratamiento sistematizado de la información".[23] En ese tenor, el Doctor Téllez identifica como objeto

[22] Congreso de la Unión. *Artículo 22 de los Lineamientos Técnicos y formales para la sustanciación del juicio en línea*. Publicado en el diario oficial de la federación el 04 de mayo de 2011. Puede consultar el texto íntegro a través del vínculo http://dof.gob.mx/nota_detalle.php?codigo=5188284&fecha=04/05/2011 visto el 29 de noviembre de 2017.

[23] TÉLLEZ VALDÉS, Julio. *Contratos Informáticos*. Contratos, Riesgos y seguros informáticos. Capítulo II. Contratos Informáticos. Universidad Nacional Autónoma de México. México, 1988. Primera

indirecto de este tipo de contratos a los bienes y servicios de naturaleza informática, que no sólo tienen que ver con transferencia de tecnología, sino con la entrega de resultados oportunos a través de la optimización de software y hardware de una empresa. Más allá de la breve definición que nos brinda el Doctor Téllez, no existen mayores elementos que permitan distinguir claramente, al menos en la doctrina, un contrato informático de otros de naturaleza similar, sin embargo, podríamos definirlo como el acuerdo de voluntades por el que se crean o transfieren derechos u obligaciones cuyo objeto indirecto es la automatización de la información mediante la implementación o contratación de servicios tecnológicos que requieren la utilización de programas de cómputo y equipo de cómputo.

En general, un contrato informático podría aplicarse respecto de cualquier máquina cuya funcionalidad sea la automatización de la información. Conforme a dicha definición, el Doctor Julio Téllez concibe dos tipos de contratos informáticos: i) Aquéllos referidos a los bienes (equipos, periféricos, dispositivos, etcétera) y, ii) Aquéllos referidos a los servicios (asistencia, formación, mantenimiento, programas, etcétera).[24]

Tal como se explicará en el capítulo XII de la presente obra, los medios electrónicos y digitales pertenecen a la familia de los medios informáticos. En ese tenor, podríamos afirmar que todo contrato electrónico o digital, por antonomasia pertenece a la familia de los contratos electrónicos, empero, procuraremos puntualizar la naturaleza de cada uno. En ese tenor, José Márquez y Luis Moisset Espanés definen al contrato electrónico como aquel que se perfecciona mediante un intercambio electrónico de datos de ordenador a ordenador. A su vez, existen autores que utilizan indistintamente el concepto de "contrato electrónico" y "contrato informático", como lo es el caso de Claudia Brizzio, quién define a ambos como la operación que se realiza mediante la utilización de algún elemento electrónico, con influencia decisiva, real y directa sobre la formación de la voluntad, el desenvolvimiento, o la interpretación de un acuerdo; específicamente, mediante *EDI*.[25] Conforme a lo anterior, es prudente señalar que los contratos electrónicos son aquéllos que formalizan el consentimiento de las partes involucradas a través de mecanismos electrónicos que no dependen de un sistema digital de transmisión de mensaje de datos, en tanto que los contratos digitales serían aquéllos que se perfeccionan con la manifestación de la voluntad y consentimiento de las partes, a través de medios digitales como lo es las plataformas

edición. Visto el 29 de noviembre de 2017 a través del vínculo https://archivos.juridicas.unam.mx/www/bjv/libros/2/909/4.pdf

[24] TÉLLEZ VALDÉS, Julio. *Derecho Informático*. Capítulo XIII. Contratos Informáticos. Editorial Mc Graw Hill. Segunda edición. México, 1998. Puede consultar el texto íntegro a través del vínculo https://biblio.juridicas.unam.mx/bjv/detalle-libro/1941-derecho-informatico visto el 29 de noviembre de 2017.

[25] BRIZZIO, Claudia. *La informática en el nuevo derecho*. Abeloa Perrot. Buenos Aires, Argentina. 2000

conectadas a Internet. Verbigracia, un contrato electrónico podría ser aquel que se perfecciona a través de una conexión telefónica o servicio de comunicación *short message service*, en tanto que un contrato digital sería aquel que ocupa plataformas conectadas a la web y que se conocen tradicionalmente como *e-commerce*. Así las cosas, en una debida apreciación semántica, los contratos que tradicional y erróneamente se denominan electrónicos, deberían definirse como digitales, al menos respecto de aquéllos que ocurren en Internet. Ahora bien, dichos contratos pueden ser de naturaleza informática –por lo que refiere a la contratación de servicios de automatización- o bien, sólo ocupar medios informáticos para su perfeccionamiento y cuyo objeto indirecto pudiera ser cualquier bien tangible o intangible.

Más allá de la doctrina, el derecho comparado nos brinda acepciones adecuadas al caso que nos ocupa. En el caso español, la Ley de la Sociedad de la Información y de Comercio Electrónico, se refiere al contrato electrónico como "todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones."[26]

VIII.1.2 Precedentes sobre la aplicación de la Ley Modelo UNCITRAL

Como consecuencia de las leyes emitidas por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), en el año de 1988 se determinó la creación de un sistema de recopilación de decisiones judiciales y laudos arbitrales relativos a los convenios, convenciones y leyes modelo, emanados de la Comisión y la difusión de la información jurisprudencial. De esa forma, surgió el sistema "**CLOUT**" (***Case Law on UNCITRAL Texts*** [Sentencias y laudos sobre textos de la CNUDMI]). En términos generales, CLOUT contiene criterios relacionados con la Convención de las Naciones Unidas sobre el Reconocimiento y la Ejecución de las Sentencias Arbitrales extranjeras (1958), Convenio de las Naciones Unidas sobre el Transporte Marítimo de Mercancías (1978), Convención de las Naciones unidas sobre los Contratos de Compraventa Internacional de Mercaderías (1980), Ley Modelo de la CNUDMI sobre Arbitraje comercial Internacional (1985), Ley modelo de la CNUDMI sobre Comercio Electrónico (1996) y, Ley Modelo de la CNUDMI sobre la Insolvencia Transfonteriza (1997). Desde ese día, todos los resúmenes, índices, compendios y demás información publicada en relación con el sistema CLOUT pueden consultarse en el sitio de la CNUDMI en Internet: http://www.uncitral.org/uncitral/es/case_law.html. En ese tenor, la modernización y armonización que propone la Organización de las Naciones Unidas,

[26] Ley 34/2002 para regular *la Sociedad de la Información y de Comercio Electrónico. Anexo. Definiciones. Inciso "h)"*. Puede consultar el texto íntegro de la ley a través del vínculo https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758 Visto el 29 de noviembre de 2017.

permite la consulta pública de los criterios que se hayan dictado a nivel internacional. A saber del presente capítulo, invocaré algunos que resultan relevantes para fortalecer las manifestaciones anteriormente vertidas:

A) Lugar y Momento en que surte efectos un contrato emitido por correo electrónico

Caso 956: CIM 6, 46 3), 47, 48 1), 50; LMCE 15 Australia: Federal Court of Australia Olivaylle Pty Ltd v Flottweg GMBH & Co KGAA 20 de mayo de 2009 Original en inglés http://www.austlii.edu.au/au/cases/cth/federal_ct/2009/522.html

El demandante, una empresa australiana, y el demandado, una empresa alemana, celebraron un contrato para la venta de una cadena de producción de aceite de oliva. Después de celebrar prolongadas negociaciones sobre las condiciones del contrato y de intercambiar varios documentos preparatorios, el demandado incorporó las observaciones finales del demandante a la versión definitiva del contrato de compraventa, que el gerente de exportaciones alemán del demandado habia enviado por correo electrónico a su representante australiano en Nueva Gales del Sur (Australia), el 8 de febrero 2005. Éste (sic) último transmitió dicho mensaje electrónico al demandante, en su establecimiento sito en Victoria (Australia), el 10 de febrero de 2005. El contrato definitivo contenía la siguiente cláusula "se aplicará el derecho interno australiano, con exclusión de la normativa de la CNUDMI". En el contrato el vendedor demandado se comprometió a que la cadena de producción cumpliera ciertos objetivos prefijados en cuanto al rendimiento y la velocidad de funcionamiento, garantizando las reparaciones y el suministro de repuestos, así como la prestación correcta de todo servicio que no se hubiera prestado correctamente, dentro de un plazo razonable; en su defecto, el comprador tenía derecho a contratar a un técnico para efectuar las reparaciones y posteriormente recuperar los costos del vendedor. Además, el contrato atribuyó al demandante el derecho a reclamar una reducción del precio de compra o a rescindir el contrato, pero solamente tras el vencimiento de un "plazo de gracia razonable", que el comprador debería indicar una vez que el vendedor hubiera incumplido sus obligaciones. El demandante alegó que tuvo diversos problemas con la cadena de producción en el curso de la primera cosecha. En febrero de 2006, el demandante notificó al vendedor que se disponía a rescindir el contrato, a menos que el vendedor subsanase los defectos alegados a más tardar para finales de junio de 2006. El vendedor expresó su desacuerdo, alegando que el no haber obtenido los resultados estipulados en el contrato se debía a un empleo defectuoso de la maquinaria, si bien admitió que se había de sustituir una caja de engranajes. El comprador no permitió que el vendedor efectuara la reparación y presentó una demanda. En cuanto al perfeccionamiento del contrato, el tribunal entendió que las observaciones del comprador sobre la propuesta de contrato que recibió del vendedor a finales de 2004

constituían una contraoferta, y sostuvo que la comunicación electrónica enviada por el vendedor en febrero de 2005 constituía una aceptación, al haberse incorporado en ella las observaciones del comprador. En consonancia con el artículo 15 de la Ley Modelo de la CNUDMI sobre Comercio Electrónico (LMCE) que Australia había promulgado en el artículo 14 de su 4 V.10-54615 A/CN.9/SER.C/ABSTRACTS/96 Electronic Transactions Act de 1999 y el estado de Victoria había promulgado en el artículo 13 de su Electronic Transactions Act de 2000 el tribunal sostuvo que el lugar en que se recibió la comunicación electrónica de aceptación se considerará el lugar del perfeccionamiento del contrato. En cuanto al momento de su perfeccionamiento, el tribunal señaló que, en sentido estricto y de conformidad con el artículo 15 de la LMCE, el contrato se perfeccionó en el momento en que la comunicación electrónica de la aceptación llegó al comprador, esto es, cuando entró en el sistema de información del comprador el 10 de febrero de 2005. No obstante, habida cuenta de que las dos partes afirmaron en sus alegaciones que el contrato se perfeccionó el 8 de febrero de 2005, y que esta cuestión no afectaba al foudo de la coutroversia, el tribunal couvino en actuar teniendo en cueuta esa afirmación. Además, el tribunal sostuvo que, al insertar una cláusula de exclusión voluntaria en el contrato de compraventa, las partes excluyeron la aplicaciou de la CIM a tenor de lo dispuesto en su artículo 6; pero al concluir que "la normativa de la CNUDMI" en este contrato se refería a la CIM, y dado que esta Convención ya formaba parte del derecho interno australiano, el tribunal entendió que la intención de las partes, conforme a lo expresado en su escrito, era resolver sus controversias contractuales con arreglo únicamente a la ley del foro. Pasando al alegato del comprador por el que éste afirmaba tener derecho a rescindir el contrato, al no haber reparado el vendedor los defectos denunciados por el comprador, dentro del plazo por éste indicado, el tribunal señaló que el concepto de "un plazo de gracia" que cuyo transcurso daría al comprador el derecho a rescindir el contrato o a una reducciou del precio de compra tenía su origen en los ordenamientos jurídicos de inspiración romanista, más que en el common law. Por lo tanto, el tribunal analizó la sección III del capítulo II de la CIM, titulada "Derechos y acciones en caso de incumplimiento del contrato por el vendedor", en particular sus artículos 46 3), 47, 48 1) y 50, buscando orientación sobre la manera de interpretar dicho concepto. Al hacer referencia a la CIM, el tribunal señaló nuevamente la intención de las partes de incorporar cláusulas de ordenamientos jurídicos de inspiración romanista en su contrato. Al basarse en el artículo 48 1) de la CIM, el tribunal sostuvo que, en febrero de 2006, el comprador no tenía derecho a fijar un plazo de gracia que finalizara en junio de ese año, porque el plazo de reparación razonable del que todo vendedor gozaba no había vencido aún en ese momento. Según el tribunal, el plazo razonable para reparar los defectos descubiertos durante la cosecha 2005 vencía a finales de junio de 2006; sólo en ese momento el comprador adquiriría su derecho a fijar un plazo de gracia y amenazar con una rescisión del contrato al expirar dicho plazo. Al considerar irrazonable que el comprador no permitiera al vendedor

reparar las cajas de engranajes, el tribunal confirmó el derecho del vendedor a reclamar la última cuota adeudada en virtud del contrato.[27]

El criterio de la corte australiana permite identificar algunos elementos expuestos con anterioridad, sin embargo, destaca aquel que señala el momento y lugar de perfeccionamiento de un contrato electrónico/ digital. Éste se entiende por perfeccionado en el momento en que existe acuse de recepción de una contraoferta o bien, en el momento en que ambas partes entienden clara la voluntad de las partes. En el caso concreto, el juez optó por el segundo criterio de ***sistema de información***, en el cual no sólo basta la expedición y envío de aceptación, sino que la contraparte emite un acuse de recibo, para definir el lugar y momento claro del perfeccionamiento del contrato.

B) Short Message Service (SMS)

Caso 964: MLEC 2 a), 3, 4, 5, 9, 15 Sudáfrica: Labour Court of South Africa (Durban) Caso núm. D204/07 Jafta v Ezemvelo KZN Wildlife 1 de julio de 2008 Publicado en inglés: [2008] ZALC 84; [2008] 10 BLLR 954 (LC); (2009) 30 ILJ 131 (LC) 1 de Julio de 2008 Original en inglés Disponible en: http://www.saflii.org/za/cases/ZALC/2008/84.html Se cita el caso núm. 661 de la Jurisprudencia de los tribunales sobre textos de la CNUDMI (CLOUT). Este caso se refiere a la celebración de un contrato laboral en relación con el uso de comunicaciones electrónicas (correo electrónico y mensajes breves por aparato portátil (SMS)). A raíz de un proceso de selección satisfactorio, el demandado, E KZN W, envió por correo electrónico una oferta de empleo al demandante, SGJ, que la aceptó provisionalmente. El demandado envió un segundo correo electrónico, incitando a adoptar una decisióu defiuitiva, a lo que el demandante respondió aceptando la oferta incondicionalmente. Aunque el sistema de información del demandante indicaba que se había enviado satisfactoriamente el correo electrónico de aceptación, éste nunca llegó al sistema del demandado. Más tarde, uno de los empleados del demandado envió un último recordatorio de la oferta pendiente mediante un mensaje corto de texto (SMS), al que el demandante respondió a la mayor brevedad confirmando su aceptación. El tribunal examinó la celebración del contrato laboral por correo electrónico y mensajes cortos de texto (SMS) en el contexto de la Electronic Communications Transaction Act de Sudáfrica, act No. 25 of 2002 ("ECT Act"), cuyas partes pertinentes se basan en la Ley Modelo de la CNUDMI sobre Comercio

[27] Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Jurisprudencia de los Tribunales sobre Textos de la CNUDMI (CLOUT)*. A/CN.9/SER.C/ABSTRACTS/96. 22 de junio de 2010. Visto el 27 de noviembre de 2017 a través del vínculo https://documents-dds-ny.un.org/doc/UNDOC/GEN/V10/546/15/PDF/V1054615.pdf?OpenElement

> Electrónico de 1996 (LMCE). En particular, el tribunal señaló la necesidad de interpretar la ECT Act a la luz del hecho de que se trataba de una ley interna inspirada en un instrumento de derecho uniforme y del carácter inherentemente transnacional de la ley de comunicaciones electrónicas; por lo tanto, el tribunal hizo referencia a la LMCE, a las leyes de otros países inspiradas en la LMCE, así como a la jurisprudencia pertinente de algunos foros extranjeros. Además, el tribunal señaló que determinados principios del derecho de las comunicaciones electrónicas gozan de una amplia aceptación en todo el mundo y se han promulgado en la legislación de Sudáfrica. Entre esos principios cabe mencionar los siguientes: no discriminación de las comunicaciones electrónicas (art. 11 de la ECT Act; art. 5 de la LMCE); el valor probatorio de los mensajes de datos (art. 15 de la ECT Act; art. 9 LMCE); y la autonomía contractual de las partes frente a ciertas normas legales (art. 21 de la ECT Act; art. 4 de la LMCE). Con respecto al perfeccionamiento del contrato, el tribunal señaló que no existían pruebas de que la respuesta que el demandante había enviado por correo electrónico V.10-54615 11 A/CN.9/SER.C/ABSTRACTS/96 con una aceptación incondicional de la oferta hubiera entrado en el sistema de información controlado por el destinatario, y que, por lo tanto, no se podía considerar que el contrato se hubiera celebrado en ese momento (véase el art. 23 b) de la ECT Act, que se inspiraba en el art. 15 2) a) i) de la LMCE, pero añadiendo el requisito de que el mensaje sea accesible al destinatario, a fin de que éste pueda procesarlo). El tribunal declaró que los mensajes breves transmitidos por aparato portátil (SMS) responden a la noción de comunicación electrónica establecida en la ECT Act, y en particular a sus definiciones de "comunicación electrónica" y de "mensaje de datos" (inspiradas en el art. 2 a) de la LMCE), y que, por lo tanto, la aceptación expresada mediante un SMS constituye un método válido para comunicar la aceptación de una oferta (art. 22 de la ECT Act; véase también el art. 11 de la LMCE).[28]

No discriminación, valor probatorio y voluntad contractual son los principios que se desprenden del criterio adoptado por el Tribunal Laboral que tuvo a bien resolver sobre la eficacia probatoria de un *SMS* como mecanismo para manifestar la voluntad de una las partes y, en su caso, como medio idóneo para satisfacer el requisito de consentimiento para el perfeccionamiento de un contrato –en este caso, de índole laboral–.

La comunicación electrónica que sirvió de base para la celebración del contrato (su aceptación) resulta un medio substituto permisible, ante la imposibilidad de celebrar el contrato por medios digitales, tal como se dispuso inicialmente. Conforme a lo anterior, es indiscutible que un mensaje de datos que incluya la aceptación de una

[28] Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Jurisprudencia de los Tribunales sobre Textos de la CNUDMI (CLOUT)*. A/CN.9/SER.C/ABSTRACTS/96. 22 de junio de 2010. Visto el 27 de noviembre de 2017 a través del vínculo https://documents-dds-ny.un.org/doc/UNDOC/GEN/V10/546/15/PDF/V1054615.pdf?OpenElement

oferta, ya sea por medios digitales o electrónicos, debe considerarse válido, siempre que contenga la voluntad del aceptante y permita la autenticación del mismo (salvo prueba en contrario); elementos que se presentan en el caso en concreto.

C) Firma autógrafa prescindible

Caso 1568: LMCE 7 Nueva Zelandia: Tribunal Superior de Nueva Zelandia, Secretaría de Auckland [2014] NZHC 164 Cox, Cowie and Sutcliffe v. Coughlan and Wilson 14 de febrero de 2014 Original en inglés sin publicar

Resumen preparado por Petra Butler, corresponsal nacional.

Los demandantes en este caso poseían una casa de vacaciones que deseaban vender. Los demandados poseían una propiedad arrendada y deseaban comprar una casa de vacaciones. Las partes negociaron y finalmente acordaron intercambiar los bienes (eran de valor casi igual). Sin embargo, justo antes de la fecha de la liquidación definitiva, los demandados se negaron a proceder, aduciendo que no cabía cumplir el acuerdo porque no habían firmado y no constaba por escrito. 8 V.16-02597 A/CN.9/SER.C/ABSTRACTS/168 El acuerdo de compraventa inicial había sido firmado por ambas partes; sin embargo, había varias omisiones importantes que era necesario subsanar. El demandante remitió la versión modificada del acuerdo (aceptada como contraoferta) al abogado de los demandados el 11 de diciembre de 2012. El abogado envió una copia electrónica a los demandados, aunque en el mensaje que la acompañaba no figuraba ninguna solicitud de que firmaran la contraoferta. En la correspondencia posterior no se trató de si se había producido el acuerdo, sino que giró en torno a los debates acerca de la liquidación. Problemas relacionados con el arrendamiento retrasaron la fecha de la liquidación hasta el año nuevo; se intercambió correspondencia explícita para modificar el acuerdo y condicionarlo a la solución de los problemas relacionados con el arrendamiento. Cuando se intercambiaron las declaraciones para la liquidación, contrariamente a lo que pensaban los demandados, había que pagar una cantidad extra de 6.000 dólares neozelandeses por la casa de vacaciones a causa de la diferencia de valor. El demandante propuso que se dividiesen la diferencia, pero los demandados rechazaron la oferta y no cumplieron el acuerdo. El primer argumento esgrimido por los demandados en contra del cumplimiento específico fue que nunca habían aceptado la contraoferta (que incluía tres cambios en los documentos que habían firmado inicialmente). El Tribunal observó que en el artículo 22 de la Ley de Transacciones Electrónicas de 2002 [concordante con lo fundamental del artículo 7 de la LMCE] se aceptaban las firmas electrónicas como manifestación de la intención de obligarse. El Tribunal se remitió a la decisión del caso Welsh v. Gatchell, en la que el Tribunal había considerado que basta una firma electrónica si el Tribunal está convencido de que su inserción tenía por objeto indicar la aprobación de la nota electrónica. Sobre este punto, el Tribunal consideró que las palabras y la conducta de las partes después del

envío de la contraoferta indicaban que se consideraban obligadas por el acuerdo. El segundo argumento de los demandados era que el acuerdo no figuraba por escrito y, por consiguiente, no podía ser exigido. En el artículo 24 de la Ley de Derecho de Propiedad de 2007 se exige que el contrato de compraventa de bienes raíces figure por escrito. En el artículo 19 de la Ley de Transacciones Electrónicas de 2002 se permite cumplir ese requisito en forma electrónica; no obstante, el Tribunal reconoció que era necesario que hubiera constancia escrita de que se habían aceptado las condiciones de la contraoferta. En opinión del Tribunal, sí existía esa constancia escrita; la contraoferta se había mencionado, expresa o tácitamente, en varios documentos posteriores. El Tribunal ordenó a los demandados que cumplieran específicamente el acuerdo de compraventa de las propiedades.[29]

El criterio neozelandés que nos ocupa podría no resultar aplicable a todas las legislaciones, sobre todo por algunos elementos de solemnidad o formalidad que requiera cada Estado –como puede ser pasar ante la fe de un notario público el contenido de dicho contrato-, sin embargo, brinda dos criterios que fortalecen lo expuesto en el presente capítulo; en primer lugar, se advierte que la firma electrónica puede considerarse cualquier manifestación de la voluntad a través de medios electrónicos o digitales, en términos de la plataforma por la cual se conciba el contrato respectivo, en el caso concreto, la simple "aceptación" por expreso permitió tener por acreditado dicho elemento de validez; en segundo lugar, la substitución –equivalencia funcional- del soporte tangible por uno electrónico para el perfeccionamiento del contrato, con independencia del breve entendimiento de las partes sobre la materia, el Tribunal de la causa tuvo por perfeccionado y materializado el contrato por pactarse a través de un soporte electrónico (léase digital), con lo que se desestimó el argumento por el que se pretendía sostener la inexistencia del acuerdo de voluntades.

D) Comunicación por Fax

Caso 1569: [LMCE 15 2) b)] Nueva Zelandia: Tribunal Superior de Nueva Zelandia, Secretaría de Auckland [2014] NZHC 151 Harris v. Commissioner of Inland Revenue 13 de febrero de 2014 Original en inglés Sin publicar.

Resumen preparado por Petra Butler, corresponsal nacional.

El demandante solicitó la revisión judicial de la decisión que sostenía que el Comisionado de Hacienda Pública había respondido a una declaración de postura dentro

[29] Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Jurisprudencia de los Tribunales sobre Textos de la CNUDMI (CLOUT)*. A/CN.9/SER.C/ABSTRACTS/168. 4 de mayo de 2016. Visto el 27 de noviembre de 2017 a través del vínculo https://documents-dds-ny.un.org/doc/UNDOC/GEN/V16/025/97/PDF/V1602597.pdf?OpenElement

del plazo de dos meses exigido en la Ley de Administración Fiscal de 1994. Se habían realizado dictámenes de falta de pago y se exigió al demandante que presentase una declaración de postura para el 20 de noviembre de 2009. El demandante así lo hizo el 20 de noviembre. El Comisionado tenía que responder para el 19 de enero de 2010; se envió una respuesta por fax a las 23.07 horas y por correo ordinario a las 23.25 horas el 19 de enero de 2010. Se aceptó que el demandante no había designado el fax como sistema de información para recibir comunicaciones electrónicas con arreglo al artículo 11 a) de la Ley de Transacciones Electrónicas de 2002. Sin embargo, también se aceptó que el Comisionado se había comunicado con el agente del demandante por fax en ocasiones anteriores. El demandante esgrimió el artículo 11 b) de la Ley de Transacciones Electrónicas de 2002, que dice lo siguiente: "Una comunicación electrónica se considerará recibida [...] en el momento en que la comunicación electrónica llegue al conocimiento del destinatario". En este caso, llegó al conocimiento del demandante el 20 de enero de 2010. El demandante alegó además que el Comisionado no debería haber hecho la notificación por fax en absoluto, debido a que había "motivos razonables para suponer" que la notificación no sería recibida por el destinatario conforme a lo dispuesto en el artículo 14 7) de la Ley de Tributación (Ajuste del Tipo Impositivo Resultante y Cuestiones Correctivas) de 2009. En cuanto a la primera cuestión, el Tribunal señaló que en el artículo 14 7) no se exige que la notificación se "señale a la atención" del destinatario, y que si se hubiese enviado por carta, no se hubiera exigido que el destinatario hubiera abierto la carta para que se hubiese considerado que había sido "recibida". Esta interpretación es coherente con el artículo 15 2) b) de la LMCE que, en caso de que el destinatario no hubiese designado un sistema de información, sólo exige que el mensaje de datos haya entrado en el sistema de información del destinatario. El Tribunal discrepó de la alegación del demandante sobre este punto. El Tribunal sostuvo también que el hecho de que el Comisionado hubiese utilizado el fax para comunicarse con el demandante en ocasiones anteriores significaba que no había motivos razonables para suponer que la notificación no sería recibida por el destinatario. La pretensión fue rechazada discrecionalmente y en cuanto al fondo.[30]

El criterio que se invoca rescata dos principios fundamentales en el entendimiento de medios tecnológicos de prueba: Neutralidad tecnológica y equivalencia funcional. No sólo se desestima el argumento del demandante al señalar que debió notificar la utilización de un medio electrónico para notificar una resolución, sino que la "aceptación" previa para recibir ese tipo de documentos resultó suficiente para tenerse por permitida para el trámite en comento; por otro lado, el tribunal neozelandés

[30] Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Jurisprudencia de los Tribunales sobre Textos de la CNUDMI (CLOUT)*. A/CN.9/SER.C/ABSTRACTS/168. 4 de mayo de 2016. Visto el 27 de noviembre de 2017 a través del vínculo https://documents-dds-ny.un.org/doc/UNDOC/GEN/V16/025/97/PDF/V1602597.pdf?OpenElement

dicta que no pudiere solicitarse mayores requisitos para tener por notificado el mensaje por fax, de aquéllos que pudieren exigirse para un mecanismo tradicional de notificación, en el entendimiento que el envío por medios provistos y aceptados, en su momento, por el particular, resulta suficiente para tener por hecha la notificación.

E) Manifestación de la voluntad: "Aceptar"

> Caso 1570: MLEC 7-Nueva Zelandia: Tribunal Superior de Nueva Zelandia, Secretaría de Christchurch [2013] NZHC 1892 RD2 International Limited v. NDP 2010 Limited 29 de julio de 2013 Original en inglés Sin publicar.
>
> Resumen preparado por Petra Butler, corresponsal nacional.
>
> El demandante en este caso solicita una orden por la que se desestime la reclamación de deuda sobre la base de que existían fundamentos razonables para una reconvención contra el demandado. Hubo una teleconferencia el 10 de febrero de 2011, en la que el demandado afirmó que ellos garantizarían el pago de una deuda contraída con el demandante. El 16 de febrero se dejó constancia escrita del acuerdo en un mensaje de correo electrónico. El 18 de febrero, el demandado contestó al mensaje de correo electrónico de la siguiente manera: "NPD 2010 Limited garantizará a RD2 la deuda de ND. "Aceptar". La palabra "Aceptar" reproducida aquí en negrita estaba escrita en letras rojas en el mensaje de correo electrónico, y se indicó que quería decir que exige "cambios u observaciones o mayor discusión". El demandante de este caso aceptó que era necesario que la garantía constara por escrito, pero se basa en el artículo 22 de la Ley de Transacciones Electrónicas de 2002 [concordante con lo fundamental del artículo 7 de la LMCE] para argumentar que el demandado firmó el documento al poner su nombre al pie del mensaje de correo electrónico. El Tribunal afirma que es defendible que el Sr. T (en nombre de NDP) suscribió el acuerdo con la palabra "Aceptar". Cuando se ocupa de lo que implica emplear letra de color rojo, el Tribunal indica que el único motivo de una declaración tan simple como "Aceptar" debe haber sido diferenciarla de las alternativas "cambios" o "mayor discusión". El Tribunal llegó a la conclusión de que el demandante tenía fundamentos razonables para una reconvención contra el demandado. Se accedió a la solicitud y se desestimó la reclamación de NDP.[31]

El reporte de la sentencia que se analiza, es la síntesis de los tres anteriormente estudiados, en el sentido que considera como "firma" el nombre al calce de un correo electrónico, sin necesidad de mayores requisitos formales o tecnológicos; por otro

[31] Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Jurisprudencia de los Tribunales sobre Textos de la CNUDMI (CLOUT)*. A/CN.9/SER.C/ABSTRACTS/168. 4 de mayo de 2016. Visto el 27 de noviembre de 2017 a través del vínculo https://documents-dds-ny.un.org/doc/UNDOC/GEN/V16/025/97/PDF/V1602597.pdf?OpenElement

lado, la "aceptación" de este acuerdo no ocurre de forma tácita como pudiere ser en otros casos, sino que existe la palabra textual al momento de cerrar comunicaciones a través de correo electrónico, por lo que el acuerdo se tuvo por suscrito desde el momento de dicha manifestación a través de un medio tecnológicamente avanzado.

F) Jurisdicción en contratación electrónica

Caso 1603: LMCE 15 4) Australia: Tribunal Federal de Australia Australian Competition and Consumer Commission c. Valve Corporation (núm. 3) [2016] FCA 196; [2016] ATPR 42-518 24 de marzo de 2016 Original en inglés Publicado en https://jade.io/j/#!/article/459877 Resumen preparado por Aynur Akhundli.

Este caso guardaba relación con el lugar de formación de un contrato celebrado por medios electrónicos a fin de determinar la ley aplicable al contrato. La parte demandada, una empresa con sede en el estado de Washington en los Estados Unidos de América (demaudado), opera una red de distribuciou de juegos eu línea con 2 milloues de cuentas de abonados australianos. Los usuarios de los juegos en línea debian firmar con la parte demandada un acuerdo de suscripción por conducto del proveedor de servicios en línea Steam (acuerdo SSA) a fin de tener acceso a los juegos en líuea. El acuerdo SSA contenía una cláusula sobre selección de ley en la que se estipulaba que la ley aplicable al contrato en cuestión era la ley del estado de Washington. El demandante inició una acción legal contra la empresa demandada en Australia por conducta equívoca y engañosa en su plataforma de juegos. Según el demandante, la parte demandada contravino la legislación australiana de protección del consumidor al incluir representaciones falsas o engañosas sobre las garantías otorgadas al consumidor. La parte demandada argumentó, entre otras cosas, que la legislación australiana de protección del consumidor no se aplicaba al caso puesto que la presunta conducta no había ocurrido en Australia y la empresa no tenía operaciones comerciales en ese país. Entre varias otras cuestiones planteadas por este caso, cabía examinar la cuestiou de la ley aplicable al contrato. El Tribunal y las partes hicieron caso omiso de la cláusula de selección de ley contenida en el acuerdo SSA. Más bien, el Tribunal se propuso determinar qué legislación tenía el vínculo más estrecho y real con la operación en cuestión, lo que la identificaría como la ley aplicable al contrato. Conforme a la legislación australiana, entre los criterios para determinar esa ley figuraban el lugar de la residencia o el establecimiento de las partes; el lugar de formación del contrato; el lugar en que se cumplió la obligación estipulada en el contrato; y la naturaleza y el contenido del contrato. Con respecto al lugar de formación del contrato, el Tribunal, aplicando la lex fori, determinó que el contrato se había formado en el lugar donde se habían recibido los mensajes electrónicos de aceptación de los consumidores (estado de Washington) y no en los lugares eu Australia desde los que se habíau enviado esos mensajes, habida cuenta de que, para ser efectivos, los contratos bilaterales por lo general requerían la recepción de una comunicación

de aceptación. El Tribunal observó que esa conclusión era coherente con la legislación australiana sobre las operaciones electrónicas, basada en el artículo 15 4) de la LMCE, en que se definía el lugar de 4 V.16-05297 A/CN.9/SER.C/ABSTRACTS/173 recepción de las comunicacioues electrónicas generalmente como el lugar donde el destinatario tenía su establecimiento. El Tribunal observó además que el lugar de formación del contrato tenía muy poco peso como factor para determinar la ley aplicable al contrato en la actual era de las telecomunicaciones avanzadas. No obstante, a la luz del análisis de los demás factores pertinentes (lugar de formación y naturaleza y contenido del contrato) se confirmaba que se había identificado correctamente la legislación del estado de Washington como la ley aplicable a un contrato para el suministro de bienes o servicios a consumidores por la parte demandada. Sin embargo, sobre la base de los méritos y de otros argumentos, el Tribunal decidió que la legislación australiana de protección del consumidor era la ley aplicable al contrato.[32]

Sin duda, el presente reporte de sentencia podría ser uno de los más debatibles por lo que refiere a la aplicación de una legislación sobre otra, respecto de un contrato que surge en la vida *on line*. En capítulos pasados dentro de la presente obra, se han analizado conceptos como *personal jurisdiction* y efectividad de la sentencia para determinar la jurisdicción sobre un acto de naturaleza digital, empero, la sentencia que se reproduce en la parte conducente resulta un criterio adecuado para la aplicación del principio *lex fori*, sobre la protección de una calidad jurídica superior como lo son los derechos de consumidor.

En el entendimiento que no puede considerarse que cualquier "renuncia de jurisdicción" en un contrato informático, electrónico o digital puede tenerse por inválida automáticamente, sino que debe atenderse su validez a la luz de la hipótesis real que se estudie. Conforme al criterio del Tribunal Federal Australiano, parece cierto que la legislación que deberá prevalecer al contrato informático es la local, respecto de la americana, en atención al lugar en que surte efectos el objeto directo del contrato.

G) Valor probatorio de documentos electrónicos que se ofrecen impresos a un procedimiento

Caso 1607: LMCE 2 a); 5; 9 Sri Lanka: Tribunal Superior de la Provincia Occidental Caso núm. HC/Civil/201/200B/MR People's Leasing Company Limited c. Muthuthantrige Iran Fernando y otros.

[32] Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Jurisprudencia de los Tribunales sobre Textos de la CNUDMI (CLOUT)*. A/CN.9/SER.C/ABSTRACTS/173. 22 de agosto de 2016. Visto el 27 de noviembre de 2017 a través del vínculo https://documents-dds-ny.un.org/doc/UNDOC/GEN/V16/052/97/PDF/V1605297.pdf?OpenElement

15 de febrero de 2016 Resumen preparado por Quynh Anh Tran.

La cuestión principal planteada en el presente caso consistía en determinar si las copias de entradas de un libro mayor en formato electróuico eran o no admisibles como elemento probatorio. El demandante y los demandados celebraron un acuerdo de arrendamiento de un camión. El demandante entabló una acción legal contra los demandantes a fin de recuperar el camión y ciertas sumas pendientes de pago. El demandante presentó copias auténticas de impresos de computadora que reproducían ciertas entradas de su libro mayor electrónico como prueba de las sumas adeudadas. Sin embargo, los demandados impugnaron la presentación de esos documentos por las siguientes razones: su origen era incierto, dado que no había pruebas prima facie de que esos documentos pertenecieran al demandante; no se habían verificado las fuentes de los datos informáticos; y los documentos no eran pertinentes para el acuerdo de arrendamiento en cuestión. El Tribunal observó que un libro mayor en formato electrónico constituía un documento electrónico conforme a la definición contenida en el artículo 26 de la Ley de Operaciones Electrónicas de Sri Lanka. La definición de documento electrónico conforme a esa Ley estaba basada en la de mensaje de datos (artículo 2 a) de la LMCE). Asimismo, a la luz del artículo 3 de la Ley de Operaciones Electrónicas (correspondiente al artículo 5 de la LMCE), el Tribunal señaló que no debía negarse reconocimiento, efectos jurídicos, validez o fuerza obligatoria a un libro mayor por la sola razón de estar en forma electrónica. El Tribunal señaló además que las entradas de un libro mayor electrónico basadas en recibos de caja eran admisibles como documentos societarios a la luz de lo dispuesto en el artículo 21 2) de la Ley de Operaciones Electrónicas (véase asimismo el artículo 9 de la LMCE). El Tribunal observó también que el artículo 21 3) de dicha Ley preveía tres presunciones refutables, las cuales guardaban relación con la integridad de la información contenida en un mensaje de datos presentado con fines probatorios, con el iniciador de ese mensaje de datos y con la autenticidad de una firma electrónica u otra marca de identificación distintiva conteuida en el meusaje. A la luz de lo anterior, el Tribunal admitió los impresos de computadora como prueba, con sujeciou a la posible refutación de las presunciones contenidas en ellos.[33]

La cita del presente criterio al final de este apartado es intencional, ya que no comparto enteramente la decisión del Tribunal de Sri Lanka. Si bien es cierto dota de fuerza probatoria a un libro electrónico de registros para poder valorarse en un proceso, no menos cierto es que le resta autenticidad al permitir que el mismo se desahogara en forma impresa; sin duda, este mecanismo de incorporación a un proceso

[33] Asamblea General de las Naciones Unidas. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Jurisprudencia de los Tribunales sobre Textos de la CNUDMI (CLOUT)*. A/CN.9/SER.C/ABSTRACTS/173. 22 de agosto de 2016. Visto el 27 de noviembre de 2017 a través del vínculo https://documents-dds-ny.un.org/doc/UNDOC/GEN/V16/052/97/PDF/V1605297.pdf?OpenElement

resulta incongruente con la naturaleza del medio de convicción que nos ocupa. Al respecto, me pronunciaré de forma puntual en el capítulo respectivo.

VIII.2 Click Wrap Agreements

En la práctica digital los cibernautas se enfrentan a una nueva modalidad de negocio jurídico que poco se ha estudiado por Tratados internacionales y la doctrina, sin embargo, es uno de los más practicados y celebrados en la web, sobre todo en plataformas que son conocidas como "redes sociales" o en aquellas que ofrecen un servicio y lanzan un *pop up* con sus términos y condiciones, permiten marcar una casilla y tienen por rendido el consentimiento del usuario al dar clic en el botón marcado con la leyenda "Aceptar".

Según el Diccionario Legal de *Black*, podríamos definir a este especial contrato, únicamente en el universo del licenciamiento de uso de software que se adquiere en la web, aplicable en el momento en que el comprador o usuario hacen clic en el botón "Acepto" del propio portal[34]; sin embargo, su campo de aplicación ha crecido más allá del licenciamiento y hoy en día es una fórmula legal que permite la celebración de contratos vinculantes.

El concepto *legally binding contracts online* se ha acuñado en sistemas anglosajones para definir a los acuerdos que se incluyen en las páginas web que contienen los términos y condiciones; inclusive, existen autores que han creado pautas mínimas legales para la creación de estos contratos vinculantes, como lo expone J. Hirby, en su contribución al Diccionario Legal de Black, cuyo artículo *Creating Legally Binding Contracts Online,*[35] determina que este tipo de contratos deben establecer pistas para el cibernauta sobre la existencia del documento jurídico y éstos, deberán crearse –a su entender- bajo los siguientes estándares:

1. Los visitantes deben prevenir la existencia del contrato en el sitio web que están buscando;
2. Los visitantes deben tener oportunidad de revisar los términos del acuerdo y contar con tiempo para tomar decisiones;
3. Los visitantes deben comprender el método por el cual se ejecutará o renunciará al contrato: y

[34] Black's Law Dictionary. *What is Click-Wrap Agreement?* Puede consultar el texto original en inglés a través del vínculo https://thelawdictionary.org/click-wrap-agreement/ visto el 29 de noviembre de 2017.

[35] HIRBY, J. *Creating Legally Binding Contracts Online.* Black's Law Dictionary. Puede consultar el texto original en inglés a través del vínculo https://thelawdictionary.org/article/creating-legally-binding-contracts-online/ visto el 29 de noviembre de 2017.

4. El propietario del sitio web o el administrador oferente, deben contar con un mecanismo para probar que el usuario aceptó o rechazó el contrato.

Según el abogado español Ricardo Fernández Flores, podemos definir al *click-wrap* agreement como el modelo de contratación por el cual las condiciones y términos de un sitio web pueden deben ser aceptados expresamente con anterioridad a la celebración de una transacción; normalmente ocurre a través de un clic sobre el botón con la leyenda "Acepto/ I Agree". Fernández Flores los distingue de los ***browse wrapping***, en el entendimiento que estos últimos ponen las condiciones de navegación al final de la página y sólo requieren la aceptación tácita del usuario, que se ejecuta en forma de navegación, es decir, el hecho que el cibernauta se mantenga en el portal web, da por entendido la celebración de este tipo de acto sin ser necesario ulterior acto de manifestación de una u otra voluntad.[36] Bajo ambas modalidades, debe ser claro que estamos en presencia de contratos de adhesión digitales en los que el usuario debe aceptar las condiciones del sitio previo a la utilización del producto o beneficiarse del servicio, en el entendido que de no aceptar los términos del portal, no podrá usar o beneficiarse del producto o servicio, respectivamente. Empero, el peso jurídico que han recibido ambos a nivel judicial ha sido polarizado, en tanto que sólo el primero de ellos cuenta con fuerza vinculante, en tanto que el segundo no requiere ulterior actividad para confirmar el entendimiento de las condiciones del portal. Así lo sostuvo en diciembre de 2005 la Corte de Apelación de Illinois del Quinto Circuito en el caso *Dewayne Hubbert, Elden L.* y otros *Vs. Dell Corporation.* En dicha apelación, los integrantes de la corte dictaron lo siguiente:

> Encontramos que el contrato en línea incluye los "Términos y condiciones de venta". El hipervínculo azul titulado "Términos y condiciones de venta" apareció en numerosas páginas web que los demandantes completaron en el proceso de pedido. Los hipervínculos azules para los "Términos y condiciones de venta" también aparecían en las páginas web de mercadeo del demandado, copias de las cuales los demandantes adjuntaron a su reclamo. Los hipervínculos azules en las páginas web del demandado, que constituyen el proceso de cinco pasos para ordenar las computadoras, deben tratarse de la misma manera que un contrato escrito en varias páginas. El hipervínculo azul simplemente lleva a una persona a otra página del contrato, similar a pasar la página de un contrato por escrito. Aunque no hay un requisito de visibilidad, el tipo azul de contraste del hipervínculo lo hace llamativo. El sentido común dicta que debido a que los demandantes compraban computadoras en línea, no eran principiantes cuando usaban

[36] FERNÁNDEZ FLORES, Ricardo. *La ejecución de los contratos click-wrap y browse wrap en Derecho español.* Economist & Jurist. Inicio. Artículos destacados. Difusión jurídica y temas de actualidad, S.L. España, 2017. Visto el 29 de noviembre de 2017 a través del vínculo http://www.economistjurist.es/articulos-juridicos-destacados/la-ejecucion-de-los-contratos-click-wrap-y-browse-wrap-en-derecho-espanol/

computadoras. Una persona que usa una computadora aprende rápidamente que hay más información disponible haciendo clic en un hipervínculo azul. Además, en tres de las páginas web del demandado que los demandantes completaron para realizar sus compras, apareció la siguiente declaración: "Todas las ventas están sujetas a los términos y condiciones de venta de Dell". Esta declaración pondría en conocimiento de una persona razonable que existían términos y condiciones adjuntos a la compra y que sería conveniente averiguar cuáles eran los términos y condiciones antes de realizar una compra. La declaración de que las ventas estuvieron sujetas a los "Términos y condiciones de venta" del demandado, combinadas con hacer que los "Términos y condiciones de venta" estén accesibles en línea mediante hipervínculos azules, fue suficiente aviso para los demandantes que comprar las computadoras en línea haría que " Términos y condiciones de venta "vinculantes para ellos. Debido a que los "Términos y condiciones de venta" formaban parte del contrato en línea y debido a que los demandantes no argumentaron que sus reclamos no estaban dentro del alcance del acuerdo de arbitraje, estaban sujetos a los "Términos y condiciones de venta", incluidos la cláusula de arbitraje. Debido a que concluimos que los "Términos y condiciones de venta" formaban parte del contrato en línea formalizado en el momento en que los demandantes compraron las computadoras, no necesitamos considerar qué efecto tienen las copias de los "Términos y condiciones de venta" en las cajas de envío, que se refieren al contrato.[37]

[Traducción del autor]

[37] CORTE DE APELACIÓN DEL QUINTO DISTRITO DE ILLINOIS. *Dewayne Hubbert V Dell Corporation*. Apelación del Circuito de Madison. Número 5-03-0643. Notificado el 8 de diciembre de 2005. Puede visualizar la versión original a través del vínculo http://pub.bna.com/eclr/hubbert081205.pdf visto el 29 de noviembre de 2017. El texto original en inglés dicta: "We find that the online contract included the "Terms and Conditions of Sale." The blue hyperlink entitled "Terms and Conditions of Sale" appeared on numerous Web pages the plaintiffs completed in the ordering process. The blue hyperlinks for the "Terms and Conditions of Sale" also appeared on the defendant's marketing Web pages, copies of which the plaintiffs attached to their complaint. The blue hyperlinks on the defendant's Web pages, constituting the five-step process for ordering the computers, should be treated the same as a multipage written paper contract. The blue hyperlink simply takes a person to another page of the contract, similar to turning the page of a written paper contract. Although there is no conspicuousness requirement, the hyperlink's contrasting blue type makes it conspicuous. Common sense dictates that because the plaintiffs were purchasing computers online, they were not novices when using computers. A person using a computer quickly learns that more information is available by clicking on a blue hyperlink. Additionally, on three of the defendant's Web pages that the plaintiffs completed to make their purchases, the following statement appeared: "All sales are subject to Dell's Term[s] and Conditions of Sale." This statement would place a reasonable person on notice that there were terms and conditions attached to the purchase and that it would be wise to find out what the terms and conditions were before making a purchase. The statement that the sales were subject to the defendant's "Terms and Conditions of Sale," combined with making the "Terms and Conditions of Sale" accessible online by blue hyperlinks, was sufficient notice to the plaintiffs that purchasing the computers online would make the "Terms and Conditions of Sale" binding on them. Because the "Terms and Conditions of Sale" were a

De dicho texto se aprecia que la Corte de Illinois tuvo claro que la existencia de un aviso vinculante presente en la plataforma, de forma destacada, a la vista de los usuarios, adicionalmente, que la experiencia de los cibernautas licenciatarios era la suficiente para reconocer el poder vinculante de los términos y condiciones de Dell, al momento de adquirir la licencia. En ese sentido el principio de "*constructive notice*" resulta fundamental para resolver la aplicabilidad de este tipo de contratos, según se sostuvo en el caso *Nguyen v. Barnes & Noble, Inc;* en el cual la Corte de Apelación de Noveno Circuito, emitió la sentencia de 18 de agosto de 2014, bajo la cual dictó que un usuario de una web no emite consentimiento vía *browse wrap*, si es que el portal no aporta pistas suficientes para permitir conocer la existencia y contenido de los términos de uso de la plataforma, máxime si estos aparecen en la parte final del sitio sin posibilidad de distinción para el usuario.[38] Este criterio toma fortaleza internacional, a raíz de la entrada en vigor del Reglamento General de Protección de Datos Personales. El 27 de abril de 2016, en Bruselas, el Parlamento Europeo y el Consejo de la Unión Europea anunciaron la creación y aplicación del Reglamento General de Protección de Datos Personales (en adelante ***RGPD***), como medida para unificar el tratamiento de dichos datos y buscar la equivalencia en los Estados Miembros.

El artículo 99 de este ordenamiento, ordenó que la entrada en vigor del RGPD sería a partir del 25 de mayo de 2018 y según se desprende de su lectura, las nuevas obligaciones trascienden el territorio de la Unión Europea, lo que obliga a cualquiera que trate datos personales, a estudiar el Reglamento y conocer, si le resulta aplicable. Sobre el particular, el *RGPD* obliga a los responsables y encargados a mantener diversos protocolos de Ciberseguridad e inclusive adaptar sus sitios web por lo que refiere a la fórmula de los *click wrap agreements*. Esta obligación implica que desaparece la figura del *Scroll Wrap Agreement/ Browse Wrap* (Consentimiento tácito por navegación), por lo que ahora el portal web deberá recabar el consentimiento del usuario de forma inequívoca (manifestación del interesado o acción afirmativa) y expreso (en caso de tratamiento de datos personales sensibles no bastará la navegación como acto de consentimiento). Debe existir una casilla en el sitio web que permita el

part of the online contract and because the plaintiffs did not argue that their claims were not within the scope of the arbitration agreement, they were bound by the "Terms and Conditions of Sale," including the arbitration clause. Because we conclude that the "Terms and Conditions of Sale" were a part of the online contract formed at the time of the plaintiffs' purchase of the computers, we need not consider what effect the copies of the "Terms and Conditions of Sale" enclosed in the shipping boxes have on the contract."

[38] CORTE AMERICANA DE APELACIÓN DEL NOVENO CIRCUITO. *Kevin Khoa Nguyen V. Barnes & Noble, INC.* Apelación número 12-56628 de 18 de agosto de 2014. Puede consultar el texto íntegro a través del vínculo http://cdn.ca9.uscourts.gov/datastore/opinions/2014/08/18/12-56628.pdf

consentimiento afirmativo claro, que refleja manifestación de voluntad libre, específica, informada, e inequívoca del interesado.[39]

Por lo que refiere al panorama internacional, el capítulo III de la LMCE de la CNUDMI, específicamente los artículos 11 y 12, en relación con el séptimo[40], parece resolver la incógnita sobre el valor vinculante de este tipo de contratos, sobre todo aquéllos que cuentan con manifestación expresa de la voluntad a través de un clic sobre el botón "Acepto". A saber, dichos preceptos reconocen el valor jurídico y efectos de la manifestación de voluntad de las partes y se tiene por aprobada la información que pudiere figurar en el contrato digital que nos ocupa. Situación legal que es similar a lo elevado a derecho positivo en España, en términos de su Ley 34/2002, que reconoce "el consentimiento desde que se manifiesta la aceptación" y, en el caso mexicano, el artículo 93 del Código de Comercio resuelve que un acto jurídico adquirirá formalidad siempre que el mensaje de datos y su información sean accesibles para una ulterior consulta, sin importar el formato en el que se encuentre o represente.

Conforme lo sostiene Adam Gatt, más de 400 millones de personas son usuarios de la red de redes de forma diaria y las cortes deben trabajar para lograr consciencia en la sociedad sobre la contratación en línea y el valor vinculante de dichos pactos que pueden crearse con un "golpe de ratón" sobre el ícono "Yo Acepto"[41]; lo anterior, toda vez que las cortes parecen reconocer dicho *click* como un substituto válido de la firma, por ende, como un elemento adecuado para la manifestación de la voluntad del cibernauta.

VIII. 3 Derechos de consumidor *online*

La historia apunta a que en el antiguo imperio romano se acuñó el derecho a la protección del consumidor, a través de la locución "*caveat emptor*", misma que constituía la advertencia hacia el comprador, ya que cualquier riesgo debía ser asumido por éste. Tal como lo sostiene la Doctora Adriana Labardini Inzunza, Directora y

[39] DÍAZ LIMÓN, Jaime. *10 Efectos del RGPD fuera de la Unión Europea.* 26 de mayo de 2018, México. Publicaciones. Abogado Digital. Newswire. Visto el 19 de agosto de 2018 a través del vínculo http://www.jaimediazlimon.com/publicaciones/abogado-digital/rgpd-efectos-globales/

[40] A saber, el artículo séptimo de la LMCE de la CNUDMI, dicta las pautas sobre la "firma" en el ámbito electrónico: "1. Cuando la ley requiera la firma de una persona, ese requisito quedará satisfecho en relación con un mensaje de datos: a) Si se utiliza un método para identificar a esa persona y para indicar que esa persona aprueba la información que figura en el mensaje de datos…". CNUDMI. *Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996).* Visto el 21 de noviembre de 2017 a través del vínculo https://documents-dds-ny.un.org/doc/UNDOC/GEN/N97/763/60/PDF/N9776360.pdf?OpenElement

[41] GATT, Adam. *Electronic Commerce. Click Wrap Agreements.* The Enforceability of Click Wrap Agreements. University of Melbourne, Australia. Computer Law & Security Report, Vol. 18, No. 6. 2002. Visto el 29 de noviembre de 2017 a través del vínculo https://edisciplinas.usp.br/pluginfile.php/2056275/mod_resource/content/1/enforceability%20of%20clickwrap%20%28Adam%20Gatt%29.pdf

Co-Fundadora de *Al Consumidor, A. C.,* y del Centro de Investigación del Consumo y del Consumidor, ese turbio origen ya vaticinó un amplísimo objeto de estudio para economistas y tratadistas del nivel de Adam Smith, quien en su obra *La riqueza de las naciones*, apunta que el sistema mercantilista se diseñó de tal forma que el interés del consumidor es constantemente sacrificado en pos del interés del productor.[42] El Derecho del consumidor alcanzó el nivel de Derecho Humano el 15 de marzo de 1962 gracias al discurso del presidente John Kennedy, cuando éste enumera seis derechos básicos de los consumidores, dando inicio al movimiento "consumerista": 1) Derecho a productos seguros y de calidad; 2) Derecho a elegir; 3) Derecho a la información veraz; 4) Derecho a recibir educación en materia de consumo, finanzas básicas; 5) Derecho a ser escuchado y; 6) Derecho a compensación por fallas, incumplimiento o daños. Este movimiento llegó a México hasta el año 1976 con la creación del Instituto Nacional del Consumidor y su norma sustantiva, la Ley Federal de Protección al Consumidor, la cual fue reformada en el año 1992, cuando también se creó la actual Procuraduría Federal del Consumidor y contiene el reconocimiento de diez principios básicos en las relaciones de consumo y disposiciones particulares que regulan las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o cualquier otra tecnología:

> Artículo 1.- La presente ley es de orden público e interés social y de observancia en toda la República. Sus disposiciones son irrenunciables y contra su observancia no podrán alegarse costumbres, usos, prácticas, convenios o estipulaciones en contrario.
>
> El objeto de esta ley es promover y proteger los derechos y cultura del consumidor y procurar la equidad, certeza y seguridad jurídica en las relaciones entre proveedores y consumidores.
>
> I. La protección de la vida, salud y seguridad del consumidor contra los riesgos provocados por productos, prácticas en el abastecimiento de productos y servicios considerados peligrosos o nocivos;
> II. La educación y divulgación sobre el consumo adecuado de los productos y servicios, que garanticen la libertad para escoger y la equidad en las contrataciones;
> III. La información adecuada y clara sobre los diferentes productos y servicios, con especificación correcta de cantidad, características, composición, calidad y precio, así como sobre los riesgos que representen;
> IV. La efectiva prevención y reparación de daños patrimoniales y morales, individuales o colectivos;

[42] LABARDINI INZUNZA, Adriana. *Del derecho a la protección de los consumidores y a su organización*. Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas, Suprema Corte de Justicia, Fundación Konrad Adenauer. México, 2013. Visto el 11 de diciembre de 2017 a través del vínculo https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/33.pdf

V. El acceso a los órganos administrativos con vistas a la prevención de daños patrimoniales y morales, individuales o colectivos, garantizando la protección jurídica, económica, administrativa y técnica a los consumidores;
VI. El otorgamieuto de información y de facilidades a los consumidores para la defensa de sus derechos;
VII. La protección contra la publicidad engañosa y abusiva, métodos comerciales coercitivos y desleales, así como contra prácticas y cláusulas abusivas o impuestas en el abastecimiento de productos y servicios.
VIII. La real y efectiva protección al consumidor en las transacciones efectuadas a través del uso de medios convencionales, electrónicos, ópticos o de cualquier otra tecnología y la adecuada utilización de los datos aportados;
IX. El respeto a los derechos y obligaciones derivados de las relaciones de consumo y las medidas que garanticen su efectividad y cumplimiento; y
X. La protección de los derechos de la infancia, adultos mayores, personas con discapacidad e indígenas.

Los derechos previstos en esta ley no excluyen otros derivados de tratados o convenciones internacionales de los que México sea signatario; de la legislación interna ordinaria; de reglamentos expedidos por las autoridades administrativas competentes; así como de los que deriven de los principios generales de derecho, la analogía, las costumbres y la equidad.

(...)

Artículo 76 Bis.- Las disposiciones del presente Capítulo aplican a las relaciones entre proveedores y consumidores en las transacciones efectuadas a través del uso de medios electrónicos, ópticos o de cualquier otra tecnología. En la celebración de dichas transacciones se cumplirá con lo siguiente:

I. El proveedor utilizará la información proporcionada por el cousumidor en forma confidencial, por lo que no podrá difundirla o transmitirla a otros proveedores ajenos a la transacción, salvo autorización expresa del propio consumidor o por requerimiento de autoridad competente;
II. El proveedor utilizará alguno de los elementos técnicos disponibles para brindar seguridad y confidencialidad a la información proporcionada por el consumidor e informará a éste, previamente a la celebración de la transacción, de las características generales de dichos elementos;
III. El proveedor deberá proporcionar al consumidor, antes de celebrar la transacción, su domicilio físico, números telefónicos y demás medios a los que pueda acudir el propio consumidor para presentarle sus reclamaciones o solicitarle aclaraciones;
IV. El proveedor evitará las prácticas comerciales engañosas respecto de las características de los productos, por lo que deberá cumplir con las disposiciones relativas

a la información y publicidad de los bienes y servicios que ofrezca, señaladas en esta Ley y demás disposiciones que se deriven de ella;

V. El consumidor tendrá derecho a conocer toda la información sobre los términos, condiciones, costos, cargos adicionales, en su caso, formas de pago de los bienes y servicios ofrecidos por el proveedor;

VI. El proveedor respetará la decisión del consumidor en cuanto a la cantidad y calidad de los productos que desea recibir, así como la de no recibir avisos comerciales, y

VII. El proveedor deberá abstenerse de utilizar estrategias de venta o publicitarias que no proporcionen al consumidor información clara y suficiente sobre los servicios ofrecidos, en especial tratándose de prácticas de mercadotecnia dirigidas a la población vulnerable, como los niños, ancianos y enfermos, incorporando mecanismos que adviertan cuando la información no sea apta para esa población.[43]

Ordenamiento que ha servido de base para la construcción de una mejor cultura de consumo en el país, inclusive el de naturaleza digital, empero, no es la única norma que menciona principios, reglas y facultades a favor del consumidor, ya que existen leyes no especializadas como la Ley General para la inclusión de personas con discapacidad, Ley de Aviación y la Norma Oficial mexicana en materia de venta de inmuebles residenciales por inmobiliarias comerciales; que pretenden ampliar el espectro de ejecución de las facultades del consumidor.[44]

A nivel internacional, existen diversos ordenamientos que protegen al consumidor, siendo las figuras más relevantes: las *Directrices para la Protección al Consumidor de la Organización de Naciones Unidas,* el artículo 39 del *Desarrollo Integral de la Carta de la Organización de Estados Americanos* y jurisprudencia que ha emitido la Corte Interamericana de Derechos Humanos.

Sin embargo, ninguno de estos ordenamientos toca de forma precisa los derechos de cousumidor en la era digital. Al respecto, la *Unión Internacional de Telecomunicaciones* –organismo especializado de las Naciones Unidas-, reconoce que tan sólo en el año 2015 existían 3,200 millones de internautas que representan el 43.4% de la población mundial y 7,100 millones de suscripciones móviles que implican más del 95% de la población mundial; estos números parecen reflejar las ilimitadas hipótesis en las cuales los usuarios de Internet realizan compras mientras navegan. Sin duda, los principios rectores y diversos ordenamientos a nivel internacional no pueden considerarse suficientes para atender la naturaleza diversa de las prácticas digitales, por ello, en el año 1998, el Comité de Política del Consumidor de la *OCDE* formuló

[43] CÁMARA DE DIPUTADOS DEL CONGRESO DE LA UNIÓN. *Ley Federal de Protección al Consumidor.* Última reforma 9 de abril de 2012. México. Vista el 11 de noviembre de 2017 a través del vínculo https://www.profeco.gob.mx/juridico/pdf/l_lfpc_ultimo_CamDip.pdf

[44] Para una mejor referencia, consultar LABARDINI INZUNZA, Adriana, supra. Cit.

un conjunto de lineamientos generales para proteger a los consumidores en el comercio electrónico, a saber:

1. No realizar ninguna práctica que resulte falsa, engañosa, fraudulenta o desleal.
2. Las empresas dedicadas a la venta, promoción o comercialización de bienes o servicios, no deben llevar a cabo prácticas comerciales que pudieran provocar riesgos en perjuicio de los consumidores.
3. Siempre que publiquen información sobre ellas mismas o sobre los bienes o servicios que ofrecen, deben presentarla de manera clara, visible, precisa y fácilmente accesible.
4. Cumplir con cualquier declaración que hagan respecto a sus políticas y prácticas relacionadas con sus transacciones con consumidores.
5. Tomar en cuenta la naturaleza global del comercio electrónico y, en lo posible, considerar las diferentes características de las regulaciones de los mercados a los que dirigen sus ofertas.
6. No deben aprovecharse de las características especiales del comercio electrónico para ocultar su verdadera identidad o ubicación, o para evadir el cumplimiento de las normas de protección al consumidor o los mecanismos de aplicación de dichas normas.
7. No utilizar términos contractuales desleales.
8. La publicidad y la mercadotecnia deben identificar a la empresa en cuyo nombre se realizan, cuando no se cumpla este requisito se consideran engañosas.
9. Desarrollar e implementar procedimientos efectivos y fáciles de usar, que permitan a los consumidores manifestar su decisión de recibir o rehusar mensajes comerciales no solicitados por medio del correo electrónico.
10. Cuando los consumidores manifiesten que no desean recibir mensajes comerciales por correo electrónico, tal decisión debe ser respetada. En algunos países, los mensajes de información comercial no solicitada por correo electrónico, están sujetos a requerimientos legales o autorregulatorios específicos.
11. Los empresarios deben tener especial cuidado con la publicidad o mercadotecnia dirigida a los niños, a los ancianos, a los enfermos graves, y a otros grupos que probablemente no tengan la capacidad para comprender cabalmente la información que se les presenta.[45]

En ese sentido, la Procuraduría Federal Consumidor, a través de la Dirección General de Estudios sobre Consumo, realiza la puntual revisión de los sitios mexicanos que comercializan productos a través de nuevas tecnologías y verifica la legal existencia de: Política o aviso de privacidad, seguridad en datos personales y financieros,

[45] PROFECO. *Derechos del consumidor en la era digital.* El día mundial de los derechos del consumidor 2017. 15 de marzo de 2017.

domicilio físico, número telefónico fijo, descripción detallada de bienes o servicios, costos totales e impuestos, formas de pago, condiciones de envío o entrega y condiciones de cancelación, devolución o cambio.

El área de *Seguridad Informática* de la Comisión Federal de Comercio de los Estados Unidos de América, advierte sobre el peligro digital debido a la presencia de estafadores, piratas informáticos y ladrones de identidad. Sugiere actualizar software, proteger contraseñas, activar sistemas de doble autentificación, transmitir información confidencial únicamente a través de sitios web codificados y hacer copias de seguridad de los archivos.[46] Estas medidas parecerían suficientes para tener claro el panorama de una compra en línea antes de atreverse a dar clic e iniciar el acto jurídico digital, sin embargo, existen algunas consideraciones adicionales que los consumidores de la web deben tener en cuenta antes de realizar cualquier compra:

- ***Payment Card Industry Security Standars.***- El "PCI" por sus siglas en inglés, es el estándar concebido en el año 2006 por el grupo financiero denominado Consejo de Estándares de Seguridad PCI, integrado por Anuerican Express, Discover Financial Services, JCB International, MasterCard y VISA. El estándar PCI-DSS (*Payment Card Industry- Data Security Standard)* consiste en 12 normas[47], agrupadas en 6 categorías (Construir y mantener redes seguras, proteger la información del tarjetahabiente, contar con programas de pruebas de vulnerabilidades, implementar controles de acceso robustos, monitorear y probar acceso a la red regularmente y mantener políticas de seguridad de la información [Versión 3.2.]), aplicables a establecimientos que transmiten,

[46] FTC. *Información para consumidores.* Seguridad Informática. Visto el 11 de diciembre de 2017 a través del vínculo https://www.consumidor.ftc.gov/articulos/s0009-seguridad-informatica

[47] Las *Normas de Seguridad de Datos de la Industria de tarjetas de pago* de abril de 2016, constituye la versión 3.2. de los estándares que estudiamos. El consejo de Estándares de seguridad (PCI) fija las directrices para utilizarse durante las evaluaciones de cumplimiento con las PCI DSS como parte del proceso de validación de una entidad. A saber, prescribe 12 puntos de revisión de alto nivel: 1) Instalar y mantener una configuración firewall para proteger los datos del titular de la tarjeta; 2) No usur valores predeterminados suministrador por el proveedor para la contraseña del sistema y otros parámetros de seguridad; 3) Proteger los datos del titular de la tarjeta que se han almacenado; 4) Cifrar la transmisión de los datos del titular de la tarjeta en redes públicas abiertas; 5) Proteger los sistemas contra malware y contar con actualizaciones de antivirus; 6) Desarrollar y mantener sistemas y aplicaciones seguros; 7) Restringir el acceso a los datos del titular de la tarjeta según las necesidades de saber que tenga la empresa; 8) Identificar y autenticar el acceso a los componentes del sistema; 9) Restringir el acceso físico a los datos del titular de la tarjeta; 10) Rastrear y supervisar todos los accesos a los recursos de red y a lso datos del titular; 11) Probar periódicamente los sistemas y procesos de seguridad; 12) Mantener una política que aborde la seguridad de la información para todo el personal. CONSEJO SOBRE NORMAS DE SEGURIDAD DE LA PCI, LLC. *Normas de Seguridad de Datos de la Industria de tarjetas de pago.* Abril de 2016. Versión 3.2. Recuperado el 11 de diciembre de 2017 a través del vínculo https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3-2_es-LA.pdf

procesen o almacenen datos de tarjetas de crédito. La fortaleza de estas normas estandarizadas ha obligado a que la industria financiera digital adopte esta certificación como mecanismo de autenticación de sitios web y como garantía de protección a favor del consumidor. Los portales que cuentan con esta validación, han pasado por un proceso de auditoría informática realizada por un *Qualified Security Assesor* (QSAs) y en todo caso, se muestra al consumidor el logo (marca mixta) que hace referencia a la certificación PCI. Si bien esto no puede garantizar ausencia absoluta de complicaciones en la operación digital, brinda certeza respecto del tratamiento de los datos bancarios que podrían ocuparse para celebrar el acto jurídico.

I. El estándar PA-QSA (*Payment Application-Qualified Security Assesor),* es aplicable a los fabricantes de software y cualquiera que desarrolle aplicaciones que realicen el tratamiento, archivo y transmisión de datos del tarjetahabiente o de la tarjeta.

- **Ley *Sarbanes-Oxley.***- A diferencia de la certificación PCI que referí anteriormente, el *SOX* es un ordenamiento de derecho positivo emitido por el gobierno de los Estados Unidos de América. SOX es la abreviatura para la ley americana "*Sarbanes Oxley Act"* cuya emisión se fechó en julio de 2002 en los Estados Unidos de América.[48] La propuesta legislativa del diputado Michael Oxley y el senador Paul Sarbanes, son el resultado de escándalos financieros americanos y propone manejo de controles contables internos y seguimiento de estándares de calidad previo a la celebración de auditorías dirigidas por entidades certificadoras americanas. De forma particular, su capitulado se divide de la siguiente forma:

I. Junta de consejo abierta a contabilidad pública de la compañía
II. Independencia del auditor
III. Responsabilidad corporativa
IV. Contenido de reportes financieros
V. Análisis de conflicto de intereses
VI. Autoridad de la Comisión de Recursos
VII. Estudios y Reportes
VIII. Fraude corporativo y criminal derivado de la contabilidad
IX. Tratamiento y penas de los delitos de cuello blanco
X. Devolución de impuestos

[48] CONGRESO DE LOS ESTADOS UNIDOS DE AMÉRICA. *Public Law 107-204-Julio 30, 2002 Sarbanes-Oxley Act of 2002. Corporate responsibility.* Congreso 107°mo. Visto el 11 de diciembre de 2017 a través del portal https://www.sec.gov/about/laws/soa2002.pdf

La importancia detrás del cumplimiento de la Ley SOX, radica en la aplicabilidad internacional. Este ordenamiento obliga a las personas jurídicas foráneas que celebren operaciones de forma tradicional en territorio de los Estados Unidos de América o bien, cuyas relaciones comerciales son preponderantemente con entidades americanas, a cumplir los procesos de manejo de contabilidad, transparencia en estados financieros y en su caso, cumplimiento a las leyes en materia de anticorrupción de la Unión Americana, así como registrar su comportamiento ante la *Securities and Exchange Comission* ("SEC" por sus siglas en inglés). A favor del consumidor, implica la certeza de realizar una operación con una empresa que cuenta con altos estándares de control contable, confiable, código de ética obligatorio y un comité de auditoría que controla los recursos de la empresa. En ese sentido, a pesar de celebrar la operación con la versión digital de dicha entidad, el respaldo de su gobierno corporativo y las normas que cumple, permite una fácil detección en caso de requerir reclamar el ejercicio de algunas de sus facultades como consumidor.

VIII. 4 Tratamiento legislativo de las Criptomonedas

Milton Friedman fue un economista ganador del Premio Nobel, gracias a sus logros en los campos de análisis de consumo, historia y teoría monetaria, estudioso de la política de estabilización y uno de los defensores más famosos de la doctrina sobre el *libre mercado.* Se le considera el fundador de los "*Chicago Boys*", junto con Arnold Harberger y un selecto grupo de académicos de la Universidad de Chicago que defendían dichos postulados y educaban a sus estudiantes bajo la modalidad *neoliberal.*

En 1999, el economista americano Friedman, fue entrevistado por *National Taxpayers Union;* intervención que le permitió hablar sobre política tributaria criminal y la participación de la tecnología en las facultades de tributación, en lo particular, destacan dos postulados que parecen vaticinar la actualidad económica digital: 1) Internet hará más difícil recolectar impuestos derivado de la facilidad de movilidad de los ciudadanos; y 2) Se creará un "e-cash" confiable (minuto 14:17) a través del cual podrás transferir fondos de "A" a "B" sin que ninguna de las partes se conozcan, ni su origen. Sin embargo, el premio Nobel de economía también tuvo la visión que esto podría complicar no sólo la recaudación de impuestos, sino la proliferación de actos delictivos, fraudulentos y redes de delincuencia que aprovecharían a Internet como un mecanismo para realizar de forma más sencilla sus transacciones ilegales.[49]

[49] Puede consultar la entrevista completa, a través del vínculo https://www.youtube.com/watch?v=mlwxdyLnMXM&feature=youtu.be Visible el 01 de diciembre de 2017. NATIONAL TAXPAYERS UNION. *Milton Friedman Full Interview on Anti-trust and Tech. YouTube.* Entrevista de 1999

La vida no le daría oportunidad a Friedman para experimentar el origen, crecimiento geométrico y popularización de las "Criptomonedas". Fue hasta el 2008 cuando el grupo japonés de desarrolladores, *Satoshi Nakamoto* (pseudónimo bajo el cual opera este club de desarrolladores), liberó la moneda virtual descentralizada denominada *Bitcoin (BTC*[50]*)*. La misma ocupa tecnología *peer-to-peer* para operar sin una autoridad central o institución bancaria, construida bajo lenguaje de programación *open source*. La celebración de transacciones (enajenaciones, cesión de derechos y otras figuras jurídicas) con esta criptomoneda (a este acto se le conoce como *mining*)[51] se soporta gracias a la fe que tiene la red en la misma, tal como si fuere dinero tradicional que se sostiene debido a la confianza que tienen los ciudadanos sobre el papel o metal que poseen, respecto de la representación comercial que pudieren tener en las arcas de la nación.

En particular, esta criptomoneda imita características de una tarjeta de crédito: i) Pagos internacionales, ii) Bajo costo de transacción, iii) Transacciones irreversibles de mercancías y, iv) Seguridad derivada de la encriptación de la operación.

Satoshi creó un mecanismo alternativo de pago como respuesta al crecimiento de las operaciones digitales, cuya motivación principal fue contar con una moneda electrónica que no fuere afectada por países, bancos o negocios. Respecto al control propuesto por los desarrolladores *Nakamoto*, sólo se liberó la cantidad –inmutable- de 21 millones de *Bitcoins* alrededor de la web, los cuáles pueden ser divididos en montos tan grandes o pequeños en atención al valor que obtengan los mismos en el mercado digital; la unidad divisible más pequeña se le conoce como *Satoshi*.

La página oficial del *BTC* percibe grandes ventajas del uso de criptomonedas frente al dinero tradicional centralizado: 1) El uso de software de código abierto permite completa transparencia en las operaciones que se celebran con dicha moneda; 2) Derivado de lo anterior, el sistema permite el uso de registros públicos de operaciones (*public ledger*), llamado *blockchain,* el cual registra la transacción empleando

publicada el 09 de agosto de 2012: "…*One thing that's missing but will soon be developed is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A – the way I can take a $20 bill and hand it over to you, and you may get that without knowing who I am..*"

[50] El diccionario OXFORD lo define como "un tipo de moneda digital cuyas técnicas de encriptación son usadas para regular la generación de unidades de dinero y verificar la transferencia de fondos, y cuya operación es independiente de un banco central…" *Bitcoin.* https://en.oxforddictionaries.com/definition/bitcoin visto el 01 de diciembre de 2017.

[51] Según la FinCEN, podemos definir a los "miners" como las personas que crean unidades de moneda virtual convertibles y venden dichas unidades a otra persona por moneda "real" o su equivalente y se considera un transmisor de dinero. HUDAK, Steve. *FinCEN Publishes Two rulings on Virtual Currency Miners and Investors.* FinCEN. Washington, Enero 20 del 2014. Visto el 01 de diciembre de 2017 a través del vínculo https://www.fincen.gov/news/news-releases/fincen-publishes-two-rulings-virtual-currency-miners-and-investors

los números de cuenta del usuario sin utilizar información personal; 3) El envío de fondos sin tiempo de espera o aceptación bancaria, en cualquier lugar y momento.[52]

Hasta ahora, más de 6 millones de usuarios ocupan la moneda *Bitcoin*, esto permite que empresas como *Wordpress* y *Subway* la reconozcan como un método de pago para celebrar transacciones y que su valor estimado oscile en 1BTC= $9613.31 USD, es decir, cada *Bitcoin* se podría traducir en casi diez mil veces su valor frente al dólar americano.

De esta forma, se sostiene la teoría monetaria tradicional de la cual depende cualquier sistema financiero, ya que el valor del *BTC* se determina conforme a la disponibilidad y demanda, es decir, cuando la demanda aumenta así lo hace su precio, en tanto que puede disminuir si la confianza sobre la moneda cae y la demanda con ello.[53] Este último modelo podría significar la *espada de Dámocles* en la construcción de un argumento sólido para defender a las criptomonedas, ya que tal como reconoce el Post-Doctor de la Universidad de Munich en Alemania, Beate Sauer, el trabajo de un banco centralizado es brindar estabilidad a la moneda que avala, así como al sistema financiero, en tanto que la moneda electrónica depende del comportamiento del mercado, única y exclusivamente, para fijar el precio de dicha moneda a la compra y venta. Ahora bien, a nivel internacional se ha presentado preocupación real sobre la aplicación monetaria de dinero virtual en la celebración de transacciones en el mundo *off line*, al respecto, el Banco de Inglaterra y el Banco Central Europeo[54] han manifestado que esto podría afectar el nivel de precios de la economía, así como la cantidad y la velocidad de rotación de dinero centralizado.

En ese tenor debe ser clara la postura de los Bancos centralizados, ya que la creación de criptomoneda (*mining*), en algún momento histórico y económico, implicaría la substitución de moneda nacional, lo que obligaría a los bancos centralizados a

[52] La página oficial PATENTSCOPE, que depende de la Organización Mundial de la Propiedad Intelectual, brinda el antecedente jurídico e histórico más serio por lo que refiere al tratamiento del *Bitcoin*. En agosto de 2016, Stephen Mollah recibió el registro internacional, la publicación y reconocimiento de la patente denominada "Bitcoin technology", a través de la cual se obtuvo protección respecto de la tecnología como un mecanismo electrónico de pago dentro de una red, que requiere un algoritmo digital binario que es transparente y auténtico, así como soportado por un sistema financiero digital auto regulable. PATENTSCOPE/WIPO. *Search International and National Patent Collections. Bitcoin Technology*. 24 de febrero de 2015. Visto el 02 de diciembre de 2017 a través del vínculo https://patentscope.wipo.int/search/en/detail.jsf;jsessionid=1A75938928EB9E338D4E14DB8AB2C578.wapp2nB?docId=GB176139235&recNum=1&office=&queryString=bitcoin+&prevFilter=&sortOption=&maxRec=1817

[53] BITCONNECT. *What is Bitcoin?* Visto el 01 de diciembre de 2017 a través del vínculo https://bitcounect.co/bitcoin-information/2/what-is-bitcoin

[54] Para lectores especializados en la materia, no resulta óbice a dicha manifestación, la existencia de la Directiva 2009/110/EC sobre dinero electrónico, ni la Directiva 2007/64/EC sobre Servicios de Pago, ya que ninguna de ellas tiene como fin primordial la regulación de criptomonedas, sino la vigilancia de la moneda de circulación legal bajo modalidades virtuales y sistemas de pago electrónicos.

ajustar sus políticas a la baja demanda de dinero, provocando inflación y baja circulación monetaria.

El profesor Sauer es preciso en sus afirmación y propuestas económicas para incentivar o reducir el uso de criptomonedas, además, comparte una postura que me parece clara y popular entre los Bancos centrales, ya que estos no buscan regular el uso de moneda electrónica, por el contrario, pretenden desincentivar su uso, así como provocar su falla, mediante la propuesta de políticas financieras que inviten a los ciudadanos a celebrar transacciones con moneda nacional.[55]

En ese tenor, la librería del Congreso de los Estados Unidos de América mantiene una lista actualizada del comportamiento gubernamental de algunas naciones frente a las criptomonedas;[56] listado del que se advierte ausencia legislativa sobre dichas monedas virtuales, en tanto que países como Nueva Zelanda,[57] Dinamarca, Islandia y Eslovenia se pronunciaron expresamente en contra del uso de criptomonedas derivado del efecto negativo sobre sus economías y prohibieron su uso, independientemente del reconocimiento sobre la falta de poder directo para regular medios alternativos de pagos y, en países de corriente "criptofavorable" como Alemania, Francia, Finlandia, Israel, Noruega, Portugal se ha aceptado a este tipo de moneda bajo una perspectiva fiscalizadora, por lo que refiere a las ganancias gravables que pudieren surgir de la inversión y adquisición de monedas electrónicas.

Situación *sui generis* ocurre en España, nación en la que si bien no se brinda valor monetario a las criptomonedas, se les otorga el valor jurídico de **bienes digitales** (sugiero al lector se remita al capítulo I de la presente obra). Pocos casos como el brasileño, cuya ley 12.865 crea la posibilidad de incorporar al sistema de pagos nacional la creación de monedas electrónicas, incluida el *BTC* y dota de facultades a su banco central para crear las normas e instrucciones necesarias para regular y, en su caso, sancionar la indebida utilización de criptomonedas y desaparecerlas del mapa financiero; en la parte conducente prescribe:

[55] SAUER, BEATE. *Central bank behaviour concerning the level of bitcoin regulations as a policy variable*. Athens Journal of Business and Economics. Athens Institute for Education & Reasearch (A World Association of Academics and Researchers. Grecia. Octubre de 2015. Visto el 01 de diciembre de 2017 a través del vínculo http://www.athensjournals.gr/business/2015-1-4-1-Sauer.pdf

[56] LIBRARY OF CONGRESS. *Regulation of Bitcoin in selected jurisdictions*. Estados Unidos de América. Dirección de Búsqueda Global Legal. Enero de 2014. Puede consultar el listado en el vínculo https://www.loc.gov/law/help/bitcoin-survey/ visto el 01 de diciembre de 2017.

[57] El texto original prescribe: "…The Reserve Bank of New Zealand Act prohibits the issuance of bank notes and coins by any party other than the Reserve Bank. However, the Reserve Bank has no direct power over any form of alternative payments medium. Non-banks do not need our approval for schemes that involve the storage and/or transfer of value (such as 'bitcoin') – so long as they do not involve the issuance of physical circulating currency (notes and coins)."

SPB (Sistema de Pagamentos Brasileiro) / The Brazilian Payments System. Law 12, 865

[...] Art. 6. – Para efecto de las normas aplicables a los sistemas de pago y las entidades de pago que pasen a formar parte del Sistema de pagos brasileños (SPB), en términos de esta ley, se deberán considerar las siguientes definiciones: I: esquemas de pago: conjunto de reglas y procedimientos que regulan la provisión de ciertos servicios de pago al público aceptados por más de un destinatario / beneficiario, mediante el acceso directo por los usuarios finales, los pagadores y los destinatarios / beneficiarios; II- propietario del plan de pago: una entidad legal responsable de un plan de pago y, cuando corresponda, mediante el uso de la marca asociada al plan de pago; III- institución de pago: persona jurídica, que se adhiere a uno o más esquemas de pago, que tiene como actividad principal o auxiliar: a) proporcionar servicios de cobro y retiro de los fondos mantenidos en cuentas de pago; b) realizar o facilitar instrucciones de pago relacionadas con el servicio de pago definido, incluidas las transferencias originadas o destinadas a una cuenta de pago; c) administrar cuentas de pago; d) emitir un instrumento de pago; e) adquirir un instrumento de pago; f) remesas; g) convertir moneda física o saldo en dinero electrónico, o viceversa, adquirir la aceptación o administrar el uso del dinero electrónico; y h) otras actividades relacionadas con la prestación de servicios de pago, designadas por el Banco Central de Brasil [...]

Art. 7. - Los esquemas de pago y las entidades de pago deberán observar los siguientes principios de acuerdo con los parámetros que establecerá el Banco Central de Brasil, de conformidad con las directrices del Consejo Monetario Nacional: I-interoperabilidad dentro del esquema de pago y entre diferentes esquemas de pago; II- solvencia y eficiencia de los sistemas de pago e instituciones de pago, promoción de la competencia y provisión para transferencias de saldos de dinero electrónico, cuando corresponda, a otros esquemas de pago o instituciones; III- acceso no discriminatorio a las infraestructuras y servicios necesarios para el funcionamiento del sistema de pago; IV- satisfacer las necesidades de los usuarios finales, en particular con respecto a la libertad de elección, seguridad, protección de sus intereses económicos, trato no discriminatorio, privacidad y protección de datos personales, transparencia y acceso a información clara y completa sobre el servicio; V- confiabilidad, calidad y seguridad de los servicios de pago; y VI- inclusión financiera, en cumplimiento de los estándares de calidad, seguridad y transparencia en todos los esquemas de pago [...]

Art. 9. - El Banco Central de Brasil, de acuerdo con los lineamientos establecidos por el Consejo Monetario Nacional, deberá: I- regular los esquemas de pago; II- regular la constitución, operación y supervisión de las entidades de pago, así como la continuidad del servicio; III- limitar el objeto estatutario en las cláusulas de las instituciones de pago; IV- autorizar esquemas de pago que operan en el país; V- autorizar la constitución, operación, transferencia de control, fusión, escisión y adquisición de la entidad de pago, incluso cuando involucre la participación de una persona física o jurídica no residente; VI- establecer las condiciones para cualquier posición en los

> órganos estatutarios de la institución de pago; VII- supervisar los esquemas de pago y aplicar las sanciones apropiadas; VIII- supervisar las instituciones de pago y aplicar las sanciones apropiadas; IX- adoptar medidas preventivas, con el objetivo de asegurar la solidez, la eficiencia y el funcionamiento adecuado de los sistemas de pago y las instituciones de pago, incluyendo: a) establecer límites mínimos de operación [...][58]
> [Traducción del autor]

Así las cosas, resulta clara la postura del gobierno de la entonces presidenta Dilma Roussef, quien propuso la incorporación de las criptomonedas a un sistema centralizado y regulable de Brasil, además otorgó facultades amplísimas a su Banco Central para evitar la incorporación de monedas virtuales que no cumplieran con los principios de **interoperabilidad, solvencia y eficacia, no discriminación, conocimiento de las necesidades del consumidor final, seguridad, protección de intereses económicos, protección de datos personales, transparencia del servicio; confianza, calidad y seguridad en el sistema de pagos e inclusión financiera** –quizá el más relevante-.

Este último componente faculta al Banco brasileño de potestad regulatoria respecto del comportamiento de las criptomonedas, inclusive para limitar el número de operaciones que pudieren celebrarse con éstas, dentro del sistema financiero. A parecer de quien escribe, la ley cuenta con un espíritu noble por lo que refiere a la incorporación paralela de las monedas virtuales al sistema tradicional, sin embargo, permite que el filo de la espada de Dámocles caiga sobre éstas y desincentiva la utilización de aquellas ante la probabilidad que no fueren reconocidas como método legal de pago ante un exceso de su uso frente a la moneda de circulación legal y atenta contra el fin primordial de las criptomonedas, esto es, ser un mecanismo virtual y descentralizado de pago.

Por otro lado, políticas de índole criminal han surgido en países como México y Estados Unidos de América; naciones en las que se ha reservado el estudio de las criptomonedas al riesgo que podría implicar en materia de lavado de dinero. En el caso mexicano, si bien es cierto la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, de 17 de octubre de 2012, no prohíbe de forma expresa la utilización de criptomonedas, restringe cierto tipo de operaciones que se efectúen mediante pago electrónico rastreable y centralizado, en términos de su artículo 32; adicionalmente, constriñe al cumplimiento de las conductas prescritas en dicho precepto, mediante la formalización ante fedatario público y

[58] BANCO CENTRAL DO BRASIL. *Law 12,865 de octubre 9 de 2013.* SPB (Sistema de pagamentos Brasileiro). Regulación de esquemas de pago e instituciones de pago que de ahora en adelante formarán parte del Sistema de Pagos Brasileño. Traducción de portugués a inglés por *DEBAN (Department of Banking Operations and Payments System).* Puede consultar el texto íntegro a través vínculo https://www.bcb.gov.br/Pom/Spb/Ing/InstitucionalAspects/Law12865.pdf visto el 01 de diciembre de 2017.

la plena identificación de la forma en que se resolvió la deuda.[59] Por su lado, la *Money Laundering Control Act of 1986*, prevé la posibilidad de celebración de operaciones con "instrumentos monetarios" diferentes a la moneda de circulación legal americana, empero, dicta vigilancia superior sobre dichas operaciones ante el riesgo que éstas pudieren tener un objeto ilícito.

Esta Acta prescribe sanciones penales y administrativas, a los particulares que no notifiquen al gobierno americano sobre operaciones que excedan los diez mil dólares o, en su caso, respecto de aquellas que soporten el cumplimiento de la obligación en instituciones o monedas diversas a las americanas, tal como lo sería el caso del uso de criptomonedas.

Uno de los casos más populares en la aplicación de sus normas anti lavado, ocurrió en julio de 2017, cuando la *Financial Crimes Enforcement Network (FinCEN)* en colaboración con el Abogado Principal de la oficina del Distrito Norte de California, lograron el arresto del ruso Alexander Vinnik, uno de los operadores de la plataforma BTC-e, por permitir el uso de monedas virtuales (Bitcoin, Litecoin, Namecoin, Novacoin, Peercoin, Ethereum y Dash) en la adquisición de *ransomware* y obtención de servicios de hackeo, robo de identidad, fraude fiscal, corrupción y tráfico de drogas. El incumplimiento de las normas americanas, se deriva de la utilización de fondos por usuarios que emiten y reciben pagos en territorio de los Estados Unidos de América; por lo que se condenó al criminal ruso al pago de una pena por doce millones de dólares y se declaró la existencia de violaciones a la ley americana, a la política *Anti-Money Laundering* y la infame *USA PATRIOT Act.*[60]

Sin que resulte óbice a los anteriores argumentos, parece ser que el criterio internacional invita a no reconocer, al menos jurídicamente, la posibilidad de considerar "moneda" a las criptomonedas; tal como ocurrió en el caso *California Bankers Association v. Schultz*, en el que la Suprema Corte de los Estados Unidos de América definió el término "moneda", como aquella que se regula y tiene circulación legal en Estados Unidos o cualquier otro país, asimismo, que tradicionalmente es aceptada como dinero en el país que la emite.[61] Bajo dicha perspectiva, parece que *Bitcoin* y otras criptomonedas, no cuentan con el tratamiento jurídico para calificar como

[59] CONGRESO DE LA UNIÓN. *Ley Federal para la prevención e identificación de operaciones con recursos de procedencia ilícita.* Publicado el 17 de octubre de 2012 en el Diario Oficial de la Federación. México. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPIORPI.pdf

[60] HUDAK, Steve. *FinCEN Fines BTC-e Virtual Currency Exchange $110 million for facilitating ransomware, Dark Net Drug Sales*. United States Department of the Treasury. FinCEN. Julio 27 del 2017. Visto el 01 de diciembre de 2017 a través del vínculo https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware

[61] MANDJEE, Tara. *Bitcoin, its Legal Classification and its regulatory framework.* Journal of Business and securities law. Michigan State University. College of Law. Digital Commons at Michigan State. Volume 15. Issue 2. Article 4. 2015. Disponible a través del vínculo https://digitalcommons.law.msu.edu/jbsl/vol15/iss2/4 visto el 01 de diciembre de 2017.

"moneda". En ese sentido, algunos expertos, como el Director de *Bain Venture Capital,* Salil Deshpande, describen a las criptomonedas como una "comodidad", una inversión a lo máximo[62] no como "moneda" de circulación legal.

Una de las salidas económicas y legales que reconozco por su practicidad y empoderamiento gubernamental, es la ocurrida en el Estado de Nueva York. Como respuesta al crecimiento de operaciones que solventan el pago de las mismas con criptomonedas, el Departamento de Servicios Financieros (NYDFS por sus siglas en inglés), lanzó al mercado la propuesta de reglas y regulaciones para la utilización de monedas virtuales en negociaciones dentro de su jurisdicción. Al respecto, el NYDFS publicó la *Part 200. Virtual Currences* del Capítulo Primero, denominado *Regulations of the Superintendent of Financial Services*. Bajo este ordenamiento, se obliga a las personas físicas y morales que celebren operaciones con moneda virtual y que pretendan recibir, transmitir, almacenar y convertir moneda virtual a moneda de circulación legal, a adquirir una licencia gubernamental para perfeccionar dichas transacciones en su jurisdicción. Este ordenamiento brinda una de las mejores disecciones a las monedas virtuales, en términos jurídicos, ya que no sólo define a las monedas virtuales, sino que fija las características que deben cumplir para considerarse como tales, frente a otras monedas digitales:

> Sección 200.2 Definiciones Para los propósitos de esta Parte solamente, se aplicarán las siguientes definiciones:
>
> [...]
>
> (p) Moneda virtual significa cualquier tipo de unidad digital que se usa como medio de intercambio o una forma de valor almacenado digitalmente. Se entiende por moneda virtual, en términos generales, a las unidades de cambio digitales que (i) tengan un repositorio centralizado o administrador; (ii) están descentralizados y no tienen un repositorio centralizado o administrador; o (iii) puede ser creado u obtenido mediante un esfuerzo informático o de fabricación. No se entenderá como Moneda Virtual a ninguna de las siguientes: (1) unidades digitales que (i) se utilizan únicamente dentro de plataformas de juegos en línea, (ii) no tienen mercado o aplicación fuera de esas plataformas de juegos, (iii) no se pueden convertir en, o canjeado por, Moneda Fiat o Moneda Virtual 6, y (iv) puede o no ser canjeable por bienes, servicios, descuentos o compras en el mundo real. (2) unidades digitales que pueden canjearse por bienes, servicios, descuentos o compras como parte de un programa de afinidad o recompensas del cliente con el emisor u otros comerciantes designados o pueden canjearse por unidades digitales en otro programa de afinidad o recompensas del cliente, pero no puede

[62] *FORBES*. "Top predictions for 2014 by VCs. Think of Bitcoin as a commodity, not a currency". 2014. Visto el 01 de diciembre de 2017 a través del vínculo https://www.forbes.com/pictures/ekij45gjle/think-of-bitcoin-as-a-commodity-not-a-currency-2/#6c13c6002a78

convertirse ni canjearse por Moneda Fiat o Moneda Virtual; o (3) unidades digitales usadas como parte de tarjetas prepagas (…)"[63] [Traducción del autor]

(El énfasis es añadido)

De dicho apartado se desprende que por moneda virtual debemos entender cualquier tipo de unidad digital que sea usada como un medio de intercambio o forma de valor almacenado (valor representativo), sin que se considere como tal a las unidades digitales que surjan y tengan aplicación exclusiva en plataformas de juegos y que no puedan convertirse en dinero legal o virtual, ni que impidan reclamar descuentos, compras o bienes del "mundo real". Una de las desventajas claras a dicho ordenamiento, es la obligación del licenciatario de ofrecer un pago inicial (similar a la fianza) por cinco mil dólares para garantizar el uso responsable de la licencia e iniciar el procedimiento de obtención de la misma; asimismo, se obliga a mantener un registro paralelo de las operaciones de conversión que realice, independientemente del *blockchain* que exista en la *Virtual Currency Business Activity.*

En ese tenor, los sujetos inmediatos de regulación son los conocidos "mineros", en tanto que estos requieren de la licencia para obtener pagos en moneda legal por las criptomonedas que pretendan vender, en tanto que los usuarios ordinarios de compra y venta de bienes u obtención de servicios no requieren la adquisición de la licencia, pues su objeto principal no es el *mining*.

Si se trata de citar casos de apoyo gubernamental e integración de las políticas públicas a la realidad tecnológica, es meritorio invocar el caso de Corea del Sur. Dicha nación es reconocida como líder en el área de tecnología e innovación y hasta el 2016, se le consideraba como el tercer país más exitoso en materia de implementación de políticas *E- Government*, según el *Global Innovation Index*.

Para febrero de 2015, el gobierno estuvo involucrado de forma activa en el desarrollo de tecnologías *Blockchain* y organizó intercambios semanales de criptomonedas. Adicionalmente, el país presidido por Moon Jae-in, patrocina la competencia de empresas emergentes que desarrollen tecnología *Bitcoin*, en la que también se involucra la iniciativa privada. Actualmente, dicha república cuenta con dos notables iniciativas en materia de *Blockchain:* i) Uso del blockchian para el voto de comunidades locales. Dicha tecnología se desarrolló con apoyo de *Blocko* y actualmente permite la captura de más de 9,000 votos; ii) Innovación financiera con base en Blockchain, bajo la consigna y seguridad gubernamental, que sostiene que este tipo de tecnología será la solución para la industria *Fintech.*[64] En ese tenor, la República de

[63] NEW YORK STATE/ DEPARTMENT OF FINANCIAL SERVICES. *Chapter 1. Regulations of the superintendent of financial services. Part 200. Virtual Currencies.* Edición de 24 de junio de 2015. Visible a través del vínculo http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

[64] OJO, Adegboyega/ MILLARD, Jeremy. *Government 3.0- Next Generation Government Technology Infraestructure and Services.* Editorial Springer. Suiza, 2017. Puede consultar la

Corea no sólo ha encontrado favorable el desarrollo tecnológico de empresas emergentes, sino que ha buscado implementar dichos sofisticados algoritmos en la implementación de estrategia política, electoral y financiera.

En los términos expuestos, parece inconcuso que el panorama regulatorio de las criptomonedas es ambiguo e incierto hasta nuestros días, empero, el aumento en la confianza de los cibernautas frente al uso de moneda centralizada, podría ocasionar la pronta atención de los organismos internacionales y fijar una postura homogénea. Caso claro de lo anterior, es lo que ocurrió en marzo 16 del 2013 en la República de Chipre, cuando el presidente Nicos Anastasiades pretendió confiscar dinero de cada cuenta de banco para solventar la crisis bancaria de aquel país, esto llevó a los ciudadanos e inversionistas a transformar su dinero en moneda virtual, específicamente *Bitcoin*, lo que llevó a dicha moneda a obtener un tipo de cambio de hasta 65 dólares[65]; en el caso concreto, la moneda electrónica mostró mayor fortaleza respecto de aquella que procura y defiende el Estado.

Según un estudio publicado recientemente por la Universidad de Cambridge (Reino Unido) titulado *Global Cryptocurrency Benchmarking Study*, reconoce que existen entre 2.9 millones y 5.8 millones de usuarios de monederos de criptomoneda, asimismo, manifiesta que al menos 1 876 personas cuentan con empleo de tiempo completo gracias a la industria de las monedas virtuales. Dicho estudio abarcó el territorio de Asia, África, Europa, Norte América y Latinoamérica y estima que el mercado de criptomonedas hoy cuenta con 27 billones de dólares en circulación, hacia abril de 2017, cuyos referentes más populares son *Bitcoin, Ether (ETH), Dash, Monero (XMR), Ripple (XRP), Litecoin (LTC),* empero, afirma que existen más de 132[66] monedas virtuales utilizadas alrededor del globo.[67] Bajo esa perspectiva, luce inverosímil proponer el licenciamiento de programas de cómputo que permitan la conversión de dichas monedas a dinero de circulación legal, asimismo, luce inasequible el pretender legislaciones hipotéticas respecto de cada criptomoneda; en ese tenor, parece que la propuesta brasileña de incorporación sistemática financiera podría ser una mejor respuesta económica, política y jurídica, sin embargo, para una debida implementación, debería reconocer la flexibilidad y auto-regulación que

versión digital a través del vínculo https://books.google.com.mx/books?id=VaI7DwAAQBAJ&lpg=PA297&ots=Rgh4_0pSHZ&dq=bitcoin%20wipo&hl=es&pg=PR7#v=onepage&q=bitcoin%20wipo&f=false

[65] BUSTILLOS, María. "The bitcoin Boom". The New Yorker. Elements. Abril 1 de 2013. Visto el 01 de diciembre de 2017 a través del vínculo https://www.newyorker.com/tech/elements/the-bitcoin-boom

[66] Algunos sitios como *coinmarketcap.com* estiman que existen más de 1800 criptomonedas, sin embargo, resulta un mero pronóstico carente de metodología en su investigación y afirmación.

[67] HILEMAN, Garrick y RAUCHS, Michel. *Global cryptocurrency benchmarking study.* Cambridge Centre for Alternative Finance. University of Cambridge. Judge Business School. With the Support of *VISA*. Reino Unido, 2017. Visible el 01 de diciembre de 2017 a través del vínculo https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

cada moneda tiene, en el entendimiento que buscar centralizar cada una de estas, podría provocar abandono de la moneda legalmente reconocida e invitar la celebración de operaciones ilegales o irrastreables en perjuicio del sistema financiero, provocando su modificación o desaparición, tal como lo conocemos.

A esto apuestan colosos digitales como *Deloitte*, quien hace un par de semanas anunció su colaboración con *Waves* y Ethereum para desarrollar un estándar de ofertas iniciales de monedas, lo que implicaría contar con un cuerpo auto-regulatorio de monedas digitales y de cualquier tecnología *blockchain;* esta tecnología permitirá –en teoría- generar reportes de carácter legal, tributario y contables, así como tecnología suficiente para implementar políticas *KYC* ("Conoce a tu cliente" por sus siglas en inglés) y *due diligence.*

Al respecto, Artem Tolkachev, Líder Corporativo Blockchain de *Deloitte CIS*, manifestó que la "digitalización (*"tokenisation")* de la economía y el aumento de fondos en las criptomonedas se mantendrá en los próximos años, por su parte, Alexander Ivanov, CEO y fundador de *Waves Platform* reconoce que la regulación es un fenómeno emergente y concierne al "criptoespacio" sentar las bases para las jurisdicciones que aún no han manifestado sus intenciones sobre el tratamiento de las criptomonedas[68]; esto parece señalar un camino cierto y de fortaleza jurídica hacia criptomonedas como Ethereum, en tanto que otras más populares que apuestan a la descentralización absoluta, como Bitcoin, generan dudas y especulaciones que provocan la ira de expertos economistas y banqueros poderosos, al llamarla la "burbuja especulativa" más grande de la historia, que en breve podría convertirse en el fraude más grande de la economía moderna. [69]

VIII. 5 Ley Fintech (México)[70]

El comercio electrónico no sólo opera a través contratación digital y actos jurídicos de adhesión virtual. Con el crecimiento de la red de redes y el movimiento económico

[68] KUTSENKO, Ekaterina. *Waves Platform, with the support of leading market players, is founding new self-regulatory body to set standars for ICO's (Initian Coin Offering).* DELOITTE CIS. Rusia, Moscú, 11 de diciembre de 2017. Visto el 13 de diciembre de 2017 a través del vínculo https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/about-deloitte/pressrelease/waves-platform-en.pdf

[69] FLORIO, Luis. "Bitcoin de récord: ¿es todo una estafa?" *La Vanguardia*. Economía. El futuro de las divisas. España, 30 de noviembre de 2017. Visto el 13 de diciembre de 2017 a través del vínculo http://www.lavanguardia.com/economia/20171130/433291143335/comprar-bitcoin-invertir-estafa.html

[70] Puede consultar el texto íntegro del proyecto del Ejecutivo Federal, así como la exposición de motivos, a través del vínculo http://www.senado.gob.mx/sgsp/gaceta/63/3/2017-10-12-1/assets/documentos/Iniciativa_Ejecitvo_Federal.pdf Asimismo, puede consultar el *Decreto por el que se expide la Ley para Regular las Instituciones de Tecnología Financiera y se reforman, adicionan y derogan diversas disposiciones de la Ley de Instituciones de Crédito, la Ley del Mercado de Valores, la Ley General de Organizaciones y Actividades Auxiliares del Crédito, la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, la Ley para Regular las Sociedades de Información Crediticia, la Ley*

y monetario de los internautas, pronto se volvió una necesidad el surgimiento de servicios financieros en el ciberespacio; de esa forma surgieron las "*Finance Technology (*Fintech)". Éstas son empresas que ofrecen productos y servicios financieros mediante la incorporación de nuevas tecnologías de la información y comunicación que pueden resumir su implementación en algo tan simple como una página web, presencia en redes sociales y aplicaciones móviles, hasta la generación de propios mecanismos de pago y creación de nuevas modalidades de financiamiento digital.

Tan sólo en México, se estima que existen alrededor de 158 Fintech que ofrecen servicios de pagos y remesas, préstamos, gestión de finanzas personales y empresariales, financiamiento de proyectos, gestión de inversiones, seguros, educación financiera y ahorro, soluciones de *scoring,* identidad y fraude, y trading y mercados; sin embargo, instituciones como la Comisión Nacional para La Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF- México), la Comisión Nacional Bancaria y de Valores (CNBV- México) y el Instituto para la Protección al Ahorro Bancario (IPAB- México) sugieren alejarse de estas empresas y sus operaciones, debido al riesgo que implica su probable desaparición y apegarse a figuras tradicionales reguladas como los Pagarés con rendimiento liquidable al vencimiento y fondos de inversión, celebrables a través de entidades financieras reguladas.[71]

En ese tenor, el pasado 5 de diciembre de 2017 el Senado de la República Mexicana aprobó con modificaciones la Ley para Regular las Instituciones de Tecnología Financiera (IFT)[72], por su parte, la Comisión de Hacienda de la Cámara de Diputador aplazó la discusión de la *Ley FinTech* para inicios de 2018, derivado de la complejidad de la materia y el fondo para el cuerpo legislativo.[73]

El proyecto que envío el ejecutivo federal mexicano en octubre del mismo año, no sólo incluye la propuesta de ley, sino diversas modificaciones a otros cuerpos normativos como la Ley de Instituciones de Crédito, la Ley del Mercado de Valores, la

de Protección y Defensa al Usuario de Servicios Financieros, la Ley para Regular las Agrupaciones Financieras, la Ley de la Comisión Nacional Bancaria y de Valores y la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita, a través del vínculo http://www.cofemersimir.gob.mx/portales/resumen/43471 COFEMER. *Ley Fintech.* México. Vistos el 13 de diciembre de 2017.

[71] CONDUSEF. ¿Qué son las fintech? Educación Financiera. Proteja su dinero. Gobierno de la República Mexicana. Visto el 13 de diciembre de 2017 a través del vínculo http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/educacion-financiera/763-que-son-las-fintech

[72] *EL FINANCIERO.* "Senado aprueba la Ley Fintech". Notimex. Economía. México, 5 de diciembre de 2017. Recuperado el 13 de diciembre de 2017 a través del vínculo http://www.elfinanciero.com.mx/economia/senado-aprueba-la-ley-fintech.html

[73] GUTIÉRREZ, Fernando. "Diputados aplazan discusión de Ley Fintech; podría irse hasta 2018". *El Economista.* México, 12 de diciembre de 2017. Visto el 13 de diciembre de 2017 a través del vínculo https://www.eleconomista.com.mx/sectorfinanciero/Diputados-aplazan-discusion-de-Ley-Fintech-podria-irse-hasta-2018-20171212-0117.html

Ley General de Organizaciones y Actividades Auxiliares del Crédito, la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, la Ley para Regular las Sociedades de Información Crediticia, la Ley de Protección y Defensa al Usuario de Servicios Financieros, la Ley para Regular Agrupaciones Financieras, la Ley para la Comisión Nacional Bancaria y de Valores y, la Ley para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita; motivado por las nuevas tendencias en el sector financiero gracias a la presencia de nuevas tecnologías que fomentan la descentralización de sistemas, como la tecnología de cadena de bloques (*blockchain)*, proliferación de economía colaborativa y los servicios financieros de persona a persona; con lo que pretende generar espacios regulatorios seguros que permitan el desarrollo de innovaciones tecnológicas en el sector financiero. Dicho proyecto pretende regular a las ITF (Fintech) cuyo objeto sea el financiamiento colectivo (*"crowdfunding")* y generación de fondos de pago electrónico.

El proyecto de ley finalmente encontró su aprobación el pasado 28 de febrero, cuando la Cámara de Diputados envío su dictamen al Ejecutivo, para su promulgación; al respecto, podrían destacar los siguientes elementos:

1. **Aprobación del Comité Interinstitucional integrado por la Comisión Nacional Bancaria y de Valores, Banco de México y Secretaría de Hacienda y Crédito Público**.- En términos del artículo 11 del anteproyecto ejecutivo, para organizarse y operar como ITF se requiere la autorización del Comité referido. Una vez que se obtiene dicha autorización, la Institución Financiera estará obligada a agregar en su denominación las palabras "institución de financiamiento colectivo" o "institución de fondos de pago electrónico", respectivamente. A saber de quien escribe, encuentro 2 graves complicaciones a lo propuesto: PRIMERO.- Según lo dicta la Constitución Política de los Estados Unidos Mexicanos, el derecho de libre asociación, consagrado en el artículo 9[74] de la misma, no podrá coartarse para ningún ciudadano mexicano sin excepción alguna. Es radicalmente diferente el autorizar a una persona jurídica su funcionamiento como institución tecnológica financiera, a pretender "autorizar" su organización. SEGUNDO.- Tal como lo expresé líneas previas al estudiar el caso de la regulación de las criptomonedas en Brasil, es compleja la labor de incorporar al sistema económico tradicional, los sistemas virtuales que ya existan en el ciberespacio, empero, podría resultar una labor titánica el pretender que las criptomonedas y sus desarrolladoras se adapten a la ley antes

[74] El texto constitucional vigente dicta: "Artículo 9o. No se podrá coartar el derecho de asociarse o reunirse pacíficamente con cualquier objeto lícito; pero solamente los ciudadanos de la República podrán hacerlo para tomar parte en los asuntos políticos del país. Ninguna reunión armada, tiene derecho de deliberar." CONGRESO DE LA UNIÓN. *Constitución Política de los Estados Unidos Mexicanos.* Visible a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf

de su surgimiento, lo que implicaría vigilar el espontáneo surgimiento de nuevas criptomonedas y las instituciones que operen bajo dichas modalidades.

2. **Ausencia de respaldo gubernamental**.- Aún sin superar el artículo 11 en comento, su segundo párrafo señala de tenor literal: "Ni el Gobierno Federal ni las entidades de la administración pública paraestatal podrán responsabilizarse o garantizar los recursos de los Clientes que sean utilizados en las Operaciones que celebren con las ITF o frente a otros, así como tampoco asumir alguna responsabilidad por las obligaciones contraídas por las ITF o por algún Cliente frente a otro, en virtud de las Operaciones que celebren…". Lo que a mi parecer, genera un *non sense* jurídico de la existencia de esta propuesta de ley, lo anterior, toda vez que por un lado el gobierno federal y sus autoridades bancarias/financieras pretenden regular el comportamiento de las ITF y sus modalidades de pago, sin embargo, en caso de existir reclamaciones por parte de los clientes, no podría acudirse a mecanismos tradicionales de solución de controversias. En ese sentido, la regulación de este tipo de instituciones se vuelve absurda, si es que no se permiten vías jurídicas para proteger a los usuarios.
3. ***Crowdfunding* sujeto a aprobación de la CNBV**.- El *crowdfunding* es un sistema de financiación colectiva conocido como "micro-mecenazgo" que permite la unión masiva de inversores sin necesidad de intermediación financiera gubernamental. Actualmente, existen plataformas muy exitosas como *Kickstarter, Patronme, Crowlending* y *Grow*, que generan millones de dólares en financiamiento entre particulares (per to per); tan sólo en 2016 en España, este mecanismo recaudó alrededor de 113, 571,990 euros[75], país en el que se regula a las plataformas de financiación participativa a través de la Ley 5/2015 de 27 de abril[76]. En el caso del proyecto que nos ocupa, obliga a las Instituciones de Financiamiento Colectivo que pongan en contacto a personas con el fin de que entre ellas se otorguen financiamientos, a través de aplicaciones informáticas,

[75] VIÑAS, Verónica. "Los nuevos mecenas de la cultura". *Diarios de León*. Cultura. España, 7 de agosto de 2012. Recuperado el 13 de diciembre de 2017 a través del vínculo http://www.diariodeleon.es/noticias/cultura/los-nuevos-mecenas-de-cultura_714384.html

[76] Tal como ocurre en el caso mexicano, la **Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial,** permite esta modalidad siempre que la plataforma cuente con autorización gubernamental de la Comisión Nacional del Mercado de Valores. A saber, su artículo 46 dicta: ***"Plataformas de financiación participativa.*** *1. Son plataformas de financiación participativa las empresas autorizadas cuya actividad consiste en poner en contacto, de manera profesional y a través de páginas web u otros medios electrónicos, a una pluralidad de personas físicas o jurídicas que ofrecen financiación a cambio de un rendimiento dinerario, denominados inversores, con personas físicas o jurídicas que solicitan financiación en nombre propio para destinarlo a un proyecto de financiación participativa, denominados promotores.*" Jefatura del Estado. *Ley 5/2015*. BOE-A-2015-4607. Documento consolidado BOE Número 101, de 28 de abril de 2015. España. Visto el 13 de diciembre de 2017 a través del vínculo https://www.boe.es/buscar/act.php?id=BOE-A-2015-4607

interfaces, páginas de Internet o cualquier otro medio de comunicación electrónica o digital, a obtener la autorización de la Comisión Nacional Bancaria de Valores. Dicha autorización únicamente se emitirá a favor de persouas morales y exclusivamente permite la celebración de alguno de los siguientes actos de comercio: I) Financiamiento colectiva de deuda, II) Financiamiento colectivo de capital o, III) Financiamiento colectivo de copropiedad o regalías.

4. ***Generadores y administradores de criptomonedas.***- El capítulo segundo de la Ley objeto de nuestro estudio, hace referencia a las Instituciones de Fondos de Pago Electrónico. A través de este apartado, se pretende regular el surgimiento de las personas morales que presten servicios de emisión, administración, rendición y transmisión de fondos de pago electrónico, mediante la previa autorización de la CNBV. Asimismo, pretende regular las operaciones que celebran este tipo de instituciones, bajo las modalidades y autorizaciones que rinda el Banco de México, lo que en sentido práctico implica, que ninguna desarrolladora podrá abrir un monedero de criptomoneda, sin la autorización del Banco centralizado nacional; circunstancia que no respeta la naturaleza de alguna moneda virtual en el campo actual. Por último, obliga a este tipo de instituciones a guardar un reporte sobre los fondos que se generen en las cuentas virtuales y, en su caso, notificar los movimientos y transacciones que realizo cada cliente, a la CNBV; bajo esta premisa, se pretende eliminar la dependencia gubernamental de la tecnología *blockchain*[77], para llevar un registro cuasi-automatizado del uso de estos fondos electrónicos. Sobre el particular, el artículo 47 de dicho ordenamiento dicta: "***Artículo 47.-*** *Cada ITF deberá llevar un registro de cuentas sobre movimientos transaccionales que permita identificar a cada titular de los recursos y los saldos que, como resultado de dichos movimientos, mantengan con la propia ITF, incluyendo los fondos de pago electrónico y activos virtuales de cada Cliente de las instituciones de fondos de pago electrónico que correspondan."* Por último y como un duro golpe a la naturaleza volátil de este tipo de fondos, el artículo 29 de este proyecto legislativo, prohíbe el pago de interés o rendimiento monetario por el saldo que se acumule en el tiempo; sin duda, bajo la intención de que los clientes prefieren la apertura de cuentas en instituciones financieras tradicionales que sí tienen permitida esta facultad.

[77] El artículo 70 del proyecto de Ley, también obliga a las ITF a: "…proporcionar a la CNBV y al Banco de México, en el ámbito de sus respectivas competencias, la información que dichas Autoridades Financieras les requieran sobre sus Operaciones y aquellas realizadas entre sus Clientes, incluso respecto de alguna o algunas de ellas en lo individual, los datos que permitan estimar su situación financiera y, en general, aquella que sea útil a la CNBV o al Banco de México para proveer el adecuado cumplimiento de sus funciones, en la forma y términos que las propias Autoridades determinen." Una grave modalidad que parece atentar contra la propia y especial naturaleza de las criptomonedas, hasta ahora.

5. ***Criptomonedas en la Ley Fintech.***- Para objetos de la ley, se entenderá por "activo virtual" a la representación de valor registrada electrónicamente y utilizada entre el público como medio de pago para todo tipo de actos jurídicos y cuya transferencia pueda llevarse a cabo a través de medios electrónicos (artículo 30). Al respecto, sujeto a consideración del lector las siguientes:

   a. ***Ventajas.***- **Primero**.- A diferencia del funcionamiento de las criptomonedas, el proyecto de ley obligaría a que las ITF autorizadas, entreguen al Cliente, la cantidad de activos virtuales de los que sea titular o bien, el monto que corresponda en moneda nacional. **Segundo.**- El artículo 32 del proyecto dicta la facultad del Banco de México para emitir las reglas de carácter general para el resguardo de las firmas, claves y autorizaciones necesarias para la operación del cliente y el uso de su activo digital. Si nos remitimos al capítulo primero de la presente obra, recuperaremos la importancia de dicho activo virtual. Actualmente, ninguna criptomoneda puede argumentar que existen protocolos para el resguardo de ese tipo de información sensible.
   b. ***Desventajas.***- **Primero**.- La inclusión de una criptomoneda en el sistema financiero mexicano dependerá, en gran medida, de la popularidad con la que se presente en el mercado financiero virtual. Esto adquiere sentido, si nos sujetamos a la lectura del tercer párrafo del artículo 30, en el que se prescribe que las ITF sólo podrán operar con activos virtuales autorizados y determinados por el Banco de México, quien tomará en cuenta el uso que el público dé a las unidades digitales como medio de cambio y almacenamiento de valor, el tratamiento que otras jurisdicciones les den a esas unidades digitales particulares, así como los convenios, mecanismos, reglas o protocolos que permiten generar, identificar, fraccionar y controlar la replicación de dichas unidades. En un sentido general, implica que aquellas criptomonedas que mejor aceptación legislativa, política y financiera presenten en el mundo, serán aquellas que el Banco de México podría aceptar con mayor diligencia dentro de nuestro sistema financiera, en tanto que aquellas que carezcan de esta fortaleza mediática podrían ser descalificadas como activo virtual mexicano. Esto podría generar severos actos de corrupción en el país, ya que invita a que las entidades desarrolladoras de criptomonedas busquen arreglos extraoficiales para que su moneda alcance dicho calificativo, independientemente de los elementos objetivos que prescribe la ley. **Segundo.**- En seguimiento al anterior razonamiento, el artículo 32 faculta al Banco de México para definir las características de los activos virtuales, así como las condiciones y restricciones de las operaciones que puedan realizar con dichos activos. Esta potestad invita a presumir que el Banco de México permitirá la menor cantidad de criptomonedas posibles en el sistema

financiero mexicano, lo anterior, debido a que todo Banco central debe consignar el poder adquisitivo de su moneda, es decir, resultaría absurdo que el Banco mexicano autorice una moneda virtual de mayor fortaleza financiera y circulación que el propio Peso Mexicano (moneda de circulación legal). Asimismo, apunta a una desafortunada posibilidad de corrupción en la probable definición de los requisitos y características que deberán poseer las monedas virtuales aceptas en el sistema financiero mexicano. **Tercero.**- Tal como lo expresé con anterioridad, el proyecto de ley se encuentra plagado de ***non sense*** normativos, a saber, el artículo 34 obliga a las ITF a divulgar los riesgos que existen por celebrar operaciones con activos virtuales; a informar mínimamente que: **I.** El activo virtual no es moneda de curso legal y no está respaldado por el Gobierno Federal, ni por el Banco de México; **II.** La imposibilidad de revertir las operaciones una vez ejecutadas, en su caso; **III.** La volatilidad del valor del activo virtual, y **IV.** Los riesgos tecnológicos, cibernéticos y de fraude inherentes a los activos virtuales. No es permisible aceptar la autorización y determinación de una criptomoneda por el Banco de México y en el mismo texto legislativo, obligar a las ITF a señalar el riesgo de su utilización, cuando en teoría, la máxima autoridad financiera nacional revisó los requisitos para permitir su inclusión al sistema financiero.

6. ***Regulatory Sandbox.***- La exposición de motivos del ejecutivo federal, se adhiere a casos de éxito como el Reino Unido y Singapur, en la cual se prueban modelos novedosos para otorgar autorizaciones temporales a las entidades financieras para llevar a cabo actividades contempladas en su objeto, al otorgar servicios experimentales a un número reducido de clientes y por un tiempo limitado, lo que permita desarrollar su innovación en el mercado real de forma controlada y supervisada por las autoridades. El Capítulo I, del Título IV del proyecto de Ley, regula las autorizaciones temporales para llevar a cabo la actividad Fintech a través de Modelos Novedosos. Las mismas están sujetas a autorización y en ningún caso podrán exceder los dos años. Obliga al ITF en cuestión a generar una propuesta que deberá ser aprobada por las autoridades financieras nacionales, sin la cual el modelo no podrá implementarse, bajo la pena de sanciones administrativas.
7. **Multas, Delitos Fintech y Autorregulación.**- La ley objeto de nuestro estudio incluye un número amplio de sanciones administrativas consistentes en multa a cargo de las ITF. Éstas pueden alcanzar las 300 000 Unidades de Medida y Actualización y pueden ser recurridas mediante recurso de revisión. Asimismo, incluye tipos penales especiales que derivan de las siguientes conductas: i) No devolver recursos a sus clientes ante suspensión de actividades (tres a nueve años de prisión y multa de 30 000 a 300 000 UMA); ii) Desviar recursos,

fondos de pago electrónico o activos virtuales (tres a nueve años de prisión y multa de 30 000 a 300 000 UMA); iii) Utilizar o divulgar información financiera o confidencial, sin autorización previa (tres a nueve años de prisión y multa de 30 000 a 300 000 UMA); iv) Ejercer cargo en el sistema financiero mexicano cuando se fue removido o suspendido de dicho cargo por resolución firme del CNBV (dos a siete años de prisión); v) Actuar como ITF sin contar con la autorización del Comité (siete a quince años de prisión y multa de 500 a 50 000 UMA); vi) Realizar actividades sin autorización del titular del activo virtual (siete a quince años de prisión y multa de 500 a 50 000 UMA); vii) Mal ejercicio del cargo del consejo de administración, directivos, funcionarios, empleados o auditores externos, de una sociedad autorizada para operar con Modelos Novedosos o ITF (dos a diez años de prisión y multa de 500 a 50 000 UMA); viii) Ostentarse públicamente como ITF o sociedad autorizada para operar con Modelos Novedosos sin contar con la autorización (uno a seis años de prisión); ix) Suplantación de identidad, representación o personalidad de Autoridades Financieras o miembro de una ITF o sociedad autorizada para operar con Modelos Novedosos (tres a nueve años de prisión y multa de 30 000 a 300 000 UMA); x) Suplantación de identidad ante ITF o sociedad autorizada para operar con Modelos Novedosos (tres a nueve años de prisión y multa de 30 000 a 300 000 UMA); xi) Acceso ilegítimo para obtener información confidencial o reservada a cargo de las ITF (tres a nueve años de prisión y multa de 30 000 a 300 000 UMA); xii) Robo de datos personales por suplantación de ITF (tres a nueve años de prisión y multa de 30 000 a 300 000 UMA). Por último, la Ley propone mecanismos de autorregulación siempre que se encuentren irregularidades administrativas que se consideren no graves en términos del propio ordenamiento. Este medio alternativo implica la corrección de las irregularidades, bajo la observación de las autoridades financieras, sin que se puede sancionar a la ITF por dicho incumplimiento.

En tenor de lo expuesto, el pasado 10 de septiembre de 2018, en el *Diario Oficial de la Federación* se publicó el primer paquete de Leyes secundarias que buscan la debida implementación de las Instituciones Tecnológicas de Financiamiento. En proceso de lo anterior, se divulgó la Circular 12/2018 dirigida a las Instituciones de Fondos de Pago Electrónico, relativa a las disposiciones de carácter general aplicables a las operaciones de las Instituciones de Fondos de Pago Electrónico[78]; a su vez, se publicaron las "Disposiciones de Carácter General a que se refiere el Artículo 58

[78] BANCO DE MÉXICO. *Circular 12/2018*. México, 10 de septiembre de 2018. Firma el Director General de Operaciones y Sistemas de pagos, así como el Director General Jurídico. Diario Oficial de la Federación. Visto el 21 de octubre de 2018 a través del vínculo https://www.dof.gob.mx/nota_detalle.php?codigo=5537421&fecha=10/09/2018

de la Ley para Regular las Instituciones de Tecnología Financiera" y las "Disposiciones de Carácter General aplicables a las Instituciones de Tecnología Financiera", cuyo objeto es:

I. Establecer las medidas y procedimientos mínimos que las ITF deberán observar para prevenir y detectar los actos, omisiones u operaciones que pudieran favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión del delito previsto en el artículo 139 Quáter del Código Penal Federal o que pudiesen ubicarse en los supuestos del artículo 400 Bis del mismo Código.
II. Prever la forma y los términos en que las ITF deberán presentar a la CNBV el Manual de Cumplimiento.
III. Señalar la forma, los términos y las modalidades conforme a los cuales las ITF deben presentar a la Secretaría, por conducto de la CNBV, los reportes relacionados con:

    a. Los actos, Operaciones y servicios que realicen con sus Clientes y las Operaciones entre estos, que pudieran estar relacionados con los supuestos previstos en los artículos 139 Quáter o 400 Bis del Código Penal Federal.
    b. Los actos, Operaciones y servicios que realicen los miembros de su consejo de administración o administrador único, sus directivos, funcionarios, empleados, comisionistas o apoderados, que pudiesen actualizar los supuestos señalados en el inciso anterior, así como contravenir o no dar cumplimiento a las obligaciones establecidas en estas Disposiciones.

IV. Precisar las características que deban reunir los actos, Operaciones y servicios que deban ser reportados por las ITF.
V. Prever los casos, la forma y los términos en que las ITF darán cumplimiento a las obligaciones previstas en la Ley y a las demás obligaciones previstas en estas Disposiciones, así como los plazos y medios a través de los cuales comunicarán o presentarán a la Secretaría, por conducto de la CNBV, o a esta última, según corresponda, la información y documentación que así lo acredite (...) Establecer el marco normativo aplicable a la organización de las ITF y la operación de las instituciones de financiamiento colectivo (respectivamente).[79]

[79] SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO. *Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera.* México, 10 de septiembre de 2018. Diario Oficial de la Federación. Firma el Presidente de la Comisión Nacional Bancaria y de Valores el 07 de septiembre de 2018. Visto el 21 de octubre de 2018 a través del vínculo https://www.dof.gob.mx/nota_detalle.php?codigo=5537450&fecha=10/09/2018

IX
CAPÍTULO

Protección a la Propia Imagen y Datos Personales

IX. 1 Protección a la Propia Imagen en Redes Sociales

En octubre de 2016 el joven australiano Ali Ziggi Mosslmani demandó a los diarios *Sydney's Daily Telegraph, The Daily Mail* y el *Australian Radio Network*, por "difamación"[1], derivado de la publicación en la cual se exhibe una fotografía con su imagen durante una fiesta de cumpleaños local. Dicha fotografía se hizo viral después que la gente se burlara de su corte de cabello. A parecer del joven demandante, dicha fotografía no sólo fue tomada sin su autorización, sino que ésta se subió a las redes sin contar con su visto bueno y ello permitió que su imagen se *viralizara* al grado de volverlo un "meme". A su vez, Keisha Johnson, mejor conocida en Instagram y el reino de los memes como "Confused Black Girl", presentó una demanda millonaria (2014) en contra de la plataforma por permitir que su imagen se *viralizara*, afectando la percepción que otros tienen de ella, respecto a su verdadera apariencia física,

[1] DAKEVYCH, Alex. "The Australian Teen suing for mullet memes". BBC Trending. *BBC News*. Noviembre 2016. Puede consultar la nota completa a través de vínculo http://www.bbc.com/news/blogs-trending-37838197

el argumento principal de la joven americana, radica en que "no luce así en la vida real". En este caso, la demanda fue desestimada al no acreditar la responsabilidad de la red social respecto del comportamiento de los usuarios, por lo cual, tampoco resultó fundado el pago de los 500 millones de dólares que la accionante solicitó por concepto de indemnización.[2] En ambas hipótesis, se advierte que la responsabilidad de la red social se difumina ante la imposibilidad material de controlar a cada usuario respecto del uso que pudiere dar a las imágenes que sube a su portal, sin embargo, ¿no existe responsabilidad derivada del uso ilícito o no autorizado de nuestra imagen en la web, específicamente, en redes sociales?

Al parecer de quien escribe, la respuesta es sí, sobre todo, en tratándose de derechos de imagen de menores de edad. Lo anterior adquiere sentido si lo sometemos a la consideración de la Convención Americana sobre Derechos Humanos o Pacto de San José Costa Rica (1981); ésta reconoce que toda persona tiene derecho al respeto de su honra y reconocimiento a su dignidad (Artículo 11).[3] Tanto la doctrina, como los Altos Tribunales distinguen dentro de los derechos de personalidad al derecho a la vida, a la integridad física y psíquica, al honor, a la privacidad, al nombre, a la propia imagen, al libre desarrollo de la personalidad, al estado civil y el propio derecho a la dignidad persona. Cualquier conducta que atente en contra de la esfera de personalidad más sensible de los humanos, no puede ser considerada absurda o inatendible por las Cortes; mucho menos debe ser ignorada por las redes sociales que prometen el resguardo de la imagen y debida protección de las reglas de la comunidad (Políticas, Términos y Condiciones o Declaraciones) que se firman en redes sociales.

Históricamente, la protección de la imagen se reconoce desde el Derecho Romano, como una prerrogativa a favor de los Emperadores, Generales y Gladiadores que morían con honor en batalla o en el coliseo. A los grandes combatientes se les reconocía el decoro de conservar su armadura intacta al momento de ser enterrados o quemados en plaza pública, sin que nadie pudiere tomar alguno de sus bienes *ad perpetuam* del reconocimiento de su imagen como gran leyenda romana (Derecho de Arenas). Alrededor del mundo, la protección de la propia imagen desde el punto de vista del derecho positivo ha crecido desde hace varios años, por ejemplo, en Brasil cuentan con la *Ley de Arena* o *Ley Pelé* (1973) que protege el uso de la imagen de los deportistas y el derecho exclusivo para la transmisión de la misma a través de señales de televisión o Internet. Conforme el Derecho de Arena romano se consagró en diversas legislaciones, éste fue adoptando el apellido de propiedad intelectual, específicamente, desde el lente de los Derechos de Autor. Al parecer de algunos teóricos,

[2] 24 HORAS. "Joven demanda a Instagram tras ser usada como meme". *Diario 24 horas*. Julio 2014. Puede consultar la nota completa a través del vínculo http://www.24horas.cl/tendencias/espectaculosycultura/joven-demanda-a-instagram-tras-ser-usada-como-meme-1321986

[3] Convención Americana sobre Derechos Humanos. Puede consultar el texto íntegro a través de https://www.colmex.mx/assets/pdfs/4-CADH_51.pdf?1493133911

la protección que existe en el caso mexicano, lo ordena la Suprema Corte de Justicia (México) en diversos precedentes al proteger -dentro de los derechos de personalidad- la dignidad humana prescrita en el artículo 1 de la Constitución política de los Estados Unidos Mexicanos[4], además que la dignidad humana es el pilar de los derechos fundamentales; por otro lado, se restringe el "uso" indebido a través del artículo 87 de la Ley Federal del Derecho de Autor, en correlación con el diverso 231, fracción II de la propia Ley. En tales apartados se regula el uso de la imagen de terceros en fotografías, se delimitan los casos de excepción en los cuales no se requiere la autorización del titular y, por último, se fijan las sanciones por el indebido o ilícito uso de la imagen de terceros. Nuestro Poder Judicial de la Federación, ha interpretado que dicho alcance protege aún más, a los menores de edad, por lo que toda conducta en detrimento de la imagen de estos se considera agravada para fines de determinar la multa. Sin embargo, la protección de los derechos de personalidad -entre ellos el de propia imagen- no concluye en leyes de propiedad intelectual, sino que esto ha trascendido al mundo del derecho civil, constitucional y penal.

En el caso de la Ciudad de México, anteriormente se contó con un tipo penal que protegió "Violaciones a la Intimidad y Vida Privada", que permitía iniciar procedimientos de orden criminal en contra de aquéllos que atentaran contra estos derechos de personalidad, como lo sería divulgar imágenes propias sin la autorización debida. Los tipos penales de referencia se derogaron para permitir el surgimiento de la Ley de Responsabilidad Civil para la Protección de la Vida Privada, el Honor y la Propia Imagen para el Distrito Federal. La ley de referencia contó con buena aceptación, sin embargo, ha tenido una indebida aplicación al pretenderse invocar en procedimientos de orden Federal. Empero, hoy en día permite contar con interés jurídico suficiente para solicitar la reparación del daño moral y la consecuente indemnización derivado de la violación o indebido uso de nuestra imagen, tanto para personas físicas, morales y aquellas consideradas figuras públicas -en la Ciudad de México-. En el ámbito Federal, el diverso 1916 del Código Civil Federal define que el daño moral se origina por la afectación a una persona en "…sentimientos, afectos, creencias, decoro, honor, reputación, vida privada, configuración y aspectos físicos, o bien en la consideración que de sí misma tienen los demás." Del Código Civil Federal, Capítulo V (De las obligaciones que Nacen de los Actos Ilícitos) se distingue:

[4] Seminario Judicial de la Federación. *Dignidad Humana, el Orden Jurídico Mexicano la Reconoce como condición y base de los demás derechos fundamentales.* Tesis P.LXV/2009. Tomo XXX, Diciembre de 2009, Novena Época. Puede consultar el texto íntegro a través del vínculo https://sjf.scjn.gob.mx/sjfsist/Paginas/DetalleGeneralV2.aspx?Epoca=1e3e10000000000&Apendice=1000000000000&Expresion=propia%2520imagen&Dominio=Rubro,Texto&TA_TJ=2&Orden=1&Clase=DetalleTesisBL&NumTE=45&Epp=20&Desde=-100&Hasta=-100&Index=1&InstanciasSeleccionadas=6,1,2,50,7&ID=165813&Hit=40&IDs=2003643,2002502,2002503,2002634,2002640,2002274,2001675,2001284,2001285,2001368,2000340,160954,161100,162174,162896,162894,162893,164772,165821,165813&tipoTesis=&Semanario=0&tabla=&Referencia=&Tema=

I. El surgimiento del interés jurídico a favor de personas morales, quienes podrían intentar la acción en todo lo que resulte aplicable, por analogía, a su esfera jurídica.
II. La acción no puede transmitirse a terceros por actos entre vivos y sólo puede heredarse cuando la misma se intentó en vida.
III. Permite la aplicación de la responsabilidad solidaria sobre aquéllos que hubiesen generado un daño en común.
IV. Inaplicabilidad de las leyes civiles sobre el ejercicio de la Libertad de Expresión, que se regula en los artículos 6° y 7° de la Constitución Política de los Estados Unidos Mexicanos.

Por lo que refiere al último apartado, nuestro Constituyente promulgó la Ley Reglamentaria del Artículo 6°, Párrafo Primero de la Constitución de los Estados Unidos Mexicanos, en Materia del Derecho de Réplica (Noviembre 2015), cuyo artículo segundo, define al Derecho de referencia como: "...El derecho de toda persona a que sean publicadas o difundidas las aclaraciones que resulten pertinentes, respecto de datos o informaciones transmitidas o publicadas por los sujetos obligados, relacionados con hechos que le aludan, que sean inexactos o falsos, cuya divulgación le cause un agravio ya sea político, económico**, en su honor, vida privada y/o imagen**."

Dentro de las ventajas que presenta esta Ley, radica aquella que permite iniciar el procedimiento ante sujetos obligados, respecto de personas que hubiesen fallecido, la imposición de multas y, en su caso, inicio de un procedimiento jurisdiccional ante autoridades Federales. La principal desventaja que presenta nuestra ley, radica en el plazo máximo para iniciar el procedimiento, ya que éste debe ser igual o menor a 5 (cinco) días hábiles.

A saber del comportamiento en redes sociales y el momento en que un meme se hace viral, el plazo que otorgan nuestras leyes en materia de derechos de autor -imprescriptible- permite una debida defensa, por lo que refiere a materia civil, tanto el plazo como la indemnización resultan productivas en términos económicos y, por último, la ley reglamentaria constitucional, parecería ser la más adecuada jurídicamente, sin embargo, los plazos para ejercer el interés jurídico ante particulares, resulta inútil frente a la forma misteriosa en que opera la web.

Respecto a la existencia de los "memes", como un movimiento legislativo reciente en la Cámara de Diputados, se aprobó la reforma al Código Civil Federal, para incorporar al artículo 1916 la posibilidad de considerar ilícita la comunicación, a través de cualquier medio, de un hecho, cierto o falso, que pueda causar deshonra. Los medios y la red calificaron a esta aprobación normativa como "Ley Mordaza"[5], en camino a obstaculizar la libertad de expresión y probables ataques en contra de los candidatos

[5] *EL FINANCIERO*. "Ley Mordaza, de última hora". Opinión. México, 15 de diciembre de 2017, visto a través del vínculo http://www.elfinanciero.com.mx/opinion/ley-mordaza-de-ultima-hora.html

presidenciales para las elecciones del 2018 en México. Bajo la humilde consideración de quien escribe, la calificación "ilícita" en un código sustantivo de naturaleza civil únicamente exhibe desconocimiento sobre las familias del Derecho y sus categorías, ya que resulta evidente que la familia dispositiva dista de la familia punitiva (acusatoria/inquisita) y por ende, es inverosímil calificar las conductas de orden civil como "ilícitas", cuando sí podría ocurrir en el universo del derecho penal; es decir, el legislador tuvo en sus manos la facultad de sancionar desde el universo del Código Penal Federal, las conductas que atenten contra la honra de las personas derivado del mal uso de redes sociales. Empero, en afán de impedir cualquier posible defensa a la reforma que propuso nuestra Congreso, pretenden agregar un interés jurídico diverso al Código Civil Federal, sin explicar, cómo es que los actores podrán acreditar la legitimación pasiva del demandado, es decir, cómo se podrá demandar a un usuario que opere en modo "anónimo" o "pseudónimo"; por otro lado, no define cuál será el alcance de ese interés subjetivo, ya que la viralización de una imagen podría implicar la posibilidad de demandar a millones de usuarios de las redes sociales e inclusive a la propia plataforma, empero, ¿cuál sería su límite y alcance?

En el año 2012, Mark Zuckerberg adquirió la plataforma Instagram por la cantidad de 1,000 millones de dólares, en octubre del 2014, concluyó la compra de la plataforma, red social y mensajera WhatsApp por la cantidad de 22,000 millones de dólares, lo cual culmina con la compra de Twitter en diciembre de ese mismo año, por la suma de 20,000 millones de dólares. Estos montos y datos históricos resultan relevantes para el caso que nos ocupa, ya que desde el año 2014 podemos afirmar la homogeneidad normativa que existe entre las distintas plataformas, toda vez estas operan como Productos afiliados y descentralizados de Facebook Inc. Así las cosas y en afán de la economía de lenguaje que me permite el presente apartado, únicamente reproduciré lo que dicta la página oficial de Facebook, al respecto, en el entendido que *mutatis mutandi* se pueden comprender las mismas para WhatsApp, Instagram y Twitter. A saber, en la última actualización a la *Declaración de derechos y responsabilidades*, de 30 de enero de 2015, se lee:

> **[...] 3. Seguridad**
> Hacemos todo lo posible para hacer que Facebook sea un sitio seguro, pero no podemos garantizarlo. Necesitamos tu ayuda para que así sea, lo que implica los siguientes compromisos de tu parte:
>
> 1. No publicarás comunicaciones comerciales no autorizadas (como correo no deseado, "spam") en Facebook.
> 2. No recopilarás información o contenido de otros usuarios ni accederás a Facebook utilizando medios automáticos (como harvesting bots, robots, arañas o scrapers) sin nuestro permiso previo.
>
> ...

3. No solicitarás información de inicio de sesión ni accederás a una cuenta perteneciente a otro usuario.
4. No molestarás, intimidarás ni acosarás a ningún usuario.
5. No publicarás contenido que resulte hiriente, intimidatorio, pornográfico, que incite a la violencia o que contenga desnudos o violencia gráfica o injustificada.

...

6. No utilizarás Facebook para actos ilícitos, engañosos, malintencionados o discriminatorios.

...

5. Protección de los derechos de otras personas

Respetamos los derechos de otras personas y esperamos que tú hagas lo mismo.

1. No publicarás contenido ni realizarás ninguna acción en Facebook que infrinja o viole los derechos de otros o que viole la ley de algún modo.
2. Podemos retirar cualquier contenido o información que publiques en Facebook si consideramos que infringe esta Declaración o nuestras políticas.

...

3. Si retiramos tu contenido debido a una infracción de los derechos de autor de otra persona y consideras que ha sido un error, tendrás la posibilidad de apelar la decisión.

...

4. Si obtienes información de los usuarios, deberás obtener su consentimiento previo, dejar claro que eres tú (y no Facebook) quien recopila la información y publicar una política de privacidad que explique qué datos recopilas y cómo los usarás.
5. No publicarás los documentos de identificación ni información financiera delicada de uadie en Facebook.
6. No etiquetarás a los usuarios ni enviarás invitaciones de correo electrónico a quienes no sean usuarios sin su consentimiento. Facebook ofrece herramientas de denuncia social para que los usnarios puedan hacernos llegar sns opiniones sobre el etiquetado.

Bajo tales consideraciones: ¿podríamos reclamar a usuarios en la red que abusan del uso de nuestra imagen en redes sociales? Y ¿podríamos responsabilizar -jurídicamente- a la red social por no impedir el comportamiento? Sí, en ambos casos. A pesar que al momento de acceder a una red social, aceptamos las diversas e infinitas condiciones de uso, el *click wrap agreement* únicamente es operante en términos del comportamiento del cibernauta en dicho portal, sin embargo, no impide que éste ejerza cualquier derecho legalmente concebido, derivado de conductas que generen un efecto en el mundo *off line;* sobre todo, en tratándose de la protección de derechos fundamentales del humano. Por otro lado, parece justo afirmar que existe

responsabilidad solidaria de las redes sociales que no bajen el contenido que afecte la más sensible esfera jurídica de un cibernauta. Es decir, en tratándose de violaciones a derechos fundamentales de personalidad, entre ellos la propia imagen, no sólo se pueden iniciar los procedimientos auto-compositivos que propone la red social, sino que es permisible iniciar procedimientos de orden autoral, civil o administrativo -inclusive penal en los Estados federados o Naciones que lo permitan en términos de las legislaciones locales-en contra de los titulares de los perfiles que afecten la dignidad o usen de forma ilícita nuestra imagen.

IX. 2 Protección a los Datos Personales en las Redes Sociales

El 21 de noviembre del año 2017 la compañía estadounidense *Bloomberg* reveló que información y datos personales de al menos 57 millones de usuarios (clientes y conductores) de Uber ™ en todo el mundo, sufrieron un hackeo el pasado octubre de 2016. De dicho delito informático, se comprometieron los nombres, direcciones de correo electrónico, números de teléfono y rutas que afectan a millones de clientes de la plataforma[6]. El CEO de Uber Technologies Inc, se disculpó con los usuarios y evitó justificaciones sobre la brecha de seguridad que sufrió la compañía, a pesar del robusto sistema de protección de datos personales que poseen; por su lado, su representación mexicana, afirmó que se encontraba en proceso de investigación ante las autoridades encargadas de la protección de datos personales en el país. Estos casos no son aislados para prestadores de servicio y redes sociales. Verbigracia: i) En el año 2013, Yahoo enfrentó el ataque informático más grande de la historia, cuando se anunció oficialmente el robo de información de cuentas personas de Yahoo a más de 3,000 millones de usuarios[7]; ii) El pasado 16 de mayo de 2017, la Comisión de Privacidad (Bélgica), la Comisión Nacional de Informática y Libertades (Francia), la Autoridad de Protección de Datos en los Países Bajos, la Comisión de Protección de Datos y Libertad de Información (Alemania), y la Agencia Española de Protección de Datos (España); emitieron conjuntamente un comunicado a través del cual informaron que se abrió en contra de *Facebook*, diversos procesos de revisión de sus políticas de protección de datos personales y la aplicabilidad de la legislación

[6] *PROCESO*. "Hackers roban datos personales de 57 millones de clientes y choferes de Uber. Bloomberg". Redacción. México, 21 de noviembre de 2017. Visto el 16 de diciembre de 2017 a través del vínculo http://www.proceso.com.mx/512086/hackers-roban-datos-personales-57-millones-clientes-choferes-uber-bloomberg

[7] *OATH, Inc*. "Yahoo provides notice to additional users affected by previously disclosed 2013 data thef". Nueva York, Octubre 3 de 2017. Recuperado el 16 de diciembre de 2017 a través del vínculo https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/

americana, cuando ésta empresa cuenta con filiales en la Unión Europea[8]; asimismo, derivado de la adquisición de *WhatsApp*, la Comisión Europea determinó multar con 110 millones de euros al coloso de las redes sociales, consecuencia del uso indebido de los datos personales de sus usuarios en la transacción comercial.[9] Empero, la caja digital de Pandora explotó en marzo del 2018, época en la que se advierte al mundo las diversas brechas de seguridad que presentan estas redes sociales, primero por la sanción impuesta el 02 de marzo por la Agencia Española de Protección de Datos en contra de WhatsApp Inc. y *Facebook* por 300 mil euros; lo que se acentuó después de filtrarse información sobre la indebida manipulación de la empresa *Cambridge Analytica* por el indebido tratamiento de datos personales obtenidos a través de *Facebook* y su *Big Data* almacenada de forma ilegal, lo que permitió que la red social perdiera un valor económico en la bolsa, equivalente al valor de todo Walmart. Esto ocurriría gracias a la App ***This is your digital life*** que desarrolló el profesor Aleksandr Kogan (2014) y que permitió explotar la compañía de Mark Zuckerberg, con fines electorales. La noticia se dio a conocer después que el CEO de Cambridge Analytica, Alexander Nix, manifestara ante una cámara oculta que han participado activamente en cientos de campañas electorales en todo el mundo, en lo particular, afectando la decisión presidencial que tiene a Donald Trump a cargo del país americano. Por su parte, Christopher Wylie, ex empleado de la compañía, reveló que el uso de la app permitió el acceso a datos de perfiles de la red social de Zuckerberg para generar anuncios personalizados con fines políticos. Cambrige Analytica "descubrió" *el hilo negro de Ariadna* y la forma de manipular la decisión del votante. Desafortunadamente, esto no se notificó a los usuarios afectados ni a la FTC, a pesar de tener conocimiento de causa.

Independientemente de la multa que podría enfrentar Zuckerberg y Cambridge Analytica (en adelante "CA") ante la Federal Trade Comission, se solicitó a Mark comparecer ante el Senado y la Cámara de Comercio y Electricidad del Congreso de los Estados Unidos de América. La primera audiencia se celebró el pasado 10 de abril ante casi la totalidad del Senado. Ésta versó sobre la vulneración de la red social Facebook en materia protección de información y datos personales, bajo la jurisdicción de los Estados Unidos de América. El CEO de Facebook, Zuckerberg, rindió testimonio en audiencia pública para aclarar lo que él mismo llamó: "La brecha de seguridad más grande que ha enfrentado FB". Por ahora, Facebook pone al alcance de sus usuarios la herramienta *¿Cómo puedo averiguar si se ha compartido mi*

[8] CONTACT GROUP OF THE DATA PROTECTION AUTHORITIES. *Common Statement.* 16 de mayo de 2017. Recuperado el 16 de diciembre de 2017 a través del vínculo https://sontusdatos.org/wp-content/uploads/2017/05/Common_Statement_16_May_2017.pdf

[9] COMISIÓN EUROPEA. *Mergers: Commision fines Facebook 110 million for providing misleading information about WhatsApp takeover.* Press Release. Bruselas, 18 de mayo de 2017. Recuperado el 16 de diciembre de 2017 a través del vínculo http://europa.eu/rapid/press-release_IP-17-1369_en.htm

información con Cambridge Analytica? A través de la cual pretenden informar a los usuarios que sufrieron afectaciones reales y directas por la brecha de seguridad en comento. Ello permitiría iniciar sesión de forma normal y en caso de resultar positivo el examen, contar con un interés jurídico acreditado para reclamar ante Facebook (con domicilio y oficinas en México) o bien, buscar la protección difusa de una acción colectiva, no sólo en contra de Zuckerberg, sino de CA.[10]

Normativamente, la presencia de la figura *Habeas Data* (según dicho término se define más adelante dentro de la presente Obra) ha permitido que los individuos interactúen con cierta tranquilidad en las redes sociales. Así legislaciones como la mexicana (Ley Federal de Protección de Datos Personales en Posesión de Particulares, Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados), colombiana (Ley 1273 de 2009 sobre Delitos Informáticos, específicamente el artículo 269 F; Ley 1266 Estatutaria de Hábeas Data), española (ley Orgánica 15 de 1999), peruana (ley 29.733 del 2 de julio de 2011); y la famosa *General Data Protection Regulation* de la Unión Europea; se erigen como la fortaleza jurídica detrás de la protección de los datos personales, sin embargo, resulta un criterio democráticamente aceptado, el brindar cierta fortaleza a las condiciones que fijan las propias redes sociales en materia de protección de nuestros datos sensibles y que permiten identificarnos de otros usuarios de la red.

Semánticamente, no todos los datos merecen el mismo nivel de protección normativa ni la seguridad con la que deben tratarse. Así, debemos atender a su nivel de confidencialidad y el grado de publicidad que poseen. En primer lugar, Alfonso Gómez Robledo define a los datos personales como el conjunto de informaciones de una persona física; reflejo de ello es el Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal, las directrices de la Organización para la Cooperación y el Desarrollo Económico sobre la protección de la privacidad y flujos transfronterizos de datos personales, y la Directiva 95/46/CE del Parlamento Europeo y del Consejo de Europa relativo a la protección de datos personales emitida en 1995, la cual define como datos personales "toda la información sobre una persona física identificada o identificable".[11] Por su parte, Oscar R. Puccinelli distingue 3 niveles de graduación en la protección de estos datos: a) los datos que son de libre circulación, como los de identificación: nombre, apellido, documento de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio; b) los de circulación

[10] DÍAZ LIMÓN, Jaime. *In Mark Zuckerberg We Trust.* 13 de abril de 2018, México. Publicaciones. Abogado Digital. Newswire. Visto el 19 de agosto de 2018 a través del vínculo http://www.jaimediazlimon.com/publicaciones/abogado-digital/in-zuckerberg-we-trust/ mediante el cual puede consultar un análisis completo sobre la primera audiencia ante el Senado.

[11] GÓMEZ ROBLEDO, Alonso. *Protección de Datos Personales en México: el caso del Poder Ejecutivo Federal.* México, Instituto de Investigaciones Jurídicas UNAM, 2006

restringida a un sector o actividad determinada, que son susceptibles de tratamiento en tanto se presente una causa de justificación legítima; y c) los de recolección prohibida, porque afectan la intimidad personal o familiar, que son los denominados datos sensibles.[12] Por último, cabe diferenciar los datos personales de los datos personales sensibles. Los primeros se refieren a la información asociada a una persoua o individuo que lo hace identificable del resto de las personas o como parte de un grupo determinado de individuos, por ejemplo: nombre, domicilio, teléfono, fotografía, huellas dactilares, sexo, nacionalidad, edad, lugar de nacimiento, raza, filiación, preferencias políticas, fecha de nacimiento, imagen del iris del ojo, patrón de la voz. Los segundos, son aquellos datos que se relacionan con el nivel más íntimo de su titular y cuya divulgación pueda ser causa de discriminación o generar un severo riesgo para su titular; en ese tenor, se consideran datos sensibles aquéllos que revelen características como origen étnico o racial, estado de salud, creencias religiosas, opiniones políticas, preferencia sexual, pertenencia a sindicatos, creencias filosóficas y morales, entre otras. Las legislaciones al respecto, suelen brindar un mayor peso a la protección y vigilancia de los últimos.

Empero, las redes sociales han optado por construir robustos sistemas de protección de datos personales y adoptar mecanismos de autorregulación normativa, que permite la reparación –ágil aunque no monetaria- de violaciones en la materia. Por su lado, la versión más reciente de la *Política de Privacidad* de Google –25 de mayo de 2018–,[13] señala que los datos que recopila a través de sus herramientas se utilizan con el fin de "ofrecer mejores servicios" a sus usuarios; estos incluyen:

- Información que el propio usuario proporciona (Nombre, número de teléfono y Contraseña)
- Información que obtienen del uso de sus servicios

  - Información del dispositivo
  - Direcciou IP, GPS, Datos del sensor de tu dispositivo
  - Datos de registro
  - Datos sobre ubicación física
  - Números exclusivos de aplicación
  - Almacenamiento local
  - Cookies y tecnologías similares
  - Actividad

[12] R. PUCCINELLI, Oscar. *Protección de Datos de Carácter Personal*. Argentina 2004, Editorial Astrea.

[13] GOOGLE LLC. *Políticas de Privacidad.* Octubre de 2017. Visible el 19 de agosto de 2018 a través del vínculo https://www.google.com.mx/intl/es_mx/policies/privacy/?fg=1 Liga a través de la cual pueden descargar las versiones anteriores de esta política.

- Los términos que buscas
- Los videos que ves
- Las visualizaciones y las interacciones con el contenido y los anuncios
- Información sobre voz y audio cuando utilizas funciones de audio
- Usuarios con los que te comunicas
- Historial de navegación

Google garantiza la seguridad de los datos a través del protocolo SSL, que implica encriptamiento de sus servicios; la función de navegación segura en *Google Chrome*, revisión continua de su política en materia de recogida, almacenamiento y tratamiento de datos; asimismo, limitan el acceso de los contratistas, los agentes y los empleados de Google a la información personal. En caso de requerir el ejercicio de alguno de los Derechos ARCO (Acceso, Rectificación, Cancelación u Oposición), la plataforma invita realizarlo de forma gratuita a través de los canales que dispone para tales fines, sin necesidad de acudir a las instancias gubernamentales. La política que nos ocupa, cumple con los marcos de autorregulación *EU-US Privacy Shield Framework* y *Swiss-US Privacy Shield Framework;* según lo establece el Departamento de Comercio de los Estados Unidos en lo que respecta a recoger, utilizar y conservar información personal de países miembros de la Unión Europea y de Suiza, respectivamente. Al respecto, Google es una plataforma que cuenta con la certificación de ***Escudo de la privacidad***;[14] lo que permite iniciar procedimientos de reclamación en términos de los marcos de autorregulación expuestos y resolver mediante panel arbitral, la controversia que se suscite por resolución vinculante para las partes. Estas consideraciones son aplicables a todos los servicios ofrecidos por Google LLC y sus filiales, incluidos YouTube, Chrome y Chrome OS, Google Play Libros, Payments, Fiber, Project Fi, G Suite for Education, YouTube Kids, Cuentas de Google gestionadas con Family Link, y los servicios que Google proporciona en dispositivos Android y los servicios ofrecidos en otros sitios web.

Por su parte, el titán de las redes sociales, Facebook, cuenta con una política de datos y que es similar a las filiales de la compañía: Instagram, Twitter y Messenger, por mencionar a las más populares. Su última versión data del 19 de abril de 2018[15] y describe el tipo de información que recopila, el modo en que se usa y cómo se comparte. Señala que la información que se recopila "permite hacer del mundo un lugar

[14] El Escudo de Privacidad se diseñó por el Departamento de Comercio de los Estados Unidos, la Comisión Europea y la Administración Suiza para proveer a las compañías con un mecanismo para cumplir con los requerimientos de protección de datos, en tratándose de transferencia de los mismos entre la Unión Europea, Suiza y los Estados Unidos de América; en apoyo al comercio transatlántico. Puede consultar más en el sitio oficial PRIVACY SHIELD FRAMEWORK https://www.privacyshield.gov/welcome

[15] FACEBOOK, Inc. *Política de Datos*. Fecha de última revisión: 19 de abril de 2018. Menlo Park, California. Visible el 16 de diciembre de 2017 a través del vínculo https://www.facebook.com/full_data_use_policy

más abierto y conectado", y únicamente será la relacionada con el usuario en función de los servicios que se use:

- Acciones e información que proporcione el usuario
- Acciones e información que otros usuarios proporcionen del titular
- Redes y conexiones
- Información sobe pagos
- Información sobre el dispositivo (Incluye número de celular, compañía proveedora del servicio e IP)
- Datos provenientes de cookies
- Información de los sitios web y las aplicaciones que se usan
- Información de socios
- Empresas de Facebook[16]

La información de referencia se ocupa para proporcionar, mejorar y desarrollar los servicios; enviar mensajes de marketing al usuario; mostrar y medir anuncios y servicios; asimismo, fomentar la seguridad y protección, mediante la investigación de actividades sospechosas o de infracciones a sus condiciones o políticas. Facebook afirma que su seguridad está a cargo de ingenieros, sistemas automatizados y tecnología avanzada, como el cifrado y el aprendizaje automático. Además, proporciona herramientas de seguridad que incorporan un nivel adicional de protección a tu cuenta, cómo "protege tu contraseña", "contraseña de aplicaciones", "aprobación de inicio de sesión", "notificaciones de inicio de sesión", "contraseñas de un solo uso", "contactos de confianza" y "seguridad en celulares". Cualquier información que se proporcione a Facebook, permite el ejercicio de los Derechos ARCO, sin embargo, la política que nos ocupa, indica que podrían consultar, procesar o conservar la información que reciben sobre el usuario (incluida información sobre transacciones financieras relativa a compras realizadas con Facebook) durante un período prolongado cuando está sujeta a una solicitud u obligación judicial, a una investigación gubernamental o a investigaciones relacionadas con posibles infracciones de las políticas o condiciones, o bien para evitar daños. También conserva información sobre las cuentas que se inhabilitaron por infringir las condiciones del sitio y guarda esos datos durante un año -como mínimo- para evitar que se repitan las conductas abusivas o las infracciones de nuestras condiciones. En ese tenor, Facebook se faculta a

[16]Muchos de estos productos y servicios (como la aplicación para celulares de Facebook, Messenger y Paper) forman parte de Facebook. Otros servicios, como Slingshot, Rooms o la aplicación Internet.org, ofrecen experiencias más independientes. Algunos de los servicios, como el administrador de páginas o las estadísticas del público, son productos que Facebook ofrece a sus socios comerciales, como los anunciantes. Todos estos servicios se rigen por la Política de datos, que describe el modo en que recopilan, usan y divulgan la información.

compartir información por vías internas en su familia de empresas o con terceros con los fines que se describen en esta política. Además de los servicios de Facebook Inc., y *Facebook Ireland Ltd*, esta condición aplica a favor de:

- Facebook Payments Inc.
- Atlas (http://atlassolutions.com/privacy-policy)
- Instagram LLC (http://instagram.com/about/legal/privacy/)
- Onavo (http://www.onavo.com/privacy_policy)
- Moves (http://moves-app.com/privacy)
- Oculus (http://www.oculus.com/privacy/)
- WhatsApp Inc. (http://www.whatsapp.com/legal/#Privacy)
- Masquerade (https://www.facebook.com/msqrd/privacy)
- CrowdTangle (https://http://www.crowdtangle.com/privacy)

En el mismo tenor que lo hace el motor de búsqueda Google, Facebook propone resolver cualquier reclamación que pueda surgir en relación con sus políticas y prácticas de privacidad a través de **TRUSTe** (cuyo nombre cambió a **TrustARC)**; un mecanismo digital de autorregulación, que se erige en términos del sistema EU-U.S. Privacy Shield Framework, y que permite a los consumidores/usuarios presentar reclamaciones a través de formularios en línea, para resolver las controversias en esa plataforma y a través de dicho portal, obtener una resolución vinculante para Facebook y optativa para el titular.

Por último y a diferencia del caso Google, Facebook invita a cuidar el nivel de privacidad de la información que se comparte, ya que está podría cambiar su categoría de "confidencial" a "pública" y el criterio de protección, según sus política se transformaría. Lo anterior, ya que entienden por "información pública" aquella que el usuario comparte públicamente, así como los datos de un perfil público o el contenido que se comparte en una página de Facebook o en otro foro público. La información pública está disponible para cualquier persona, tanto dentro de la red social como fuera de ella, y se puede ver o acceder a ella a través de motores de búsqueda en Internet, interfaz de programación de aplicaciones ("API" por sus siglas en inglés) y medios no relacionados con Internet, como la televisión. Este apartado resulta coincidente con el criterio emitido por el Poder Judicial de la Federación mexicano, el pasado noviembre de 2015; mismo que de tenor literal prescribe:

> PRUEBA ILÍCITA. NO LA CONSTITUYE LA OBTENCIÓN DE LA IMPRESIÓN FOTOGRÁFICA DEL PERFIL DEL IMPUTADO EN UNA RED SOCIAL (FACEBOOK) EN CUYAS POLÍTICAS DE PRIVACIDAD SE ESTABLECE QUE AQUÉLLA ES PÚBLICA (LEGISLACIÓN PARA EL DISTRITO FEDERAL).
> Conforme con la tesis aislada 1a. CLVIII/2011 de la Primera Sala de la Suprema Corte de Justicia de la Nación, visible en el Semanario Judicial de la Federación y su Gaceta,

Novena Época, Tomo XXXIV, agosto de 2011, página 217, de rubro: "DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. MEDIOS A TRAVÉS DE LOS CUALES SE REALIZA LA COMUNICACIÓN OBJETO DE PROTECCIÓN.", todas las formas existentes de comunicación y aquellas que sean fruto de la evolución tecnológica, deben quedar protegidas por el derecho fundamental a la inviolabilidad de las comunicaciones privadas. Ahora bien, constituye "prueba ilícita" cualquier elemento probatorio que se haya obtenido o incorporado al proceso en violación a derechos fundamentales, como son la inviolabilidad del domicilio o el secreto de las comunicaciones, de manera que cuando la prueba es obtenida mediante una conducta dolosa transgresora de derechos humanos, será espuria, y como tal, deberá privársele de todo efecto jurídico en el proceso penal en atención al respeto de las garantías constitucionales. Por otra parte, a toda persona asiste el derecho humano a la vida privada (o intimidad), cuya noción atañe a la esfera de la vida en la que puede expresar libremente su identidad, en sus relaciones con los demás, o en lo individual. Este derecho a la vida privada tiene vinculación con otros, como aquéllos respecto de los registros personales y los relacionados con la recopilación e inscripción de información personal en bancos de datos y otros dispositivos, que no pueden ser invadidos sin el consentimiento de su titular. En esta tesitura, partiendo de lo dispuesto en el artículo 135, párrafo penúltimo, del Código de Procedimientos Penales para el Distrito Federal, **la información contenida en páginas de Internet, constituye un adelanto científico que puede resultar útil como medio probatorio, siempre que para su obtención no se utilicen mecanismos para violar la privacidad de las personas**. Bajo tal contexto, y **tomando en cuenta que dentro de las políticas de privacidad que se establecen en la red social (Facebook), si bien cada usuario es libre de administrar el contenido y la información que publica o comparte, no obstante, entre esos lineamientos se establece que la fotografía del perfil "es pública", por consiguiente, quien decide usar dicha red social, asume las "políticas de privacidad" que la misma determina, entre las cuales se encuentra la citada, y en ese orden, no puede calificarse como "prueba ilícita" la obtención de la impresión fotográfica del imputado cuando, para conseguirla, la ofendida no hizo otra cosa que acceder a la red social mencionada, e introducir versiones del nombre que recordaba de su probable agresor**, comportamiento que bajo ninguna perspectiva puede calificarse como ilegal o violatorio de los derechos humanos del quejoso.[17] **(El énfasis es añadido)**

[17] QUINTO TRIBUNAL COLEGIADO EN MATERIA PENAL DEL PRIMER CIRCUITO. *Prueba ilícita. No la constituye la obtención de la impresión fotográfica del perfil del imputado en una red social (Facebook) en cuyas políticas de privacidad se establece que aquella es pública (legislación para el distrito federal)*. **Tesis I.5o.P.42 P (10a.).** Gaceta del Semanario Judicial de la Federación. Libro 24, Noviembre de 2015, Tomo IV. Décima Época. Página 3603. Visible a través del portal https://sjf.scjn.gob.mx/sjfsist/Paginas/tesis.aspx

En tales términos, parece claro que el Poder Judicial de la Federación tiene presente los alcances de las políticas de esta red social y reconoce el valor vinculante de dichas condiciones.

Conforme lo hemos expuesto, existen elementos autocompositivos que permiten reparar la esfera de los particulares en materia de datos personales, sobre todo aquéllos de naturaleza sensible, empero, eso no limita a los individuos el buscar la solución de sus controversias a través de los mecanismos legales que cada nación ha instaurado al respecto, en el entendido que el contrato privado (*click wrap agreement* según se definió anteriormente) que se celebra con cada portal o red social, no puede estar, en ningún escenario, por encima de la ley. Esta última aseveración adquiere sentido, si nos remitimos a los casos de sanciones en contra de Facebook y Google *(ver Richter vs Google)*, por violaciones al manejo de datos personales de sus usuarios, no sólo en la Unión Europea, sino en los diversos países en que tiene presencia su servicio.

X CAPÍTULO

Acceso a las Tecnologías de la Información de la Comunicación como Derecho Fundamental

El 16 de mayo de 2011, el relator de las Naciones Unidas, Frank La Rue entregó a la asamblea general de la organización internacional un documento intitulado "*Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*"[1], mismo que fue replicado por diversos diarios alrededor

[1] LA RUE, Frank. *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression*. Human Rights Council. Seventeenth session. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. General Assembly. United Nations. 16 mayo de 2011. A/HRC/17/27. Puede consultar la versión original –en inglés- a través del vínculo http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf Visto el 25 de junio de 2017.

del globo bajo la premisa: "Frank La Rue/La ONU declara el acceso a Internet como un derecho humano". Esto sin brindar un correcto peso jurídico al documento de referencia, ni a los silogismos complejos y estudio profundo que brindó el relator. Esto generó que reporteros y juristas comenzaran a analizar la posibilidad real de colocar a Internet dentro de la segunda clase de Derechos Humanos, los de categoría política, económica, social y cultural. A pesar de las aceleradas conclusiones de los medios y los casos de éxito, en derecho positivo, que enfrentó La Rue, el relator no emitió de forma absoluta –como algunos diarios y abogados lo han expresado- que "el acceso a Internet" sea un indiscutible Derecho Humano, sin embargo, el documento si incluye la siguiente conclusión:

> Acceso a Internet y la infraestructura necesaria. Dado que Internet se ha convertido en una herramienta indispensable para la realización de una serie de derechos humanos, la lucha contra la desigualdad, y la aceleración del desarrollo y el progreso humano, garantizar el acceso universal a Internet debería ser una prioridad para todos los Estados.[2] [Traducción del autor]

[2] El texto Original en inglés, dicta: "*Access to the Internet and the necessary infrastructure. Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States*". Mi preocupación a las desafortunadas declaraciones de los diarios alrededor del globo, así como de algunos juristas, es que esto genera interpretaciones paranoicas sobre el fin y conclusiones efectivamente logradas por Frank La Rue, entra las cuales, destaca la presencia en derecho positivo, en algunos casos contados de soberanías, del acceso a Internet como derecho humano, sin embargo, esto no es la regla general en las legislaciones que La Rue estudió –entre ellas la Sur Coreana y la mexicana-. Al respecto, resulta aún más preocupante que gran parte de las opiniones periodísticas hubieron basado su mensaje en el resumen presentado por el relator a la ONU, en la cual, dichos diarios ofrecieron una traducción y reproducción aislada, del texto que invoqué –en idioma original-, para llevar al lector a la temeraria apreciaría que, a partir de 2011, pudiere ser invocado el Derecho de Acceso a Internet como Derecho Humano. En la red de redes, podrá encontrarse la siguiente traducción no oficial: "La única y cambiante naturaleza de Internet no sólo permite a los individuos ejercer su derecho de opinión y expresión, sino que también forma parte de sus derechos humanos y promueve el progreso de la sociedad en su conjunto…" en diarios como EXPANSIÓN y CNN. Notas que pueden consultarse a través de http://expansion.mx/tecnologia/2011/06/08/la-onu-declara-el-acceso-a-internet-como-un-derecho-humano (*CNN*, "La ONU declara el acceso a Internet como un derecho humano". 8 de junio de 2011) y http://cnnespanol.cun.com/2011/06/09/el-acceso-a-internet-un-derecho-humano-segun-la-onu/ (*CNN*, "El acceso a Internet, un derecho humano según la ONU". 9 de junio de 2011). Situación que se vio replicada por catedráticos y expertos en la materia como la Doctora María Elena Menesses Rocha (del Tecnológico de Monterrey), a través de su artículo intitulado *Internet como derecho humano* de septiembre de 2012, en el que hace referencia al reporte de referencia (http://www.itesm.mx/wps/wcm/connect/snc/portal+informativo/opinion+y+analisis/firmas/dra.+maria+elena+meneses+rocha/op%2814sep12%29mariaelenameneses) y el Doctor Miguel Carbonell, a través de su página oficial, que se presenta con el artículo *El acceso a Internet como Derecho Humano*, de junio de 2016 (Mismo que puede consultarse a través de http://www.miguelcarbonell.com/docencia/El_acceso_a_Internet_como_Derecho_Humano.shtml)

El reporte de referencia adquirió valor público, cuando en junio de 2011 se divulgó el mismo a través de la página oficial de la Organización de las Naciones Unidas y tanto el objetivo como las conclusiones de Frank La Rue, fueron desafortunadamente sacados de su contexto. En primer lugar, el objeto del reporte era explorar las claves y retos de los individuos al buscar, recibir y emitir información e ideas de cualquier tipo a través de Internet, en el entendido de la naturaleza única y cambiante de la red de redes como un catalizador que permite a los individuos ejercer su derecho de libertad de expresión y opinión.

No es óbice a las anteriores precisiones, lo descrito en el párrafo 65 del mismo reporte, en el que de forma medular, Frank La Rue sostiene que algunos Estados con buen desarrollo económico han reconocido el acceso a Internet como un derecho. Casos como el de Estonia (2000), cuyo parlamento reconoció el acceso a Internet como derecho humano básico, el consejo francés (2009), las cortes de Costa Rica tomaron una decisión similar (2010) y, en un estudio aventajado a nuestro momento jurídico, el gobierno de Finlandia (2009) decretó que cada conexión en el país debe tener, al menos, un nivel de interconectividad/ancho de banda de un megabit por segundo; empero, ninguna de estas hipótesis políticas, jurídicas o jurisdiccionales ha generado una corriente axiomática que permita comprender a Internet y su acceso como un Derecho Humano indiscutible. Al respecto, propongo al lector dos corrientes que tuvieron origen a partir de la declaración de la ONU en torno a la libertad de expresión y opinión a través de Internet (2011). La primera de ellas la he denominado de forma concomitante: **Teoría Fundamentalista Digital**, que respeta el silogismo bajo el cual algunos doctrinarios conciben el acceso a Internet como un Derecho Humano; y por otro lado, la denominada **Acceso a las Tecnologías de la Información de la Comunicación como Derecho Fundamental**; siendo esta última la que prefiero en lo particular, por la fortaleza metódica y jurídica de los silogismos, a favor de esta corriente.

X. 1 Teoría Fundamentalista Digital

Se puede considerar la corriente y doctrina que defiende la existencia del derecho humano de acceso a Internet, esto derivado del reporte que brindó Frank La Rue el pasado junio de 2011 ante la Asamblea General de las Naciones Unidas. La presente corriente adquiere valor jurídico y mérito propio, al rescatar los casos de éxito que el propio relator brinda en su estudio, a saber, los casos de Francia, Costa Rica, Estonia y Finlandia, naciones en las que se ha elevado a categoría de derecho humano el **acceso a Internet**. Dicha teoría surge como necesidad para vencer el concepto conocido como "*digital divide*", que refiere a la diferencia que existe entre personas con acceso efectivo a tecnologías digitales y de la información, a través de Internet y, entre aquellas que no tienen acceso alguno. Según se desprende del

trabajo de relatoría, para el año 2011, únicamente existían 21.1 usuarios de Internet por cada 100 habitantes en los Estados que formaron parte de la encuesta realizada por la compañía *Key Global Telecom Indicators for the World Telecomunications Service Sector*, de la *International Telecomunication Union*; empero, dichas cifras han cambiado y evolucionado en progreso de cada sociedad, inclusive en aquellas menos aventajadas, según se desprende de los resultados y datos propuestos en el capítulo I de la presente obra.

Al respecto y congruentemente a la visión humanista de Internet, expertos de la talla de Tim Berners-Lee[3], han afirmado que el progreso de la red de redes únicamente puede encontrarse a través de la "redescentralización", que permita un acceso libre, gratuito y sólo así podremos hablar de éste como un derecho humano. Él también reconoce que si bien no se puede considerar a Internet como un derecho de necesidad básica (agua), sí significa una diferencia de poder económico y social entre alguien con acceso y sin él. Al crear su fundación WWW (2009) el 20% del mundo tenía acceso a la web y se formuló la misión de conectar al 80% del globo. Para el año 2017 las Naciones Unidas han informado que hasta noviembre de 2016, el 47% de la población ya se encuentra conectada; lo que permite brindar un panorama aceptable para las aspiraciones del galardonado científico e informático.[4]

Tim Berners comentó ante el Instituto Tecnológico de Massachusets (*MIT*) y la *Technology Review* sobre el invento que le concedió el **Premio Turing** (servidor CERN centralizado), que el futuro de Internet debe estar en espacios de colaboración como *Wikipedia* y el *crowdfunding*, ya que redes centralizadas, como las redes sociales, permiten deshabilitar una fuente importante de información, es decir, estos datos que se encuentran alimentando la web únicamente se pueden consultar a través de las redes particulares, lo que aleja la información del acceso universal que persigue Berners-Lee. Por supuesto que esta postura presenta un problema fundamental jurídico: el relacionado con la privacidad de la información y el ejercicio de los Derechos digitales que se han estudiado en la presente obra. Al respecto, el galardonado informático, ha desarrollado el programa *Proyecto Solid*, que permite a los internautas comprender la relevancia sobre la generación de información y la responsabilidad que adquieren al liberar la misma a la web, en el entendido que estos se transforman no sólo en generadores de contenido, sino en sus administradores y operadores, lo que elimina la dependencia por parte de los cibernautas a favor

[3] En 1989 escribió una propuesta para un sistema distribuido de hipertexto, en 1991 la primera página web entra en línea, en 1994 fundó el World Wide Web Consortium para estándares de Internet, en 2001 hizo un llamamiento para el desarrollo de una web semántica legible por ordenadores y en 2009 fundó la Fundación World Wide Web para ampliar el acceso a Internet.

[4] SOMONITE, Tom, et al. *Tenemos que hablar de Internet como un derecho humano*. MIT TECHNOLOGY REVIEW. Abril de 2017. Puede consultar el texto íntegro de la entrevista al inventor de Internet, a través del vínculo https://www.technologyreview.es/s/7615/tenemos-que-hablar-de-internet-como-un-derecho-humano Visto el 25 de junio de 2017.

de medios de comunicación centralizada como *Facebook* o métodos de pago como *Criptomonedas* que traen consigo *Blockchain*.

X. 2 Acceso a las TIC'S como Derecho Humano

El concepto de "brecha digital" o "*digital divide*" permite a los Estados conocer la distancia que existe entre los sectores más favorecidos de su población, respecto de aquéllos que no poseen las condiciones mínimas para contar con acceso a las nuevas tecnologías de la información y comunicación. El diccionario en inglés de Oxford, la define como la distancia entre aquéllos que tienen acceso a computadoras e Internet, frente a aquéllos que no lo tienen. Este parámetro puede considerarse como el estándar global para identificar a los países más pobres respecto a los que poseen mayores recursos para proporcionar tecnología a sus ciudadanos. A saber de la Organización de las Naciones Unidas y la Unión Internacional de Telecomunicaciones (*International Telecommunication Union)*, la conectividad que poseen los individuos gracias a la tecnología 3G y fácil acceso económico a equipos móviles, permite que la brecha se reduzca considerablemente, para evitar que la distancia se alargue con los nuevos avances tecnológicos, en los cuáles países como Inglaterra, Japón y la República de Corea[5] muestran una gran respuesta para que este concepto desaparezca de la agenda pública y presentar menos del 1.8% de brecha digital, si los comparamos con el resto de las naciones; en el caso mexicano, esta brecha refleja problemas de inequidad y pobreza en ciertas áreas, ya que con tan sólo 51.2 millones de habitantes siendo internautas, no se puede garantizar que menos de la mitad de la población total cuente con los mecanismos adecuados de acceso a la información[6]. Este problema parece replicarse en América Latina si comparamos a Colombia, México y Paraguay con promedios debajo del 50% contra promedios arriba del 86% de Dinamarca, Noruega y Bélgica.

El discurso jurídico parece ser claro, no es permisible confundir el mal referido "Derecho Humano de Acceso a Internet" con un "Derecho Humano de Acceso a Tecnologías de la Información y la Comunicación"; en principio, toda vez que el segundo reconoce un valor intrínseco en su texto, que es el rezago gubernamental por parte de sus funciones para dotar a cada ciudadano de las medidas suficientes para brindarle el acceso prometido, en tanto que el primero implicaría –si es que efectivamente

[5] UN/ ITU. *Digital Divide closing, but still significant, says United Nations Telecoms agency.* Centro de Noticias. 11 de octubre de 2012. Visto el 10 de diciembre de 2017 a través del vínculo http://www.un.org/apps/news/story.asp?NewsID=43265#.Wi4GsdKWbIU

[6] AMIPCI. *Estudio sobre los hábitos de los usuarios de Internet en México 2014.* México, 2014. Visto el 10 de diciembre de 2017 a través del vínculo http://www.amipci.org.mx/estudios/habitos_de_internet/Estudios_Habitos_del_Internauta_Mexicano_2014_V_MD.pdf

pudiéramos reconocerle calidad de Derecho Humano- que se está un paso adelante y que el Estado ha dotado, satisfactoriamente, a sus ciudadanos de las herramientas suficientes para disfrutar del libre y gratuito acceso a Internet, como lo debería ser, al tener calidad de derecho humano. En la práctica, me parece prudente reconocer el **Acceso a las TIC's** como Derecho Fundamental y Humano, no sólo por semántica, sino por la eficacia política que eso demuestra a favor de brindar un acceso plural y oportuno a favor de los humanos. No es óbice a lo anterior, recordar al lector que no se puede hablar de sinonimia en lo referente a los conceptos de Derecho Fundamental y Derecho Humano. Tal como expone el Maestro Ramón Carreón Gallegos, los derechos fundamentales, en su dimensión objetiva, se consideran elementos superiores del ordenamiento jurídico y resultan importantes para el sistema y el individuo, éstos incluyen la más alta elevación ética y moral que dan forma a los principios rectores de cualquier sistema; por otro lado, los derechos humanos podrían concebirse, desde una perspectiva neo-iuspositivistas, como las realidades jurídico-positivas que protegen desde un punto subjetivo al individuo.[7] En palabras del Maestro Luigi Ferrajoli, los Derechos Humanos forman parte de una clase dentro de los Derechos Fundamentales:

> 1. Una definición formal del concepto de derechos fundamentales
> Propongo una definición teórica, puramente formal o estructural de "derechos fundamentales": son derechos fundamentales todos aquellos derechos subjetivos que corresponden universalmente a todos los seres humanos en cuanto dotados del *status* de personas, de ciudadanos o personas con capacidad de obras; entendiendo por derecho subjetivo cualquier expectativa positiva (de prestaciones) o negativa (de no sufrir lesiones) adscrita a un sujeto por una norma jurídica; y por *status* la condición de un sujeto, prevista asimismo por una norma jurídica positiva, como presupuesto de su idoneidad para ser titular de situaciones jurídicas y/o autor de los actos que son ejercicio de éstas.
>
> ...
>
> La ciudadanía y la capacidad de obrar han quedado hoy como las únicas diferencias de *status* que aún delimitan la igualdad de las personas humanas. Y pueden, pues, ser asumidas como los dos parámetros –el primero superable, el segundo insuperable- sobre los que fundar dos grandes divisiones dentro de los derechos fundamentales: la que se da entre *derechos de la personalidad y derechos de ciudadanía*, que corresponden, respectivamente, a todos o sólo a los ciudadanos y la existente entre *derechos primarios (o sustanciales) y derechos secundarios (instrumentales*

[7] CARREÓN GALLEGOS, Ramón. *Derechos humanos, garantías individuales y derechos fundamentales*. Los derechos humanos en el momento actual. Instituto de Investigaciones Jurídicas. Universidad Nacional Autónoma de México. 2012. Visible el 10 de diciembre de 2017 a través del vínculo https://archivos.juridicas.unam.mx/www/bjv/libros/7/3171/7.pdf

o de autonomía), que corresponden, respectivamente, a todos o sólo a las personas con capacidad de obrar. Cruzando las dos distinciones obtenemos cuatro clases de derechos: **los *derechos humanos*, que son los derechos primarios de las personas y conciernen indistintamente a todos los seres humanos**, como por ejemplo (conforme a la Constitución italiana), el derecho a la vida y a la integridad de la persona, la libertad personal, la libertad de conciencia y de manifestación del pensamiento, el derecho a la salud y a la educación y las garantías penales y procesales, los *derechos públicos*, que son los derechos primarios reconocidos sólo a los ciudadanos, como (siempre conforme a la Constitución Italiana) el derecho de residencia y circulación en el territorio nacional, los de reunión y asociación, el derecho al trabajo, el derecho a la subsistencia y a la asistencia de quien es inhábil para el trabajo; los *derechos civiles*, que son los derechos secundarios adscritos a todas las personas humanas capaces de obrar...; los *derechos políticos*, que son, en fin, los derechos secundarios reservados únicamente a los ciudadanos con capacidad de obrar, como el derecho de voto…

Tanto en nuestra definición como la tipología de los derechos fundamentales construida a partir de ella tienen un valor teórico del todo independiente de los sistemas jurídicos concretos e incluso de la experiencia constitucional moderna. En efecto, cualquiera que sea el ordenamiento que se tome en consideración, a partir de él, son <<derechos fundamentales>> -según los casos, humanos, públicos, civiles y políticos- todos y sólo aquéllos que resulten atribuidos universalmente a clases de sujetos determinadas por la identidad de <<persona>>, <<ciudadano>> o <<capaz de obrar>>.[8]

En ese tenor y en espera de invocar de forma adecuada al Maestro Ferrajoli, es justo afirmar que los derechos primarios, como el acceso a la información y las nuevas tecnologías tienen un reconocimiento universal que les permite considerarse dentro de la esfera de los Derechos Fundamentales y, metodológicamente hablando, en la consideración de Derechos Humanos. Bajo ese tenor, es la obligación de las naciones el proteger esta facultad fundamental, a través de mecanismos gratuitos, libres y plurales, que coloquen la información y la tecnología en manos –y sus monitores- de los ciudadanos, en respeto al reconocimiento fundamental de dicha prerrogativa.

Frente a esta desafortunada postura internacional, el gobierno mexicano a cargo del entonces presidente Enrique Peña Nieto,[9] promovieron un paquete de

[8] FERRAJOLI, Luigi. *Los fundamentos de los derechos fundamentales.* Primera Vista. Editorial Trotta. Madrid, 2001. Edición de Antonio de Cabo y Gerardo Pisarello. Visto el 10 de diciembre de 2017 a través del vínculo http://www.miguelcarbonell.com/artman/uploads/1/Derechos_fundamentales_ferrajoli.pdf

[9] Sobre esta consideración, deseo realizar distinción y un merecido reconocimiento al trabajo de Yolanda Martínez, Coordinadora Nacional de la Estrategia Digital, quién no sólo ha incorporado

reformas estructurales para elevar el "derecho fundamental de acceso a Internet" a rango constitucional y así lo estudia el Doctor e Investigador, Juan Manuel Mecinas Montiel en su artículo *The Digital Divide in México: A mirror of Poverty*[10]. Como bien indica el Doctor, no sólo bastan los 26,000 kilómetros de fibra óptica y el monopolio del servicio de Internet para brindar un acceso asequible y equitativo, la desafortunada conducta de nuestra nación y algunos países involucrados en corrupción, no genera las mejores condiciones para que la información y la tecnología lleguen a las zonas más desfavorecidas geográfica, económica y políticamente. Empero, el texto constitucional parece no bastar para considerar que se reproduce la *Teoría Fundamentalista Digital* en nuestra Carta Magna. En ese tenor, el artículo sexto de la Constitución Política de los Estados Unidos Mexicanos, prescribe:

> Artículo 6o. La manifestación de las ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.
>
> Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.
>
> 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. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios (Párrafo reformado DOF 13-11-2007, 11-06-2013).[11]

un mayor número de servicios digitales al gobierno federal, implementación de políticas de ***Datos Abiertos,*** cédula profesional electrónica; además impulsa el desarrollo de tecnologías Blockchain de aplicación gubernamental y desde la administración pública, ha permitido que México se considere el lugar 22 –entre 193 países- dentro del Índice De Las Naciones Unidas Sobre El Gobierno Electrónico; posicionando al país, como el mejor de América Latina y el Caribe, junto a Brasil.

[10] MECINAS MONTIEL, Juan. *The Digital Divide In Mexico: A mirror of Poverty.* Mexican Law Review. Universidad Nacional Autónoma de México. Julio-Diciembre de 2016. Número 1, Volumen IX. México. Visible el 10 de diciembre de 2017 a través del vínculo https://revistas.juridicas.unam.mx/index.php/mexican-law-review/article/view/10432

[11] CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. *Constitución Política de los Estados Unidos Mexicanos.* México, Septiembre de 2017. Vista el 10 de diciembre de 2017 a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf

El párrafo tercero del texto constitucional que invoco, reconoce que el Estado debe garantizar el derecho de **acceso a las tecnologías de la información y comunicación, así como los servicios de banda ancha e Internet.** A saber de quien escribe, las letras constitucionales no bastan para reconocer que el gobierno mexicano registró el Derecho Humano de Acceso a Internet en nuestro máximo ordenamiento, sin embargo, sí representa un gran progreso legislativo para México antes del 2013 (año de la reforma a ese texto); no sólo porque el gobierno se obligaría a generar condiciones económicas y de competencia efectivas para que los ciudadanos contaran con mayor oferta de los servicios descritos, lo que, a *prima facie*, implicaría reducción de costos y precios al consumidor final, sino que implica el reconocimiento expreso que el derecho a la información y a su libre acceso, sólo es posible bajo la bandera del *Open Government* y el Gobierno Digital. Si somos estrictos con el texto constitucional que propone la Cámara de Diputados del Estado mexicano, es insostenible argüir que son defensores del Derecho Humano de Acceso a Internet como lo pretenden demagógicamente, pero sí es plausible el progreso constitucional que muestra nuestra carta magna, respecto de otras en Latinoamérica. Bajo una prudente consideración, el tercer párrafo del artículo sexto constitucional reconoce un derecho fundamental a favor de sus ciudadanos por lo que refiere al acceso de las *TIC's* y servicios competitivos de banda ancha e Internet, lo que parece ser la llave –al menos en el papel- para vencer la brecha digital que enfrenta nuestro país. Efectivamente incluye un derecho fundamental en su modalidad de derecho humano, empero, no el de "acceso a Internet", como equivocadamente se ha llamado en otros textos jurídicos y políticos.

X. 3 Big Data

Sin que exista una definición académica o doctrinariamente aceptada, invocaré algunas de las acepciones de mayor fuerza comercial en la red. El grupo de desarrollo de IBM define *Big* Data como aquella información que no se puede procesar o analizar mediante procesos o herramientas tradicionales y permite un nuevo enfoque de entendimiento y toma de decisiones, la cual es utilizada para describir enormes cantidades de datos –exabytes- que no pueden ser almacenados en una base de datos regular. Los expertos de IBM describen 5 tipos de Big Data, según el contenido y uso de la información:

1. *Web and Social Media.*- Es la información de la red y aquella que se obtiene gracias a las redes sociales;
2. *Máquina a máquina.*- Son los datos que se obtienen de dispositivos que traducen eventos en particular, en información significativa.
3. *Big Transaction Data.*- Son los datos que provienen de registros de facturación y registros de telecomunicaciones como lo son las llamadas;

4. *Biométricos.*- Información que contiene huellas digitales, escaneo de la retina, reconocimiento facial y datos genéticos;
5. *Generado por Humanos.*- Son aquéllos que fueron emitidos conscientemente por el usuario humano, tales como las llamadas, notas de voz, correos electrónicos, documentos electrónicos o digitales.[12]

Para el experto legal David Navetta, Big Data es el estudio de grandes cantidades de datos estructurados y no estructurados, cuyo proceso tecnológico se define por tres características esenciales: i) Grandes cantidades de volumen de datos, ii) Procesados a alta velocidad y iii) de diversa variedad[13]. Para Rob Kitchin esta información además debe ser exhaustiva, relacional, de alta resolución y flexible. En sentido general, podemos diferenciar la función práctica de la Big Data, a partir que incluye datos masivos que no se pueden almacenar en bases de datos convencionales.

Las diversas posibilidades en el uso de los datos que provienen a través de las variadas fuentes de la web, ha permitido que Big Data se transforme en una herramienta imprescindible para algunos sectores y campañas mediáticas.

En noviembre del año 2016 se anunció al mundo el triunfo del candidato republicano, Donald Trump, para ocupar el cargo del "hombre más poderoso del planeta". Alrededor del globo se expresaron emociones consternadas y preocupación hacia el futuro de las relaciones diplomáticas con el otrora empresario y actual presidente de los Estados Unidos de América. Para enero del siguiente año, muchos atribuían la derrota de Hillary Clinton al abstencionismo de sus votantes, la guerra sucia en su contra, así como pereza del sector más joven de los votantes. Sin embargo, la teoría que más razón parece mostrar, es la que sostiene que la firma *Cambridge Analytica* está detrás del éxito de la campaña presidencial del presidente Trump, mediante la adquisición, control, análisis y manejo de la *Big Data* que arrojaba Internet y que permitió al candidato conocer el ritmo de la contienda electoral, sus siguientes estrategias de campaña y el tono que debía ocupar en cada uno de sus polémicos discursos. A través del sitio oficial de la firma, afirmaron poseer cerca de cinco mil puntos de datos con más de 230 millones de votantes americanos, los cuales combinaron con sus bancos de información para conocer los "mensajes clave" para los votantes relevantes. Después de su notable éxito en la campaña del presidente Trump, a *Cambridge Analytica* se le atribuye el resultado del *Brexit* y actualmente, apoya la

[12] BARRANCO FRAGOSO, Ricardo. ¿Qué es Big Data? DeveloperWorks. IBM. 18 de junio de 2012. Aprenda/ Information mgmt. Visto el 13 de diciembre de 2017 a través del vínculo https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/index.html

[13] NAVETTA, David. *Legal implication of Big Data.* ISSA Journal. Marzo 2013. Visto el 13 de diciembre de 2017 a través del vínculo https://c. ymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0313.pdf

campaña de re-elección del presidente Uhuru Kenyatta, en Kenia[14]. En un país con más de 30 millones de pobladores, 88% de ellos con acceso a Internet a través de sus teléfonos, ausencia de legislación en protección de datos personales y una historia marcada por rebeliones sangrientas, parece que el resultado está programado para una fácil y pacífica continuidad, gracias al fácil mecanismo de respuesta que es la *Big Data*. El sitio *Bloomberg News* afirma que *Cambridge Analytica* se involucró en la campaña para elección presidencial del 2018 en México, lo que permitió a Andrés Manuel López Obrador contar con el 49% de aceptación positiva en redes sociales, frente a su contendiente más cercano con el 18% de aceptación. [15]

Sin embargo, no todo es político cuando se habla de *Big Data*. En septiembre de 2016, la Fundación BBVA y las Naciones Unidas celebraron un convenio para usar la Big Data para resolver catástrofes. BBVA, *BBVA Data & Analytics*, el Centro de Innovación en Inteligencia de Datos de las Naciones Unidas y *UN Global Pulse*, desarrollaron un proyecto que pretende medir la resiliencia en zonas afectadas por desastres naturales a través de los datos que los internautas generan. En ese tenor, en la sesión 45 de la Comisión Permanente de las Naciones Unidas se aprobó la creación de un grupo global en *Big Data* de funcionamiento permanente para investigar los beneficios y retos del uso Big Data, lo que incluye el uso potencial para monitorear y reportar las metas del desarrollo sostenible. En ese contexto, el *Global Working Group (GWG)* y el Oficial superior de la comisión permanente, reconocieron la necesidad de determinar un adecuado plan de trabajo para partir de una metodología, calidad, tecnología, acceso a datos, legislación, privacidad, administración y financias, así como proveer un análisis adecuado del costo-beneficio del uso de Big Data. Como resultado de lo anterior, en noviembre de 2017 se celebró la cuarta Conferencia Mundial sobre Big Data para Estadísticas Oficiales, de lo cual resultó la *Declaración de Bogotá* y 3 recomendaciones puntuales:

> Recomendamos -el GWG- colaboración mundial de datos, facilitar una plataforma mundial con el potencial de almacenar diferentes tipos de datos confiables, servicios y aplicaciones. La colaboración mundial de datos a través de la plataforma global deberá funcionar de la siguiente manera: a) Hacer sencillo para las naciones participar en la red mundial; b) Entregar un mercado y una infraestructura flexible basada en la tecnología de la nube que permite datos confiables, métodos, servicios

[14] BRIGHT, Sam. "After Trump, "big data" firm Cambridge Analytica is now working in Kenya". *BCC Trending*. 3 de agosto de 2017. Recuperado el 13 de diciembre de 2017 a través del vínculo http://www.bbc.com/news/blogs-trending-40792078

[15] CATTAN, Nacha. "Trump's Big Data Gurus Scout Presidential Candidate In Mexico". *Bloomberg*. Politics. Estados Unidos de América, 19 de Julio de 2017. Visto el 13 de diciembre de 2017 a través del vínculo https://www.bloomberg.com/news/articles/2017-07-19/trump-s-big-data-gurus-scout-presidential-candidate-in-mexico

> y aplicaciones para ser compartidos como un bien público útil, en lo legalmente posible; c) Desarrollar acuerdos de colaboración transparentes con organizaciones del sector público y privado, para que dichas socios contribuyan y generen valor a través de modelos de negocio individualmente sostenibles para interesados y asegurar acceso a datos confiables.[16]

Al respecto, esta iniciativa pretende generar la base de datos gubernamental más grande y confiable del mundo, que muestre la aplicación efectiva de la *Big Data* en diversos rubros de los Estados involucrados. Los resultados de su inventario se pueden consultar por proyecto, país, organización, fuente, área de la estadística o meta a través del vínculo *Big Data Project Inventory*[17]. Verbigracia, en México se reporta el proyecto "*Use of data from social networks to obtain statistical and geographical information*" que pretende explorar la posibilidad de usar información de Twitter para producir información estadística a cargo del Instituto Nacional de Geografía y Estadística.

X. 3. 1 Tratamiento jurídico de Big Data

X. 3. 1. 1 Protección De Datos personales en tratamiento masivo

Jurídicamente parece despertar lentamente el interés de los legisladores y abogados, debido a las implicaciones normativas que hay detrás de su uso, resguardo y manipulación; implicaciones que pueden estudiarse desde el universo de Derechos de Autor, o bien desde la perspectiva de Protección de Datos Personales. Resultado de lo anterior, Colombia y la Unión Europea parecen ser referentes universales por lo que refiere al tratamiento legislativo de *Big Data*. En Colombia, cuentan con el Proyecto de Ley 134 de 2015[18] por medio de la cual se regula la actividad de operación y procesamiento masivo de datos, en cuya exposición de motivos, indica que el objeto de regulación corresponde a la actividad económica de procesamiento Big Data; este ordenamiento no sólo obliga a la inscripción de los operadores de información, sino a generar bases de datos confiables que

[16] Puede ver el texto originan en inglés, a través de: GWG/UN. *Bogota Declaration*. 4th Global Conference on Big Data for Official Statisitics. 8-10 November 2017. Colombia. https://unstats.un.org/unsd/bigdata/conferences/2017/Bogota%20declaration%20-%20Final%20version.pdf

[17] Organización de las Naciones Unidas. *Big Data Project Inventory* https://unstats.un.org/bigdata/inventory

[18] CONGRESO DE LA REPÚBLICA DE COLOMBIA. *Proyecto de Ley 134 de 2015.* Visto el 13 de diciembre de 2017 a través del vínculo http://www.imprenta.gov.co/gacetap/gaceta.mostrar_documento?p_tipo=05&p_numero=134&p_consec=42958

deberán registrarse en dependencia gubernamental, para vigilar la correcta obtención de los datos personales que contenga. En el caso español, el Reglamento Europeo de Protección de Datos (2016/679 *General Data Protection Regulation*) pretende armonizar la normatividad relativa de los países miembros de la Unión Europea y de cualquier empresa que realice operaciones en dicho territorio; sustituyó la Directiva de Protección de Datos de 1995, a partir del 25 de mayo de 2018 y regula, desde el universo de la protección de datos, la utilización de Big Data. En la parte conducente, prescribe:

> (156) El tratamiento de los datos personales con fines de archivo, con fines de interés público, investigación científica o histórica o con fines estadísticos debe estar sujeto a las salvaguardas adecuadas de los derechos y libertades del interesado de conformidad con el presente Reglamento. Esas salvaguardias deben garantizar la existencia de medidas técnicas y organizativas para garantizar, en particular, el principio de la minimización de datos. El procesamiento adicional de datos personales para fines de archivo con fines de interés público, investigación científica o histórica o con fines estadísticos se llevará a cabo cuando el responsable del tratamiento haya evaluado la viabilidad de cumplir esos fines mediante el procesamiento de datos que no permitan o dejen de permitir el identificación de los sujetos de datos, siempre que existan salvaguardas apropiadas (como, por ejemplo, *seudonimización* de los datos). Los Estados miembros deberían prever garantías adecuadas para el tratamiento de datos personales con fines de archivo de información con fines de interés público, investigación científica o histórica o con fines estadísticos. Se debe autorizar a los Estados miembros a proporcionar, en condiciones específicas y con las garantías adecuadas para los interesados, especificaciones y excepciones con respecto a los requisitos de información y los derechos de rectificación, borrado, olvido, restricción de la tramitación, transferencia de datos, y objetar al procesar datos personales con fines de archivo de interés público, científicos o de investigación histórica o con fines estadísticos.[19]
>
> [Traducción del autor]

Texto normativo que parece coincidente con la Declaración de Bogotá que estudiamos con anterioridad y que establece un uso legítimo gubernamental para Big Data y, en su caso, uso de particulares, siempre que el tratamiento de datos personales que se encuentren inmersos en la adquisición masiva de información sean tratados desde la óptica de la investigación, estadística, interés público o búsqueda científica e histórica.

[19] Puede consultar el texto original en inglés, a través de: COUNCIL OF THE EUROPEAN UNION. *General Data Protection Regulation.* Bruselas, 6 de abril de 2016. Visto el 13 de diciembre de 2017 a través del vínculo http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

X. 3. 1. 2 Propiedad Intelectual en Big Data

En un sentido amplio, existen dos consideraciones que deben atenderse respecto de estudio jurídico de las bases de datos masivas que nos ocupan. Según Steven Tepp, miembro de la Cámara de Comercio de los Estados Unidos de América, debe recordarse que los datos no producen resultados por si solos, si es que no se les trata de forma tecnológicamente adecuada. Para que la captación masiva de datos tenga sentido, debe analizarse, interpretarse y comunicarse con significado alguno. Para Tepp, existen tecnologías hardware que merecen patentabilidad debido a la forma novedosa con la cual pueden recolectar y archivar los datos involucrados. Por otro lado, la organización y análisis de los datos podría considerarse objeto de protección desde el universo de Derechos de Autor.[20] Bajo tales consideraciones es prudente señalar que no sólo esos universos podrían considerarse en el espectro de protección. Para ello invocaremos lo contenido en la Ley de Propiedad Industrial y la Ley Federal de Derechos de Autor (México).

- **Esquemas de trazado de circuitos integrados.**- Tal como señala Steven Tepp, existen diversas consideraciones en lo referente a Big Data. En lo relativo al hardware, la Ley de Propiedad Industrial protege los esquemas de trazado de circuitos integrados. Según el artículo 178 bis 1 de esta Ley, por circuito integrado se entiende el producto, en su forma final o intermedia, en el que los elementos, de los cuales uno por lo menos sea un elemento activo, y alguna o todas las interconexiones, formen parte integrante del cuerpo o de la superficie de una pieza de material semiconductor, y que esté destinado a realizar una función electrónica. Por otro lado, la fracción IV del mismo artículo define al esquema de trazado original como el resultado del esfuerzo intelectual de su creador y no habitual o común entre los creadores de esquemas de trazado o los fabricantes de circuitos integrados en el momento de su creación. Sin duda, estas figuras podrían resultar aplicables al tratamiento de Big Data, empero, la tecnología implementada para su procesamiento es más habitual en el universo del *Software.*
- **Programa de cómputo.**- Existen diversas consideraciones para conocer la parte medular de protección de un Software. Los colosos del comercio digital como Deloitte, Oracle, Cisco, Microsoft y otros, han desarrollado *software* que permite el análisis, tratamiento y, en algunos productos, almacenamiento *Cloud* gracias al sofisticado código fuente detrás de cada herramienta propuesta. Estos modelos de negocio se desarrollan para grandes empresas que no sólo

[20] TEPP, Steven. *Big Data and Intellectual Property Go Hand in Hand.* U.S. Chamber of Commerce Foundation. Abril 25 de 2014. Recuperado el 14 de diciembre de 2017 a través del vínculo https://www.uschamberfoundation.org/blog/post/big-data-and-intellectual-property-go-hand-hand/34384

dependen de los datos que generan, sino de aquéllos que obtienen de sus clientes y los que obtienen de la red.

- **Bases de Datos.-** En términos de la Ley Federal del Derecho de Autor, queda claro que existen bases de datos que podrían considerarse no originales, sin embargo, a estas las protege para uso exclusivo por el lapso de 5 años, independientemente de su mérito autoral. En términos del artículo 5° del Tratado de la OMPI sobre Derechos de Autor y 107 de la Ley Federal del Derecho de Autor, comprendemos que las compilaciones de datos o de otros materiales, en cualquier forma, que por razones de selección o disposición de sus contenidos constituyan creaciones de carácter intelectual, están protegidas como tales. Asimismo, ambos preceptos excluyen de protección los datos y materiales en sí mismo. La Ley Federal del Derecho de Autor inclusive avanza un poco más y precisa (artículo 109) que la publicación, reproducción, divulgación, comunicación pública y transmisión de información que incluya datos privados o personales, requerirá la autorización previa de los titulares.

XI
CAPÍTULO

Derechos Digitales

El objeto principal de la presente obra ha sido definir algunas categorías novedosas sobre facultades, obligaciones y tratamiento normativo de figuras jurídicas que surgen en el ciberespacio o como consecuencia de su uso; asimismo, proponer la flexibilización de términos que doctrinariamente parecen axiomas indiscutibles, empero, el surgimiento de conductas tan novedosas como variadas obliga al abogado, al legislador y a los usuarios a comprender el Derecho desde nuevas corrientes y conceptos que han mutado del Derecho Internacional Público, para ahora ocupar espacio en cuerpos normativos de Derecho Sustantivo. El surgimiento de Internet y su crecimiento acelerado como medio universal de comunicación obligó a tratadistas y juristas ahondar sobre sus orígenes y compreuder las implicaciones del comportamiento de los usuarios en la red, que sólo tienen aplicación en el ciberespacio y de difícil espectro en el universo tradicional. Esto obligó a las naciones el reconocer que gran parte del comportamiento de los internautas queda fuera de su alcance y así se acuñó el concepto de "ciudadanía digital". Se puede comprender a éste como el vínculo jurídico que existe entre una persona física y un usuario con sus responsabilidades digitales y las libertades que brinda la red de redes. De esa forma los Estados soberanos reconocieron que debían respetar lo que ocurría en Internet como un terreno neutral en el cual las reglas y normatividades eran construidas por los propios usuarios. A saber de Mike Ribble, el ciberespacio y sus ciudadanos han creado nueve áreas de comportamiento que han sido reforzadas por cada portal o red social:

1. Etiqueta.- Implica reconocer los códigos de conducta y procedimientos instaurados en el sitio en que navegamos

2. Comunicación.- El objeto de Internet es el intercambio automatizado y electrónico de información, por lo que cualquier ciudadano digital debe rendir honores a dicha consigna
3. Educación.- Proceso de enseñanza y aprendizaje sobre la tecnología y como usarla
4. Acceso.- Permitir la libre y amplia participación de la sociedad digital
5. Comercio.- Compra-venta de bienes y servicios
6. Responsabilidad.- Responsabilidad electrónica para acciones y respeto a los derechos de propiedad digital y material.
7. Derechos.- Libertades cuyo origen y aplicación se entienden reservados para el ciberespacio
8. Seguridad.- Procurar el bienes físico y psicológico en el mundo digital
9. Seguridad (autoprotección).- Tomar todas las precauciones necesarias para no caer en estado de vulnerabilidad digital.

Estas consignas fueron diseñadas bajo los parámetros de la autorregulación y procuración de ausencia gubernamental; es decir, los defensores de la ciudadanía digital parten de la premisa que Internet debe ser un territorio neutro y con ausencia de instituciones de Gobierno que pudieran vulnerar, coactivamente, el comportamiento libre de los internautas. Esto no pareció quedar claro para los gobernantes del mundo y el 17 de diciembre de 1998, la Asamblea General de las Naciones Unidas, determinó la celebración de la Cumbre de Milenio, a través de la cual 149 líderes mundiales, dictarían políticas globales para favorecer la unificación en distintos rubros, entre ellos, generar gobiernos abiertos y transparentes a favor de sus ciudadanos (Open Government). La misma dio origen a la *Conferencia NetMundial* (Reunión Global de Múltiples Actores interesados sobre el Futuro de la Gobernanza de Internet), que tuvo lugar en abril de 2014 en Río de Janeiro; y la *Cumbre Mundial sobre la Sociedad de la Información* a cargo de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO); de las cuáles de desprendieron documentos relativos a la importancia de la presencia del Estado, cómo vínculo rector entre la información, la educación, las nuevas tecnologías y la brecha digital, y la forma en que los usuarios pueden ejercer sus facultades en la red de redes. A pesar de lo anterior, la presencia de Organizaciones No Gubernamentales como *ONG Derechos Digitales*[1],

[1] Derechos Digitales es una organización latinoamericana cuya fundación ocurrió en 2005. Defiende 3 ejes rectores, de forma esencial: Libertad de expresión, privacidad y datos personales, y derechos de autor. Su misión es la defensa, promoción y desarrollo de los derechos humanos en el entorno digital, mediante la incidencia en políticas públicas y prácticas privadas. La fortaleza de esta ONG se ha mostrado en casos de protesta como lo ocurrido en Chile, cuya movilización social permitió a ese país reconsiderar su postura frente al Acuerdo de Asociación Transpacífico. Para consultar más sobre la Organización visite https://www.derechosdigitales.org/quienes-somos/derechos-digitales/ Para conocer más sobre la protesta en contra del AAT consulte LIMÓN, Jaime. *Propiedad Intelectual en el Marco*

defienden la neutralidad de la red y la defensa de los Derechos Digitales en la red de redes, frente al comportamiento gubernamental. En ese tenor, a pesar de no existir doctrina axiomática al respecto, logramos distinguir los siguientes Derechos Digitales, tradicional o consuetudinariamente aceptados:

1. Privacidad y datos personales (privacidad digital/ *privacy online*)
2. Derechos de Autor y acceso al conocimiento
3. Libertad de expresión
4. Derecho a compartir (libre acceso al ciberespacio)
5. Derecho a la neutralidad de la red

Estos resultan consonantes con la *Carta de APC sobre derechos en Internet*[2] de la Asociación para el Progreso de las Comunicaciones, misma que es consultor categoría nivel 1 ante la ONU, una asociación sin fines de lucro con presencia mundial y cuyo origen se fecha en 1987 cuando los esfuerzos de *GreenNet* y el Instituto para Comunicaciones Globales, se sumaron para probar a los Estados la utilidad de compartir información a través de medios electrónicos, en pro de la paz, los derechos humanos y el medio ambiente. De tal suerte, con fundamento en los artículos 18, 19, 20, 26, 28 la Declaración Universal de Derechos Humanos, el Pacto Internacional sobre Derechos Civiles y Políticos y la Convención sobre la Eliminación de todas las formas de discriminación contra la mujer, en noviembre de 2006 la Asociación publicó la Carta sobre derechos en Internet, en los que incluye: 1) Acceso a Internet para todos y todos; 2) Libertad de expresión y asociación: 3) Acceso al conocimiento; 4) Intercambio de aprendizaje y creación-software libre y desarrollo tecnológico; 5) Privacidad, vigilancia y encriptación; 6) Gobernanza de Internet; y 7) Conciencia, protección y realización de los derechos:

Tema 1 Acceso a Internet para todos y todas

Artículo 26, Declaración Universal de los Derechos Humanos (DUDH): La educación tendrá por objeto el pleno desarrollo de la personalidad humana y el fortalecimiento del respeto a los derechos humanos y a las libertades fundamentales

1.1 El impacto del acceso sobre el desarrollo y la justicia social Un acceso asequible, rápido y fácil a Internet puede ayudar a generar sociedades más igualitarias. Puede servir para fortalecer los servicios de educación y salud, el desarrollo

del Tratado de Asociación Transpacífico. Foro Jurídico. México, 2 de agosto de 2016. https://www.forojuridico.org.mx/propiedad-intelectual-en-el-marco-del-tratado-de-asociacion-transpacifico/

[2]APC. *Carta APC sobre derechos en Internet*. Estados Unidos, Noviembre de 2006. Visto el 15 de diciembre de 2017 a través del vínculo https://www.apc.org/es/pubs/carta-de-apc-sobre-derechos-en-internet

económico local, la participación pública, el acceso a la información, la buena gobernanza y la erradicación de la pobreza. Pero no habría que dar por sentado que la innovación tecnológica genera un beneficio automático. Las organizaciones de la sociedad civil (OSC), los gobiernos y los entes reguladores deberían ser concientes del poteucial de Internet para reforzar las desigualdades existentes.

1.2 El derecho a acceder a la infraestructura sin importar dónde se viva Internet funciona como una estructura pública global. Dicha infraestructura debe estar ampliamente distribuida y ser soporte del ancho de banda suficiente para permitir a las personas de todas partes del mundo utilizar ese potencial para hacerse oír, mejorar su vida y expresar su creatividad. La gente tiene derecho a contar con una columna vertebral de la red (conocida como 'backbone') bien distribuida y conectada a la red internacional.

1.3 El derecho a los conocimientos.- El conociuiento y las aptitudes permiten a las personas usar y adaptar Internet para cubrir sus necesidades. Los gobiernos locales y nacionales, las organizaciones internacionales y comunitarias, y las entidades del sector privado deben apoyar y promover oportunidades gratuitas o de bajo costo en las áreas de capacitación, metodologías y materiales relativos al uso de Internet para el desarrollo social.

1.4 Derecho a interfaces, contenido y aplicaciones accesibles para todos y todas (diseño inclusivo) Las interfaces, contenidos y aplicaciones deben diseñarse para garantizar el acceso a todos y todas, incluso las personas con discapacidades físicas, sensoriales o cognitivas, las personas analfabetas y las que hablan lenguas minoritarias. Se debe promover y apoyar el principio de diseño inclusivo y el uso de tecnologías de asistencia para ayudar a las personas con capacidades diferentes a tener los mismos beneficios que aquellas que no son discapacitadas.

1.5 Derecho al acceso igualitario para hombres y mujeres En varios lugares, las mujeres y los hombres no tienen acceso igualitario a informarse, definir, acceder, usar y adaptar Internet a sus necesidades. Los esfuerzos en pos de incrementar el acceso deben reconocer y eliminar las desigualdades de género existentes. Debe haber plena participación de la mujer en todas las áreas relativas al desarrollo de Internet para garantizar la igualdad de género.

1.6 Derecho a un acceso asequible Los/as responsables de la formulación de políticas y regulaciones deben garantizar que cada persona tenga un acceso asequible a Internet. El desarrollo de la infraestructura de telecomunicaciones y el establecimiento de normas, precios, impuestos y aranceles debería hacer posible el acceso a personas de cualquier nivel de ingresos.

1.7 Derecho al acceso en el lugar de trabajo Para muchas personas, el lugar de trabajo es el principal –o único- punto de acceso a Internet. Ellas deben poder acceder a la red en los lugares de trabajo, incluso con fines educativos y para la protección de los derechos laborales.

1.8 El derecho al acceso público Muchas personas no gozarán nunca de acceso privado a computadores o a Internet. Debe haber puntos de acceso público disponibles, como telecentros, bibliotecas, centros comunitarios, clínicas y escuelas, para que todas las personas puedan tener acceso a una distancia razonable de su lugar de residencia o trabajo. Esto es especialmente importante para la gente joven de los países donde el acceso a Internet aún no está suficientemente extendido o no es asequible.

1.9 Derecho a acceder y crear contenidos cultural y lingüísticamente diversos En los sitios web, las herramientas en línea y el software predominan las lenguas latinas. Ello afecta el desarrollo de contenidos locales en lenguas no latinas e impide el intercambio de contenidos entre las culturas. El desarrollo técnico debe alentar la diversidad lingtlística en Internet y simplificar el intercambio de información entre las lenguas.

Tema 2 Libertad de expresión y asociación

Artículo 18, DUDH: Toda persoua tiene derecho a la libertad de pensamiento, de conciencia y de religión.

Artículo 19, DUDH: 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.

Artículo 20, DUDH: Toda persona tiene derecho a la libertad de reunión y de asociación pacíficas.

2.1 Derecho a la libertad de expresión La libertad de expresión debe protegerse contra infracciones por parte de los gobiernos y los actores no estatales. Internet es un medio para el intercambio público y privado de opiniones e informaciou a través de todo tipo de frouteras. La gente debe poder expresar opiniones e ideas, y compartir infornación libremeute cuando usa Iuternet.

2.2 Derecho a estar libre de censura Internet debe estar protegida coutra todo intento de silenciar las voces críticas y de censurar contenidos o debates sociales y políticos.

2.3 Derecho a participar en manifestaciones en línea Las organizaciones, comunidades e individuos deben tener libertad para usar Internet con el propósito de organizar manifestaciones y participar en ellas.

Tema 3 Acceso al conocimiento

Artículo 27, DUDH: Toda persona tiene derecho a tomar parte libremente en la vida cultural de la comunidad, a gozar de las artes y a participar en el progreso científico y en los beneficios que de él resulten.

3.1 Derecho a tener acceso al conocimiento El acceso al conocimiento y a un fondo comunal y saludable de conocimiento difundidos es la base del desarrollo humano sustentable. Dado que Internet permite el intercambio de conocimientos y la creación colaborativa de conocimiento a una escala sin precedentes, debería ser el foco de la comunidad del desarrollo.

3.2 Derecho a la libertad de información Los gobiernos nacionales y locales, así como las organizaciones internacionales públicas, deben garantizar la transparencia y la responsabilidad poniendo a disposición la información relevante para la opinión pública. Deben asegurarse de que dicha información se difunda en línea mediante el uso de formatos compatibles y abiertos, y de que la misma sea accesible incluso si se usan computadores más antiguos y conexiones lentas a Internet.

3.3 Derecho al acceso a la información financiada por fondos públicos Toda la información que se produce con el apoyo de fondos públicos, incluso las investigaciones científicas y sociales, deben ser accesibles en forma gratuita para todos y todas.

Tema 4 Intercambio de aprendizaje y creación – software libre y desarrollo tecnológico

Artículo 27, DUDH: Toda persona tiene derecho a tomar parte libremente en la vida cultural de la comunidad, a gozar de las artes y a participar en el progreso científico y en los beneficios que de él resulten.

4.1 Derecho al intercambio Internet ofrece una extraordinaria posibilidad de intercambio de información y conocimiento, así como nuevas formas de creación de contenidos, herramientas y aplicaciones. Los proveedores de herramientas, servicios y contenidos de Internet no deben prohibir a las personas la utilización de Internet para compartir el aprendizaje y la creación de contenidos. La protección de los intereses de los creadores debe hacerse de manera coherente con la participación abierta y libre en el flujo de conocimiento científico y cultural.

4.2 Derecho al software libre Apoyamos el uso de software libre. El manejo de ese software es empoderador, genera nuevas aptitudes, es más sustentable y estimula la innovación local. Alentamos a los gobiernos a elaborar políticas que estimulen el uso de software libre, sobre todo en el sector público.

4.3 Derecho a estándares tecnológicos abiertos Los estándares técnicos que se usan en Internet deben mantenerse abiertos para permitir la interoperatividad y la innovación. Los nuevos desarrollos tecnológicos deben cubrir las necesidades de todos los sectores de la sociedad, sobre todo los que se ven enfrentados a limitaciones y obstáculos cuando están en línea (como las comunidades que usan escritura no latina o las personas con capacidades diferentes, las que usan computadores más antiguos y las que carecen de conexiones de alta velocidad).

4.4 Derecho a beneficiarse de la convergencia y los contenidos multimedia Internet es una plataforma multimedia. El acceso y la regulación deben basarse en su potencial de uso para diversificar la creación y la posesión de contenidos en línea en múltiples formatos – por ejemplo, la radio y la televisión comunitarias.

Tema 5 Privacidad, vigilancia y encriptación

Artículo 12, DUDH: 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.

5.1 Derecho a la protección de datos Las organizaciones públicas o privadas que requieren información personal de los individuos deben recolectar los datos mínimos necesarios y durante un mínimo período de tiempo. Sólo deben procesar datos para los mínimos propósitos establecidos. La recolección, uso, entrega y retención de dicha información debe cumplir con una política transparente de privacidad y que permita a las personas saber para qué se les piden datos, cómo serán usados y corregir errores. Los datos recolectados deben protegerse contra su difusión sin autorización y los errores de seguridad deben rectificarse sin demora. La información se debe borrar cuando ya no es necesaria para los objetivos para los que fue obtenida. La opinión pública debe ser alertada sobre el potencial mal uso de los datos suministrados. Las organizaciones tienen la responsabilidad de notificar a las personas cuando ocurre una violación, pérdida o robo de información.

5.2 Derecho a no estar bajo vigilancia Las personas deben poder comunicarse sin correr peligro de vigilancia ni intercepción.

5.3 Derecho a usar encriptación Las personas que se comunican por Internet deben tener derecho a usar herramientas de codificación de mensajes que garanticen una comunicación segura, privada y anónima.

Tema 6 Gobernanza de Internet

6.1 Derecho a una supervisión multilateral y democrática de Internet.- La gobernanza de Internet debe ser multilateral y democrática, con plena participación de los gobiernos, el sector privado, la sociedad civil y las organizaciones internacionales. Ningún gobierno deberá tener un papel preeminente con relación a la gobernanza de Internet.

6.2 Derecho a la transparencia y la accesibilidad Todos los procesos de toma de decisiones relativos a la gobernanza y al desarrollo de Internet deben ser abiertos y accesibles a nivel mundial, regional y nacional.

6.3 Derecho a contar con un Internet descentralizado, colaborativo e interoperable El desarrollo tecnológico y la administración central de recursos de Internet deben

estar descentralizados y ser colaborativos, además de ayudar a garantizar que la red sea interoperable, funcional, estable, segura, eficiente y extensible en el largo plazo.

6.4 Derecho a una arquitectura abierta Internet, como "red de redes", está hecha de varias redes interconectadas, con base en la idea técnica subyacente de una arquitectura de red abierta, en la que cualquier tipo de red pueda ser conectada y estar disponible públicamente. Se debe proteger esa característica de la arquitectura.

6.5 Derecho a estándares abiertos La mayoría de los protocolos esenciales de Internet se basan en estándares abiertos eficientes, confiables y aptos a la implementación mundial con escasas –o inexistentes- restricciones de licenciamiento. Las especificaciones de los protocolos deben seguir estando a disposición de todas las personas, sin costo, reduciendo los obstáculos para el acceso y permitiendo la interoperatividad.

6.6 Derecho a la neutralidad de Internet y al principio de extremo-a-extremo La neutralidad de Internet, referida sobre todo al transporte efectivo de paquetes, permite que la inteligencia se base sobre todo en computadores, aplicaciones, servidores, telefonía móvil y otros dispositivos que se encuentran en los puntos terminales de la red. Esto ha permitido el desarrollo de un amplio abanico de nuevas actividades, industrias y servicios de Internet en los extremos de la red y ha convertido a la red en una herramienta importante dentro del amplio contexto del desarrollo económico y social. La mayor parte del poder y el alcance de Internet se deriva del valor de su efecto de red. Cuanta más gente accede a la red, mayor es su valor como medio de intercambio de información y comunicación. **El principio de extremo a extremo y la neutralidad de la red deben defenderse contra todo intento de centralizar el control y tener un Internet "de primera y segunda categoría"**.

6.7 Derecho a Internet como un todo integral.- Esta interoperatividad básica forma parte del valor de Internet como bien público global y no debería fragmentarse por amenazas de creación de intranets nacionales, el uso de filtros de contenidos, una vigilancia sin garantías, invasión de privacidad y limitaciones a la libertad de expresión.

Tema 7 Conciencia, protección y realización de los derechos

7.1 Derecho a la protección de derechos, la conciencia y la educación.- Los derechos de las personas como usuarias de Internet deben estar protegidos por declaraciones internacionales de derechos humanos, legislación y prácticas políticas. Los organismos nacionales, regionales y mundiales de gobierno deben poner a disposición la información sobre derechos y procedimientos relativos a Internet. Esto implica una educación pública para informar a las personas sobre sus derechos cuando usan Internet y sobre los mecanismos para contrarrestar violaciones a esos derechos.

7.2 Derecho a anteponer un recurso cuando ocurre una violación de derechos La gente necesita un acceso público y gratuito a mecanismos eficientes y confiables para tratar los casos de violación de derechos. Cuando los derechos humanos y derechos en Internet están en peligro debido a contenidos de la red, o por vigilancia ilegítima, e incluso cuando se limita la libertad de expresión y otros derechos, las personas afectadas deben tener acceso a mecanismos para anteponer recursos contra las infracciones.

Sobre esta Carta

Esta Carta fue desarrollada por primera vez en 2001-2002 por miembros de APC y organizaciones socias en los talleres sobre "Derechos en Internet" que se realizaron en Europa, Asia, América Latina y África. Los temas y principios que se subrayan expresan los puntos de vista y los objetivos de nuestra comunidad con relación a los derechos de los pueblos y las organizaciones a usar Internet libremente, sobre todo para su trabajo en pos de la justicia social, económica y ambiental. Nos referimos específicamente a Internet, pero estos principios son relevantes a todas las TIC (incluso el teléfono, la radio y otras).

La Carta no pretende abarcar todo. Subraya algunos temas específicos que los individuos, las organizaciones de la sociedad civil, los medios comunitarios, los organismos reguladores y los/as responsables de políticas deben considerar en sus esfuerzos de protección del derecho a comunicarse libremente vía Internet y realizar su potencial para crear un mundo mejor informado y más justo.

La Carta se inspiró originalmente en la "Carta de comunicación de los pueblos" y en la declaración del "Movimiento mundial por la voz del pueblo en los medios y la comunicación del siglo XXI", y estaba asociada a ambos.

Esta versión revisada de dicha Carta pretende sobre todo incluir temas de la gobernanza de Internet que fueron planteados durante la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y se incluyeron en el informe del Grupo de Trabajo sobre la Gobernanza de Internet y en la Agenda de Túnez para la Sociedad de la Información. También tiene en cuenta la discusión sobre Internet como bien público global, que tuvo lugar en las deliberaciones de la CMSI y en la Fuerza de Tarea en TIC de la ONU. Esta revisión se basa también en las recomendaciones sobre gobernanza de Internet que hizo APC a la CMSI.

En ese mismo tenor, las Naciones Unidas han sumado esfuerzos con sus países miembros para generar una respuesta normativa a las inquietudes de los cibernautas. Por lo anterior y como consecuencia del Foro para la Gobernanza en Internet, surgió la Carta de Derechos Humanos y Principios para Internet. La misma se emitió en el año 2009 por la Coalición Dinámica por los Principios y Derechos de Internet (IRPC). Después de un par de borradores, en el año 2015 se logró la versión vigente, que rescata el reporte de Frank La Rue para las Naciones Unidas y de esta se desprenden 10 principios fundamentales:

1. Universalidad e Igualdad: Todos los seres humanos nacen libres e iguales en dignidad y derechos, que deben ser respetados, protegidos y cumplidos en el entorno *on* line.
2. Derechos y Justicia Social: Internet es un espacio para la promoción, protección y cumplimiento de los Derechos Humanos y el avance de la justicia social. Toda persona tiene el deber de respetar los derechos de los demás en el entorno *on line*.
3. Accesibilidad: Toda persona tiene igual derecho a acceder y utilizar Internet de forma segura y libre.
4. Expresión y Asociación: Toda persona tiene derecho a buscar, recibir y difundir información libremente en Internet sin censura ni interferencias. Todo el mundo tiene derecho a asociarse libremente a través de Internet, con fines sociales, políticos, culturales o de otro tipo.
5. Confidencialidad y protección de datos: Toda persona tiene derecho a la privacidad online. Esto incluye el no ser vigilado, el derecho a utilizar cifrado y el derecho al anonimato. Todo el mundo tiene derecho a la protección de datos, incluyendo el control sobre la recolección, retención, transformación, eliminación y divulgación de sus datos personales.
6. Vida, Libertad y seguridad: El derecho a la vida, la libertad y la seguridad deben ser respetados, protegidos y cumplidos en Internet. Estos derechos no deben ser infringidos o utilizados para infringir los derechos de otros.
7. La Diversidad: La diversidad cultural y lingüística en Internet debe ser promovida, la innovación técnica y política deben alentar y facilitar la pluralidad de expresión.
8. Igualdad: Todo el mundo tendrá acceso universal y abierto a los contenidos de Internet, libre de priorizaciones discriminatorias, filtrado o control de tráfico por razones comerciales, políticas o de otro.[3]
9. Normas y Reglamento: La arquitectura de Internet, los sistemas de comunicación y los formatos de documentos y datos se deben basar en estándares abiertos que garanticen la interoperabilidad completa, la inclusión y la igualdad de oportunidades para todos.
10. Gobierno: Los Derechos Humanos y la Justicia Social deben ser la base jurídica y normativa sobre la que operar en Internet. Esto sucederá de manera transparente y multilateral, con un Internet basado en los principios de la participación inclusiva y la rendición de cuentas.

Por ahora, las cosas parecen marchar conforme lo dicta la Carta de la APC y la Carta de la Coalición Dinámica, en beneficio del comportamiento de los cibernautas, sin embargo, el proceder del Estado insiste en involucrarse en perjuicio de la

[3] Éste es el derecho que se ha estudiado de forma consuetudinaria como "neutralidad en la red".

neutralidad de la red. A saber, el 14 de diciembre de 2017 la Comisión Federal de Comunicaciones de Estados Unidos, revocó la norma 2015 que protegía la neutralidad de la red[4] y aseguraba el acceso igualitario a Internet de todos los individuos y compañías. Este principio adoptado por el otrora presidente Barack Obama, permitía asegurar una Internet libre y abierta e impedía a los proveedores de servicios de banda ancha en la unión americana, bloquear, ralentizar o dar prioridad a algunos contenidos disponibles en línea. La medida que ahora toma el gobierno de Donald Trump, no sólo genera críticas de los cibernautas, sino de empresas tecnológicas como Google, Facebook y *Alphabet* (producto de Google). La revocación en comento, favorece a empresas tecnológicas como Verizon y AT&T, pero pone en grave peligro los derechos digitales de los cibernautas y podría implicar una excesiva vigilancia de los proveedores de servicio de Internet, que discriminarían por sector, ancho de banda y posición económica, el contenido que podría estar disponible a favor de cada usuario; situación que luce posible, ante las políticas racistas que ha favorecido el actual presidente americano.

Este tipo de escenarios parecen fortalecer la postura de los organismos no guberuamentales y sociedad civil que protestan la participación del Estado en las reglas de Internet. El objeto del presente capítulo, será analizar algunas de las libertades consagradas en el ciberespacio a favor de los ciudadanos digitales y cómo es que los gobiernos han enfrentado, legislativamente, la regulación de estas prerrogativas.

XI. 1 Gobierno Abierto y Gobierno Electrónico

En su origen, no existe una doctrina universalmente reconocida sobre la temporalidad del nacimiento de estas filosofías, que regulan el comportamiento del Estado frente a los ciudadanos. Sin embargo, parece que debemos respeto a la paternidad detrás del concepto "Gobierno Abierto" (en adelante "GA") a Wallace Parks, en cuyo artículo póstumo utilizara el término "open government" de forma escrita, aún en su cargo de consejero del Subcomité Especial sobre Información Gubernamental del Congreso de los Estados Unidos; este texto se puede consultar en la famosa *Freedom of Information Act*. A pesar del difícil debate que enfrentó la ley sobre la libertad de información, el presidente Lyndon B. Johnson finalmente promulgaría el cuerpo normativo en el año 1966, logrando que Estados Unidos reconociera el "derecho a saber", acreditando su calidad de "sociedad abierta". Jurídica y políticamente el GA adquirió relevancia cuando Barack Obama lo aplicara como eje fundamental de la

[4] *BBC*. "El gobierno de Donald Trump pone fin a las normas que aseguraban la neutralidad de Internet en Estados Unidos". BBC MUNDO. 14 de diciembre de 2017. Recuperado el 15 de diciembre de 2017 a través del vínculo http://www.bbc.com/mundo/noticias-internacional-42359904

Directiva 2009 *Memorandum on Transparency and Open Government* a través de la cual afirmó que el Gobierno debía ser transparente, participativo y colaborativo:

> [...] **El gobierno debe ser transparente**. La transparencia promueve la responsabilidad y proporciona información para los ciudadanos sobre lo que está haciendo su gobierno. La Información mantenida por el gobierno federal es un activo nacional. Mi Administración tomará las medidas apropiadas, consistente con la ley y la política, para divulgar información rápidamente en formas que el público puede encontrar y usar fácilmente Los departamentos y agencias ejecutivas deberían aprovechar las nuevas tecnologías para poner la información sobre sus operaciones y decisiones en línea y de fácil acceso para el público. Los departamentos y agencias ejecutivas también deberían solicitar comentarios del público para identificar la información de mayor uso para el público.
>
> **El gobierno debe ser participativo**. El compromiso público mejora el gobierno efectividad y mejora la calidad de sus decisiones. El conocimiento está ampliamente disperso en la sociedad y los funcionarios públicos se benefician al tener acceso a ese conocimiento disperso. Los departamentos ejecutivos y agencias deberían ofrecer a los estadounidenses mayores oportunidades para participar en formulación de políticas y proporcionar a su gobierno los beneficios de su experiencia colectiva e información. Los departamentos y agencias ejecutivas también deberían solicitar comentarios del público sobre cómo podemos aumentar y mejorar las oportunidades de participación pública en el gobierno.
>
> **El gobierno debe ser colaborativo**. La colaboración involucra activamente a los estadounidenses en el trabajo de su gobierno. Los departamentos y agencias ejecutivas deberían usar herramientas innovadoras, métodos y sistemas para cooperar entre sí, en todos los niveles del gobierno, y con organizaciones sin fines de lucro, negocios e individuos en el sector privado. Ejecutivo los departamentos y las agencias deberían solicitar comentarios del público para evaluar y mejorar su nivel de colaboración e identificar nuevas oportunidades para la cooperación.[5]
>
> **(El énfasis es añadido)** [Traducción del autor]

En ese tenor, el concepto no sólo pertenece al discurso político, sino al sector tecnológico quiénes afirman que el movimiento GA surge de 3 corrientes fundamentales: i) Ley de Acceso a la Información, ii) Partidarios de *software libre* y datos académicos abiertos; y iii) Emprendedores de innovaciones abiertas, incluyendo los

[5] OBAMA, Barack. *Memorandum on Transparency and Open Government. Administration of Barack H. Obama, 2009.* Transparencia y gobierno abierto. Memorándum para los jefes de los departamentos ejecutivos y agencias. Estados Unidos de América, enero 21 de 2009. Visto el 16 de diciembre de 2017 a través del vínculo https://www.archives.gov/files/cui/documents/2009-WH-memo-on-transparency-and-open-government.pdf

enrolados en el Gov 2.0. La OCDE ha definido como gobierno abierto a aquel que se caracteriza por la transparencia de sus acciones, la accesibilidad de los ciudadanos a sus servicios e información, y la receptividad gubernamental a nuevas ideas, demandas y necesidades; por otro lado, el Banco Mundial define al gobierno electrónico como aquel que usa tecnologías de información capaces de transformar su relación con ciudadanos, empresas y otras ramas del gobierno, y pueden servir una variedad de fines: mejor producción de servicios gubernamentales, una interacción más fluida con la empresa privada, mayor empoderamiento del ciudadano a través del acceso a la información o un desempeño gubernamental más eficiente; y de acuerdo con Gartner Research, el gobierno abierto (o, según sus términos, gobierno 2.0) se define como el uso gubernamental de las tecnologías de la web 2.0 para aumentar la colaboración y transparencia, así como para transformar potencialmente la forma en que las agencias gubernamentales operan y se relacionan con los ciudadanos.[6] Sin embargo, no parece justo convertir en sinónimos los conceptos de GA e *E-government*, ya que todo gobierno abierto depende del uso de las tecnologías de la información y comunicación (TIC) para la prosecución de los fines propuestos, por lo que indefectiblemente ha de transformarse en un sistema gubernamental que busque el acercamiento transparente y colaborativo a través de la Internet 2.0; es decir, un gobierno abierto ha de ser gobierno electrónico, para ser dignamente llamado de esa forma, conforme lo dicta esta doctrina política.

El debate sobre la definición se acotó en el año 2015, cuando se celebró la 70 Asamblea General de las Naciones Unidas, en la que se adoptó la Agenda 2030 para el Desarrollo Sostenible y se firmó la *Carta Internacional de Datos Abiertos*. A saber del gobierno federal mexicano, la Carta es una iniciativa de gobiernos, organizaciones de la sociedad civil, sector privado y expertos en la materia, que articula los principios fundamentales para coordinar y promover la adopción de los Datos Abiertos a nivel global. Por "datos abiertos" debemos entender los datos digitales que son puestos a disposición con las características técnicas y jurídicas necesarias para que puedan ser usados, reutilizados y redistribuidos libremente por cualquier persona, en cualquier momento y en cualquier lugar. Estos datos deben regirse por principios de acción común para que los datos sean un medio para el desarrollo sostenible.[7] En ese tenor, la página oficial de *Open Data Charter,* reconoce 6 principios rectores:

[6] OSLAK, Oscar. *Ideas sobre gobierno abierto.* Gobierno Abierto. El valor social de la información Pública. Isa Luna Pla y José Antonio Bojórquez Pereznieto, Coordinadores. Instituto Tabasqueño de Transparencia y Acceso a la Información Pública. Instituto de Investigaciones Jurídicas, UNAM. México, 2015. Visible el 16 de diciembre de 2017 a través del vínculo https://archivos.juridicas.unam.mx/www/bjv/libros/9/4016/17.pdf

[7] GOB.MX/ México Digital. *Carta Internacional de Datos Abiertos.* Acciones y Programas. México, 30 de septiembre de 2015. Visible el 16 de diciembre de 2017 a través del vínculo https://www.gob.mx/mexicodigital/acciones-y-programas/carta-internacional-de-datos-abiertos

1. Abiertos por defecto
2. Oportunos y exhaustivos
3. Accesible y útil
4. Comparable e interoperable
5. Para mejorar la gobernanza y la participación ciudadana
6. Para el desarrollo incluyente y la innovación[8]

Actualmente, México actúa como Presidente de la Alianza para el Gobierno Abierto, junto con otros 12 países; y junto con los países miembros del Comité Directivo de la AGA (Brasil, Chile, Croacia, Estados Unidos, Filipinas, Francia, Georgia, Indonesia, Reino Unido, Rumania, Sudáfrica y Tanzania) lideró la firma de una declaración de alto nivel para impulsar la implementación efectiva de la Agenda 2030 a través de los principios de gobierno abierto, resaltando el uso de los datos abiertos como catalizador de la colaboración entre todos los sectores de la sociedad. En México dichas directrices corren a cargo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), del Archivo General de la Nación y de la Coordinadora de la Estrategia Nacional Digital (Yolanda Martínez).

A favor de los ciudadanos y cibernautas, estos principios aparecen como facultades y prerrogativas frente a los Estados en su comportamiento *on line* y *off line*. Sin duda, un gobierno abierto resulta el mejor ambiente para la implementación de cualquier política que pretenda respetar las calidades fundamentales de sus ciudadanos, en un escenario de competitividad y progresividad tecnológica. Es decir, la plataforma idónea para el ejercicio de cualquier derecho digital, de ahí la importancia de su estudio para el presente capítulo y la obra que propongo al respetable lector.

XI. 2 Habeas Data

El concepto que refiere a *Habeas Data* tiene su origen en Latinoamérica, cuyo nombre se compone de dos vocablos: del latín *habeas* (que significa tener) y del término en inglés *data* (que significa información o datos) y está destinada a salvaguardar el derecho a la protección de datos personales ante un tribunal competente. El Maestro Martín Pérez Cazares lo considera sinónimo del Derecho a la Intimidad en el Derecho Informático, y los define como una derivación del *Habeas Corpus*, que permite

[8] OPEN DATA CHARTER. *Carta Internacional de Datos Abiertos. Principios.* Versión completa en español. Octubre 28 de 2015. Visto el 16 de diciembre de 2017 a través del vínculo https://opendatacharter.net/principles-es/

al ciudadano el acceso a datos, información o registros y tener conocimiento de datos propios en poder de otro.[9]

Históricamente, la Constitución brasileña de 1988 es la primera en introducir la acción de *hábeas data*, que se ocupa de garantizar el derecho de los ciudadanos al acceso y rectificación de sus datos personales en posesión de terceros. Seguirían a este movimiento constitucionalista Argentina, Ecuador, Perú, Paragnay, Uruguay y Venezuela. Posteriormente, Chile es el primero en emitir una ley de protección de datos (1999), mientras en Argentina, con su ley de 2000, es el país que más ha desarrollado el derecho en América Latina. Según lo define el Maestro Ángeles Guzmán, la acción de *hábeas data* es "el derecho que asiste a toda persona –identificada o identificable- a solicitar judicialmente la exhibición de los registros –públicos o privados- en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud, a requerir la rectificación, la supresión de datos inexactos u obsoletos o que impliquen discriminación. Se considera una herramienta que protege a la persona contra calificaciones sospechosas incluidas en registros"[10]. En el caso mexicano, parece correcta la apreciación del Maestro Pérez Cazares, en el sentido de argüir que la legitimación de esta figura, aparece en los artículos 14 y 16 de la Constitución Política de los Estados Unidos Mexicanos, mismos que en la parte conducente, dictan:

> Artículo 14. A ninguna ley se dará efecto retroactivo en perjuicio de persona alguna. **Nadie podrá ser privado** de la libertad o de sus propiedades, posesiones o **derechos**, sino mediante juicio seguido ante los tribunales previamente establecidos, en el que se cumplan las formalidades esenciales del procedimiento y conforme a las Leyes expedidas con anterioridad al hecho.
>
> Artículo 16. Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo.
>
> **Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley**, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones

[9] PÉREZ CAZARES, Martín. *El Habeas Data o Derecho a la Intimidad en el Derecho Informático.* Orden Jurídico Nacional. Gobierno Federal de los Estados Unidos Mexicanos. Recuperado el 15 de diciembre de 2017 a través del vínculo http://www.ordenjuridico.gob.mx/Congreso/pdf/98.pdf

[10] GUZMÁN, Ángeles. *Hábeas Data.* Diccionario de Derecho Procesal, Constitucional y Convencional. Tomo II. Instituto de Investigaciones Jurídicas. Serie Doctrina Jurídica Número 693.

de orden público, seguridad y salud públicas o para proteger los derechos de terceros…[11] **(El énfasis es añadido)**

Por lo que refiere a la regulación secundaria, México después concebiría la Ley Federal para la Protección de Datos Personales en Posesión de Particulares y recientemente, la Ley General para la Protección de Datos Personales en Posesión de Sujetos Obligados. En ese mismo tenor, el artículo 15 de la Constitución Política Colombiana, parece ser el mejor ejemplo normativo –comparado con otras constituciones- que consagra el derecho fundamental de *Habeas Data;* mismo que en la parte conducente, prescribe:

Artículo 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.[12]

Para consideración del lector, el Maestro Cazares propone la existencia de cinco objetivos en la protección del Habeas Data, con independencia de si esto ha de formularse en la Carta Magna o en leyes secundarias.

1. Que una persona pueda acceder a la información que sobre ella conste en un registro de datos;
2. Que se actualicen los datos atrasados;
3. Que se rectifiquen los inexactos;
4. Que se asegure la confidencialidad de cierta información legalmente obtenida para evitar su conocimiento por terceros;
5. Supresión en los procesos de obtención de información del requisito de la llamada información sensible, entre ellas la vida íntima, ideas políticas, religiosas, gremiales, cuentas bancarias.[13]

[11] CONGRESO DE LA UNIÓN. *Constitución Política de los Estados Unidos Mexicanos.* Visible a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf

[12] CORTE CONSTITUCIONAL. *Constitución Política de Colombia.* Consejo Superior de la Judicatura. Centro de Documentación Judicial-CENDOJ. Biblioteca Enrique Low Murtra. Actualizado 2016. Recuperado el 14 de diciembre de 2017 a través del vínculo http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf

[13] Supra. Cit. 311

XI. 3 Derecho al Olvido Digital (*Right to erasure/ Right to be forgotten)*

Este derecho parece tener su incierto origen en el universo del Derecho Penal, específicamente, en el Derecho Penitenciario, tal como lo reconoce el Doctor Eric Tardif Chalifour, al afirmar que el **Derecho al olvido digital** surge del concepto de *droit á l'oubil* que desarrolló el sistema jurídico Francés y que resguarda el bien jurídico de la "reputación"; en este sistema, los convictos que purgaban su sentencia en reclusión, invocaron esta facultad bajo la premisa que se les tuviera por rehabilitados y por ende, desligados de su pasado.[14] Se puede considerar a éste como la modalidad digital del Derecho al Olvido que proviene del añejo Derecho de Privacidad que se acuñó en 1890 por Brandeis y Warren, en su famoso artículo para *Harvard Law Review.*[15] Sin duda, debe su fortaleza al estudio y progreso legislativo que se ha mostrado en el globo, respecto al tratamiento de los datos personales y el derecho de privacidad de referencia. Fue en el año 2014 cuando la Corte de Justicia de la Unión Europea, tuviera la compleja labor de definir el alcance y espacio que guarda el Derecho al Olvido, frente a otras prerrogativas fundamentales. En lo particular, el caso que inició en el 2010 ante Cortes Españolas, incluye la demanda de un ciudadano español en contra del litisconsorcio conformado por un diario nacional, Google Spain y Google Inc., toda vez que el actor estimó que el mostrar sus datos personales referidos en un proceso jurisdiccional, dentro de los resultados del motor de búsqueda, era innecesario e irrelevante por haberse cumplido la sentencia condenatoria. En la demanda que nos ocupa, el actor solicitó al diario eliminar su nombre de las páginas impresas y digitales que incluyeran sus datos personales, asimismo, demandó a Google remover los datos personales y eliminarlo de los resultados de búsqueda. Por Sentencia del 13 de mayo de 2014, la Corte de la Unión Europea –que atrajo el asunto por solicitud de la corte española- emitió su resolución en términos de la Directiva 1995 sobre Protección de Datos y el *right to be forgotten,* en él contenida, bajo las siguientes consideracioues:

a) Aplicación de las leyes de la Unión Europea: Aún si el servidor físico de los demandados en el que se procesan los datos se encuentra fuera de la Unión Europea, la Corte estimó la aplicabilidad de las normas de la unión si el motor de

[14] TARDIF CHALIFOUR, Eric. *El Derecho al Olvido Digital: Entre el Derecho a la Privacidad y el Derecho a la Libertad de Expresión.* Foro Jurídico. México, 2 de diciembre de 2016. Visto el 14 de diciembre de 2017 a través del vínculo https://www.forojuridico.org.mx/derecho-al-olvido-digital-derecho-la-privacidad-derecho-la-libertad-expresion/

[15] WARREN, Samuel & BRANDEIS, Louis. *The Right to Privacy.* Hard Law Review. Vol. 14. Número 5. Diciembre 15 de 1890. Recuperado el 14 de diciembre de 2017 a través del vínculo http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf

búsqueda operaba a través de una subsidiaria de un país miembro que promoviera los recursos de la matriz;

b) Aplicación de las leyes de la Unión Europea para protección de datos para motores de búsqueda.- Los motores de búsqueda se consideran controladores de datos personales. Por lo anterior, Google es responsable ante la ley europea al incluir datos personales en los resultados de su motor. En ese sentido, resulta aplicable la norma europea y el derecho al olvido reconocido por ésta.
c) Sobre el Derecho al Olvido.- Los individuos tienen el derecho –bajo ciertas condiciones- para solicitar a los motores de búsqueda remover vínculos con información personales acerca de ellos. Esto aplica cuando la información es imprecisa, inadecuada, irrelevante o excesiva para los propósitos del tratamiento de datos. Sobre el caso que nos ocupa, la Corte otorgó mayor peso al derecho de protección de datos, sobre el interés económico del motor de búsqueda, a pesar de reconocer, que este derecho no puede considerarse absoluto y debe ponderarse contra otros derechos fundamentales como la libertad de expresión en los medios. Este derecho y el criterio de la Corte se fortalecen con la entrada en vigor del Reglamento General de Protección de Datos.

En palabras de la propia Corte, no se puede considerar el Derecho al olvido como un "Súper Derecho" que siempre venza a otros derechos fundamentales como la libertad de expresión y la libertad de los medios. En ese tenor, un justo balance debería analizar el interés legítimo de los usuarios de Internet frente los derechos fundamentales de los demandados. En ese sentido, podríamos argüir que el Derecho al olvido digital se coloca entre los derechos fundamentales de protección de datos personales y la libertad de expresión y resultaría aplicable en límites precisos. En una reflexión puntual, la Corte indica que este derecho no se trata sobre transformar a gente prominente en menos prominente o hacer a los criminales, menos criminales.[16]

Gracias a reformas recientes para la Unión Europea, este derecho se ha elevado a Directiva General, a través del Reglamento Europeo de Protección de Datos (2016/679 *General Data Protection Regulation*). En lo particular, el artículo 17 regula el derecho a ser olvidado (derecho a eliminar), de la siguiente manera:

> Artículo 17. Derecho a Eliminar (Derecho al Olvido)
>
> El titular de los datos tendrá el derecho de obtener del "controlador" la eliminación de datos personales concernientes con él o ella, sin demora y el controlador deberá

[16] EUROPEAN COMISSION. *Factsheet on the Right to be Forgotten ruling (C-131/12).* Press release. Justice. Recuperado el 14 de diciembre de 2017 a través del vínculo http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

obligarse a borrar los datos personales sin demora, siempre que aplique alguna de las siguientes motivaciones:

a) Los datos personales ya no son necesarios en relación con el propósito para el cual fueron recolectados o procesados;
b) El titular de los datos retiro su consentimiento o el tratamiento acordado se basa en el punto a) del artículo 6 (1) o punto a) del artículo 9 (2); y no existe otra razón para continuar procesándolos.
c) El titular de los datos objeta el procesamiento en términos del artículo 21 (1) y no existen razones legítimas para continuar su tratamiento; o el titular de los datos objeta el procesamiento en términos del artículo 21 (2);
d) Los datos personales han sido ilegalmente procesados;
e) Los datos personales deben ser borrados en cumplimiento con una obligación legal de la Unión o ley de los Estados Miembro, en la cual el controlador sea sujeto;
f) Los datos personales han sido recolectados con la intención de ofrecer información de servicios societarios referidos en el artículo 8 (1)

A su vez, el inciso (2) del artículo en cita obliga al responsable del manejo de los datos que hubiese hecho públicos los mismos, a borrarlos mediante el uso de cualquier tecnología disponible y absorbiendo los costos de su implementación. Sin embargo, el controlador no estará obligado a la eliminación, cuando el tratamiento de los datos sea necesario para el ejercicio de la libertad de expresión e información, por cumplimiento a una ley de la Unión de los Estados Miembros, que considere dichos datos de interés público para ejercicio de la autoridad oficial; por razones de salud pública; por razones de archivo para beneficio del interés público o búsquedas científicas o históricas o fines estadísticos.

En términos de la exposición de motivos del Reglamento General para la Protección de Datos que nos ocupa, tiene clara la importancia del derecho al olvido digital para los iudividuos que forman parte de la Unión Europea. Los párrafos 65 y 66 de la parte conducente dictan:

[...]Un interesado debe tener derecho a que se rectifiquen los datos personales que le conciernen y un "derecho al olvido" cuando la retención de dichos datos infrinja el presente Reglamento o la legislación de la Unión o del Estado miembro a la que esté sujeto el responsable del tratamiento. En particular, **un interesado debe tener derecho a borrar sus datos personales** y dejar de procesarlos cuando los datos personales ya no sean necesarios en relación con los fines para los que se recopilan o procesan, cuando el interesado haya retirado su consentimiento u objete al tratamiento de los datos personales que le conciernen, o cuando el tratamiento de sus datos personales no se ajuste a lo dispuesto en el presente Reglamento. Ese derecho es relevante en particular cuando el sujeto de los datos ha dado su consentimiento como un niño y no es

plenamente consciente de los riesgos que conlleva el procesamiento, y luego desea eliminar dichos datos personales, especialmente en Internet. El sujeto de los datos debe ser capaz de ejercer ese derecho a pesar de que ya no es un niño. Sin embargo, la retención adicional de los datos personales debe ser legal cuando sea necesario, para ejercer el derecho a la libertad de expresión e información, para el cumplimiento de una obligación legal, para el desempeño de una tarea llevada a cabo en interés público o en el ejercicio de la autoridad oficial conferida al controlador, por razones de interés público en el área de la salud pública, para fines de archivo de interés público, con fines de investigación científica o histórica o con fines estadísticos, o para el establecimiento, ejercicio o defensa de reclamos legales.

Para reforzar el derecho al olvido en el entorno en línea, el derecho a borrarlo también debe ampliarse de tal forma que un responsable del tratamiento que ha hecho públicos los datos personales esté obligado a informar a los controladores que procesan dichos datos personales para borrar cualquier enlace, copias o réplicas de esos datos personales. Al hacerlo, ese controlador debería tomar medidas razonables, teniendo en cuenta la tecnología disponible y los medios disponibles para el controlador, incluidas las medidas técnicas, para informar a los controladores que procesan los datos personales de la solicitud del interesado [...][17]

(El énfasis es añadido)

Para fines prácticos, gran parte de las legislaciones en la orbe no reconocen dentro de su derecho positivo el Derecho a ser olvidado, empero, incluyen robustas figuras de Protección de Datos Personales que permiten el ejercicio de los Derechos ARCO: Acceso, Rectificación, **Cancelación y Oposición**. En los términos expuestos, resulta inconcuso que este derecho se puede estudiar desde la perspectiva del ejercicio de "**Cancelación y Oposición**", debido a los alcances jurídicos similares que presentan. En ese tenor, podemos afirmar que el inicio del ejercicio de esta facultad surge con la solicitud de protección de datos personales bajo algunas de las modalidades ARCO, empero, el olvido en la web resulta aplicable bajo la solicitud de oposición y cancelación, en el entendido que para verse satisfechos, también existen hipótesis que limitan su ejercicio en beneficio del interés público o bien, otro derecho fundamental que pudiere poseer mayor peso en el caso concreto.

A pesar de los esfuerzos legislativos que hemos invocado, no todo resulta progresivo en la aplicación de este derecho e inclusive, algunas organizaciones defensoras de Derechos Digitales consideran que éste es un disfraz para "censurar Internet" y dejar en manos de Tribunales el coartar la libertad de expresión en medios digitales

[17] Traducción LIMÓN, Jaime. Puede consultar el texto original en inglés, a través de: COUNCIL OF THE EUROPEAN UNION. *General Data Protection Regulation.* Bruselas, 6 de abril de 2016. Visto el 13 de diciembre de 2017 a través del vínculo http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

bajo el pretexto de la correcta aplicación del derecho a ser olvidado. Verbigracia, la *Red en Defensa de los Derechos Digitales* (México) promovería juicio de amparo en contra de la sentencia emitida por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), por la que ordenaba a Google México retirar un enlace en la *Revista Fortuna.* R3D (por su acrónimo digital) obtuvo la sentencia favorable del Séptimo Tribunal Colegiado de Circuito del Centro Auxiliar de la Primera Región, se concedió el amparo y el INAI debió reiniciar el procedimiento de protección de datos personales, garantizando el derecho de audiencia de la Revista Fortuna.[18] Estos precedentes permiten que algunos internautas consideren a esta prerrogativa el Derecho de Censura y un grave enemigo de la libertad de expresión en Internet, empero, no debe soslayarse la existencia de hipótesis normativas que limitan el ejercicio de la eliminación de datos personales en la web y que generan un adecuado balance con otros derechos fundamentales.

Más allá del derecho positivo, la práctica de este derecho digital a favor de clientes que han confiado su imagen a mi firma, me ha llevado a optar por mecanismos de autocomposición que proponen las mismas redes sociales y portales web, los cuales brindan herramientas digitales muy sencillas para eliminar información que pudiere atender contra la imagen, reputación, honor o decoro de una persona; tal es el caso de *Blogger,* un producto de la familia *Google*, que permite la denuncia de contenido que viola derechos de autor, suplantación de identidad, copia ilegalmente información con reserva de derechos e inclusive, sitios que publiquen desnudos de menores de edad, inciten al odio o violencia, incurran en actividad de *Spam* y particularmente, que divulguen datos personal o imágenes que atenten contra derechos de personalidad. Así las cosas, a través de su mecanismo de "denuncia" y un sencillo reporte que incluye copiar *Url* que direccione al contenido que se desea eliminar, impresión de pantalla y una breve manifestación bajo protesta de decir verdad, se procede a analizar el sitio por los administradores del Producto; insisto, en la experiencia digital, los asuntos que he tramitado por esa vía se resuelven en máximo 24 horas. Para conocer las condiciones particulares sobre cada hipótesis, sugiero visitar el vínculo https://support.google.com/blogger/contact/private_info y en el caso de cada herramienta, estudiar los mecanismos de autocomposición que proponen los portales, en afán de proteger el *derecho al Olvido.*

XI. 4 Personalidad Virtual, Derecho al Anonimato y Cifrado

La personalidad virtual consiste en la representación digital de la identidad del usuario y el modelo que elija el internauta para operar y navegar en la red de redes, ya

[18] R3D. ¡Ganamos! Tribunal anula resolución del INAI sobre el faso "derecho al olvido". México, 24 de agosto de 2016. Visto el 14 de diciembre de 2017 a través del vínculo https://r3d.mx/2016/08/24/amparo-inai-derecho-olvido/

sea través de la publicidad o el anonimato. En el primer escenario, el cibernauta elige brindar acceso total a su imagen y nombre, así como demás datos personales que permitan su libre identificación, sin embargo, existe la facultad digital para evitar que estos datos sean publicados, lo que permite al cibernauta acudir a la red a través de un pseudónimo o alias, a esto se le considera derecho digital de anonimato. La *Electronic Frontier Foundation* define a esta prerrogativa como la facultad para actuar o comunicarse sin usar o presentar el nombre o identidad propios (**anonimato**); protege la determinación del nombre o identidad propios; asimismo, faculta el uso del nombre asumido o inventado que no se pueda asociar con una identidad legal o habitual (**seudonimato**). La *World Wide Web* Foundation -organización global sin ánimo de lucro fundada por el inventor de la Web, sir Tim Berners-Lee- , a través de la Carta de Internet Guatemala, defiende el Derecho al Acceso, Derecho a la neutralidad de la red, derecho a cruzar las fronteras, derecho a participar, derecho a no ser sujeto a la vigilancia, derecho a los datos, derecho a publicación propia, derecho a disentir, derecho a quedar libre de responsabilidad y finalmente, su artículo 5° prescribe el Derecho Al anonimato, el cual regula de la siguiente forma:

> Todo ser humano tiene derecho a no ser identificado y a no revelar su identidad cuando utiliza Internet y las tecnologías digitales. Este derecho comprende la libertad de expresión en el anonimato, a leer de forma anónima, a navegar por Internet de forma anónima y a utilizar herramientas de comunicación seguras, especialmente herramientas de encriptación de hardware y software. Todo ser humano puede acceder a Internet y comunicarse electrónicamente usando instrumentos, incluyendo sistemas técnicos, que protejan su anoninato y evitar la recogida de datos personales, en particular, con el fin de ejercer las libertades civiles y políticas sin ser objeto de discriminación ni censura.
>
> En el caso de violaciones de la dignidad y los derechos fundamentales de cualquier persona, así como en otros casos previstos por la ley, los tribunales pueden requerir la ideutificación del autor de una comunicación con un auto motivado.

El 22 de mayo de 2015, el relator especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, de la Asamblea General, de las Naciones Unidas, David Kaye, presentó un informe sobre la utilización del cifrado y el anonimato en las redes digitales. En este informe concluye que el cifrado[19] y el

[19] En el reporte de referencia, Kaye define al cifrado como: "…un proceso matemático de "convertir mensajes, información o datos en algo ilegible, excepto para el destinatario deseado" 2 , protege la confidencialidad y la integridad del contenido contra el acceso o la manipulación de terceros. El cifrado fuerte, que antes era exclusivo de los militares y los servicios de inteligencia, ahora está al alcance del público, a menudo de manera gratuita, para proteger los correos electrónicos, las comunicaciones telefónicas, las imágenes, los discos duros y los navegadores. Con el "cifrado de clave pública", la forma dominante de seguridad de extremo a extremo para los datos en tránsito, el remitente utiliza la clave

anonimato en la era digital, permiten a los individuos un mejor ejercicio de sus derechos de libertad de opinión y de expresión y, por lo tanto, merecen una protección sólida. Estas son prerrogativas que surgen en respuesta al **derecho a no ser molestado a causa de opiniones**, en términos del artículo 19, párrafo I, del Pacto Internacional de Derechos Civiles y Políticos; el reconocimiento de razón y conciencia que emana del artículo primero de la Declaración Universal de Derechos Humanos; al **derecho a la libertad de expresión** previsto en el artículo 19, párrafo 2, del Pacto Internacional de Derechos Civiles y Políticos; así como el **derecho a la vida privada** que regula el artículo 12 de la Declaración Universal de Derechos Humanos y el diverso 17 del Pacto Internacional de Derechos Civiles y Políticos. De este reporte, destaca positivamente lo siguiente:

- Es importante que los usuarios hallen medios para protegerse en línea, que los gobiernos ofrezcan dicha seguridad en la ley y en las políticas y que los actores empresariales diseñen, elaboren y comercialicen productos y servicios seguros por defecto;
- Una herramienta de anonimato conocida, la red Tor, cuenta con más de 6.000 servidores descentralizados en todo el mundo que reciben y transmiten datos varias veces para ocultar la información de identidad sobre los puntos extremos, creando así un anonimato sólido para sus usuarios;
- El cifrado y el anonimato, separados o en su conjunto, crean una zona de privacidad para proteger opiniones y creencias;
- Los artistas pueden servirse del cifrado y el anonimato para salvaguardar y proteger su derecho a la expresión, en especial en las situaciones en que, además que el Estado crea restricciones, la sociedad tampoco tolera las opiniones o formas de expresión poco convencionales;
- El cifrado ofrece seguridad para que los individuos puedan "verificar que sus comunicaciones sean recibidas únicamente por los destinatarios a las que están dirigidas, sin injerencias ni modificaciones, y que todas las comunicaciones que reciban estén también libres de injerencias" (véase A/HRC/23/40 y Corr.1, párr. 23). Dado el potencial del análisis de los metadatos para explicitar "el comportamiento, las relaciones sociales, las preferencias privadas y la

pública del destinatario para cifrar el mensaje y sus adjuntos, y el destinatario utiliza su propia clave privada para descifrarlo. El cifrado también se puede utilizar para crear firmas digitales con el fin de garantizar que un documento y su expedidor son auténticos, para autentificar y verificar la identidad de un servidor y para proteger la integridad de las comunicaciones entre clientes contra la falsificación o la manipulación del tráfico por terceros (ataques de intermediario)…"KAYE, David. *Informe del Relator Especial sobre la Promoción y protección del derecho a la libertad de opinión y de expresión.* Consejo de Derechos Humanos. 29° período de sesiones. Asamblea General de las Naciones Unidas. A/HRC/29/3. 22 de mayo de 2015. Visto el 16 de diciembre de 2017 a través del vínculo http://www.eldiario.es/cultura/G1509588_EDIFIL20151209_0001.pdf

identidad de una persona" (véase A/HRC/27/37, párr. 19), el anonimato puede ser muy importante para proteger la correspondencia;
- Las personas y la sociedad civil pueden ser objeto de injerencias y a taques de actores estatales y no estatales, contra los cuales el cifrado y el anonimato pueden proporcionar protección;
- Las restricciones al cifrado y el anonimato, como elementos facilitadores del derecho a la libertad de expresión, deben cumplir tres requisitos bien conocidos: cualquier limitación a la libertad de expresión debe estar fijada por la ley; únicamente puede imponerse por razones legítimas (descritas en el artículo 19, párrafo 3, del Pacto Internacional de Derechos Civiles y Políticos); y debe ajustarse a estrictos criterios de necesidad y proporcionalidad; y
- El cifrado y el anonimato, y los conceptos de seguridad subyacentes, proporcionan la privacidad y seguridad necesarias para el ejercicio del derecho a la libertad de opinión y de expresión en la era digital.

Sin embargo, David Kaye reconoce la presencia de un lado oscuro detrás del cifrado y el anonimato[20], ya que terroristas y delincuentes comunes utilizan estas herramientas para esconder sus actividades, por lo que se dificulta a los gobiernos la prevención y la realización de investigaciones. Por otro lado, algunos Estados han aplicado o han propuesto aplicar el denominado "acceso de puerta trasera" en los productos disponibles en el mercado, obligando a los desarrolladores a instalar puntos débiles que permitan a las autoridades gubernamentales acceder a las comunicaciones cifradas (Sugiero lectura sobre el Capítulo XII sobre el caso "San Bernardino"). Verbigracia, autoridades del Reino Unido y los Estados Unidos abogan por que se exija un acceso de puerta trasera, como un mecanismo necesario para interceptar el contenido de las comunicaciones cifradas por delincuentes o terroristas.

Este derecho se abordó desde la luz del "pseudónimo" en el Reglamento Europeo de Protección de Datos (2016/679 *General Data Protection Regulation*); a saber, el inciso 5), artículo primero define:

> [...] 'seudonimización' significa el tratamiento de datos personales de tal manera que los datos personales ya no pueden atribuirse a un sujeto de datos específico sin el uso de información adicional, siempre que dicha información adicional se mantenga por

[20] Según la Ley 428884-6 que modifica la Ley de Información, Tecnologías de la Información y Protección de la Información de la Federación Rusa, demanda a los blogueros que cuenten con más de tres mil lectores diarios a inscribirse en el registro de la entidad reguladora de los medios de comunicación e identificarse de forma pública; asimismo, obliga a los usuarios que accedan a las redes públicas de Wi-Fi a identificarse legalmente. *REUTERS*. "Russia demands Internet Users show ID to access public Wifi". Business Insider. Moscú, 8 de agosto de 2014. Visto el 16 de diciembre de 2017 a través del vínculo http://www.businessinsider.com/r-russia-demands-internet-users-show-id-to-access-public-wifi-2014-08

separado y esté sujeta a medidas técnicas y organizativas para garantizar que los datos personales no se atribuyan a una persona física identificada o identificable [...][21]

Por su parte, la Coalición Dinámica sobre Derechos y Principios en Internet (*Dynamuc Coalition on Internet Rights and Principles*), propone la Carta de Derechos Humanos y Principios en Internet con base en la Declaración de Principios de Ginebra y la Agenda de Túnez para la Sociedad de la Información (la cuál referimos con anterioridad en la presente obra). En esta carta se propone la regulación y respeto de diversos derechos digitales, sin embargo, el capítulo Privacidad en Internet, propone la posibilidad de presentarse de forma anónima en la web y a utilizar cifrado en las comunicaciones, de la siguiente manera:

8.- Privacidad en Internet Tal y como se consagra en el artículo 12 de la Declaración Universal: "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". En Internet el derecho a la privacidad incluye:

d) Protección de la personalidad virtual: **Toda persona tiene derecho a una personalidad virtual: La personalidad virtual de la persona humana (es decir, la identificación personal en la información) es inviolable. Las firmas digitales, nombres de usuario, contraseñas, códigos PIN y TAN no deben ser utilizadas o modificadas por terceros sin el consentimiento del propietario. La personalidad virtual de la persona humana debe ser respetada**. Sin embargo, el derecho a una personalidad virtual no debe ser mal utilizado en detrimento de los demás.
e) Derecho al anonimato y utilizar el cifrado Toda persona tiene derecho a comunicarse de forma anónima en Internet. **Toda persona tiene derecho a utilizar la tecnología de encriptación para garantizar una comunicación segura, privada y anónima**.[22]
(El énfasis es añadido)

El documento que invoco adquiere fortaleza y sentido, si tomamos en cuenta que la Coalición tuvo su origen en el Foro de Gobernanza en Internet de las Naciones

[21] COUNCIL OF THE EUROPEAN UNION. *General Data Protection Regulation.* Bruselas, 6 de abril de 2016. Visto el 13 de diciembre de 2017 a través del vínculo http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

[22] INTERNET RIGHTS & PRINCIPLES COALITION. *Carta de Derechos Humanos y Principios en Internet.* Enero de 2015. Primera Edición. Organización de las Naciones Unidas. Visto el 15 de diciembre de 2017 a través del vínculo http://internetrightsandprinciples.org/site/wp-content/uploads/2017/03/IRPC_spanish_1stedition_final.pdf

Unidas. Así las cosas, en enero de 2015 se publicó la versión "Carta 2.0" y pretende proveer un marco de trabajo reconocible en los Derechos Humanos Internacionales para el cumplimiento y el avance de los Derechos Humanos en el ambiente *on line*.

XI. 5 Testamento Digital Inverso

Este acto jurídico no debe confundirse con el Derecho al Olvido y constituye una modalidad del testamento digital que se estudió en el capítulo segundo de la presente Obra. A diferencia del Derecho al Olvido, que constituye la facultad por la cual el usuario determina que no quiere que ciertos datos personales, privados o confidenciales sobre su persona sean recordados por la web, a través de sus diversos motores de búsqueda, el testamento digital inverso ("TDI") actúa como el acto jurídico a través del cual, el usuario determina la eliminación total de su identidad digital en un portal, sitio o herramienta. Tal como lo expone el Director Jurídico de *i-Olvido*, Ramón Rey Ruíz, el TDI podría considerarse como una especie de "derecho al olvido post-mortem".[23] En palabras de Rey Ruíz, el TDI implica que al fallecimiento del causante, toda su herencia digital, por su propia y única voluntad, debe ser eliminada y nadie tendrá acceso a la misma. Así, sus cuentas de correos, perfiles de redes sociales y cualquier portal que capture su identidad digital, deberán ser canceladas. Por su lado, Francisco Márquez Villén define al TDI de la siguiente manera:

> El Testamento Digital Inverso supone…no dejar ninguna de las pertenencias del patrimonio digital en herencia. Todo el patrimonio digital se borraría, evitando así cualquier uso indebido, hackeo o phishing. Si bien se considera una forma sucesión digital, lo que se deja en herencia es una obligación de hacer, en este caso borrar el contenido del patrimonio digital que poseía en vida el fallecido…[24]

Tal como se sostuvo en el capítulo segundo de la presente obra, las plataformas centralizadas como Twitter, Instagram, Facebook y las diversas herramientas de Google, han adoptado mecanismos que garantizan el libre y anticipado ejercicio de esta modalidad a través de los canales prescritos por cada plataforma, en la cual se puede definir el tiempo, características y, en su caso, legatario que podrá ejecutar la

[23] REY RUIZ, Ramón. "Testamento Digital Inverso, ¿una forma de ejercicio del derecho al olvido?" *Diario Jurídico*. España, 23 de octubre de 2014. Visto el 16 de diciembre de 2017 a través del vínculo http://www.diariojuridico.com/testamento-digital-inverso-una-forma-de-ejercicio-del-derecho-al-olvido/

[24] MÁRQUEZ VILLÉN, Francisco. *Testamento Digital. Nuevas tecnologías y derecho*. Publicaciones de IN DIEM. Abogados. Madrid, Sevilla. Enero, 2016. Visto el 16 de diciembre de 2017 a través del vínculo https://www.in-diem.com/wp-content/uploads/2016/01/CUADERNOS-IN-DIEM-Abogados-Testamento-Digital.pdf

voluntad anticipada del usuario. Empero, la complicación jurídica de esta modalidad ocurre cuando dicha voluntad no se fija a través del portal o red social y ésta se pretende colocar en un Testamento Público ante Notario Público, es decir, un acto jurídico de corte tradicional. Al respecto, se sugieren fijar las siguientes condiciones en el testamento:

1. Se deberán fijar los nombres de usuario (ID) y contraseñas necesarias para tener acceso al patrimonio original que se pretenda incluir en la herencia;
2. Al heredero en particular (o herederos) se deberá dejar instrucción específica sobre el ejercicio de la voluntad post-mortem. En ese sentido, es menester que se indique si se opta por la transmisión a través de un Testamento Digital o bien, si ocurrirá bajo un Testamento Digital Inverso. En el caso del último, especificar si se han ocupado las herramientas que cada portal o red social ofrece para tal efecto;
3. En caso que exista controversia entre el Testamento Público que se otorgue ante fedatario público y la voluntad que se fije a través de los portales o redes sociales, se debe brindar mayor peso a la que se otorgue ante el perito en Derecho, ya que, se presume, se otorgó con las solemnidades y formalidades que exigen las leyes civiles locales.

Adicionalmente, el titular del patrimonio digital deberá tener control sobre los bienes digitales que pretende incluir en la herencia y conocer si las plataformas permiten transmisión post-mortem, en afán de no dificultar la tarea jurisdiccional en la ejecución y adjudicación de los bienes virtuales respectivos. Es importante señalar al lector, que debido a lo complejo y novedoso de la presente figura, no existen referentes en el derecho positivo que fortalezcan el contenido del presente parágrafo, con independencia, de lo expuesto en el capítulo segundo de la presente obra.

XII
CAPÍTULO

Valoración de la Prueba Cibernética e Informática: Electrónica y Digital

Desde 2014 *Apple* brinda una herramienta de encriptación a sus equipos que permite que estos sean matemáticamente infranqueables, lo que brinda mayor seguridad a sus usuarios y desincentiva el ataque de hackers o probables intervenciones del gobierno. Sin embargo, esta garantía de invulnerabilidad (*no backdoor*) se convirtió en el dilema del gobierno americano en el año 2015, cuando el 2 de diciembre dos practicantes radicales del Islam atacaron un edificio en el sur de California; a esto se le conoció como el caso "San Bernardino".[1] Uno de los sospechosos, Syed Farook, trabajó para el condado y durante su gestión se le entregó un iPhone 5C. Esto facilitó la investigación del FBI ya que los equipos anteriores a esa categoría aún cargaban automáticamente los datos, imágenes y archivos del equipo

[1] Si desea conocer más sobre este caso, puede consultar la web con el golpe de voz "San Bernardino shooting" o bien, a través del vínculo http://www.bbc.com/news/world-us-canada-34993344 (NEWS, *BBC*. "San Bernardino Shooting: What we know so far". Diciembre 2015)

al servicio de nube conocido como *iCloud*. Empero, esto no demostró los hechos ni acreditó las causas probables del atentado terrorista, debido a que sólo lograron rescatar datos hasta octubre de 2014, fecha en la que la *Apple* liberó su sistema de encriptamiento y transformó sus equipos móviles en los "más seguros del mundo". Hasta este punto, el Buró Federal de Investigación requirió a la compañía fabricante el desencriptar los equipos o, en su caso, desarrollar un *backdoor* para su propio sistema operativo, es decir, *hackear* el equipo de tal suerte que se permitiera la continuidad en investigación. La respuesta de Tim Cook –CEO de la compañía- fue tajante, pues a pesar de manifestar que no simpatizan con los terroristas, también indicó que los extremistas fallecidos eran usuarios *Apple* con garantía de protección activa, ello se tradujo en seguridad y encriptamiento absoluto de su información, incluida aquella relacionada en la comisión del delito. En respuesta a las declaraciones de Cook, Barack Obama –el entonces presidente de los Estados Unidos de América- se expresó públicamente en contra de la decisión de la compañía desarrolladora, arguyendo un inverosímil estado de Derecho que protege la privacidad de un par de usuarios, sobre la seguridad nacional, en tanto que el Buro de investigación a su cargo, amenazó con hackear estos equipos con la ayuda de *Apple* o sin ésta. Procesalmente, es importante comprender que la indebida intervención de los equipos pudiere generar la ilicitud en las pruebas obtenidas –independientemente del "envenenamiento" de las mismas conforme a la "Teoría del Fruto del Árbol Envenenado"-, sin embargo, las consecuencias de derecho no sólo se limitan a su debida obtención, sino a la debida incorporación procesal, en atención de su naturaleza.

Sin entrar a un debate de moral según lo plantea el dilema político-jurídico anterior, ¿cómo aportar un correo electrónico a un proceso?, ¿cómo incorporar un mensaje de *WhatsApp* a un procedimiento jurisdiccional? Ello sin vulnerar la privacidad de las partes involucradas y, en su caso, sin atentar contra la naturaleza no tradicional de dichos medios de convicción. Independientemente del precedente negativo que implica el caso de San Bernardino para la seguridad internacional, es indiscutible que cada día son más los procesos que requieren la incorporación jurídica de probanzas que se generan a través de medios cibernéticos, informáticos, electrónicos y digitales, sin embargo, ha sido poco el estudio jurídico que se brinda a los mismos y, en muchas ocasiones, se ocupan sinónimos que únicamente entorpecen el camino hacia su desahogo judicial, por tanto, también complican el camino legislativo que pudiere ser la delgada línea de legalidad entre la prudente intervención de comunicaciones o la obtención de pruebas ilícitas en perjuicio de la privacidad de los usuarios. El objeto del presente capítulo no sólo será el diseminar la ambigüedad con la que se trata a estos medios de convicción, sino delimitar los principios de valoración de la prueba y estándares que el juez debe tomar en cuenta –de forma obligatoria- para dictar una sentencia adecuada a la naturaleza *sui generis* de estos medios de convicción.

XII. 1 Concepto de Documento *Lato Sensu* (sentido amplio)

El Diccionario de la Real Academia Española en su segunda y tercera acepción brindan aquellas de mayor importancia para la construcción de la presente obra: "Escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo…Cosa que sirve para testimoniar un hecho informar de él, especialmente del pasado."[2]A su vez, el Diccionario de Derecho Procesal Civil de Eduardo Pallares, sostiene que: "…documento es toda cosa que tiene algo escrito con sentido inteligible"; en el entendido que "escribir" se comprende como la actividad mediante la cual el hombre expresa ideas y sentimientos por medio de la palabra escrita, sin importar si dicha escritura se hace sobre papel o cualquier otro material, ni resultando indispensable que el lenguaje esté formado por "vocablos". En ese tenor, el procesalista Pallares, manifiesta: "¿Los documentos taquigráficos son pruebas científicas o documentales? El Código las incluye entre las científicas, pero deben considerarse como documentales, porque contienen algo escrito con sentido inteligible…".[3]

En atención a su raíz etimológica, la voz documento deriva de *docere* (enseñar, hacer, conocer) y conforme lo dicta el Maestro Hernando Devis Echandía, es posible comprender un concepto de documento, desde el punto de vista estricto y amplio, a saber:

> El documento, como el testimonio o la confesión, es el resultado de una actividad humana; pero, como observa *Carnelutti*, mientras los últimos son *actos*, el primero es una cosa creada mediante un acto y de allí se concluye que mientras que el acto testimonio o confesión es por sí mismo representativo del hecho testimoniado o confesado, el acto que crea el documento no es representativo del hecho narrado en éste, sino que se limita a crear el vehículo de representación, que es ese documento. En **sentido estricto**, es documento <<toda cosa que sea producto de un acto humano, perceptible cou los sentidos de la vista y el tacto, que sirve de prueba histórica indirecta y representativa de un hecho cualquiera>>…Ha existido la tendencia de identificar los conceptos de documento e instrumento o escrito, como si todos los documentos consistieran en escritos; esto es consecuencia de que el Código Civil de Napoleón y los que en éste se basan, se refieren únicamente a los últimos, distinguiéndolos en instrumentos públicos y privados. Pero, como de lo acabado (sic) de exponer se concluye, existen numerosos documentos que no consisten en escritos, como planos, dibujos, cuadros, fotografías, radiografías, películas, cintas magnetofónicas y discos con grabaciones de conversaciones y sonidos de cualquier clase…La representación, por lo tanto, no está en el

[2]Diccionario de la Real Academia Española. *Documento*. Puede consultar todas las acepciones a través del vínculo http://dle.rae.es/?id=E4EdgX1. Consultado en línea el 10 de julio de 2017.

[3]PALLARES, Eduardo. *Diccionario de Derecho Procesal Civil. Concepto de "documento"*. Editorial Porrúa. Vigésima Octava Edición. México, 2005.

> documento, sino en el juicio de quien lo asume como medio de prueba e incluye en un concepto **amplio de documento** la huella de un evento natural o de un pie, por lo cual concluye afirmando que <<una definición correcta del documento prescinde del concepto de representación, que es propiamente la operación lógica de quien lo asume como medio de prueba, y debe operar únicamente en la relación documento-prueba>>, porque lo esencial no es la representación, sino un *posterius* respecto de su existencia[4]

Según la Doctrina de Chiovenda, podemos comprender que documento *lato sensu* es toda representación material destinada e idónea a reproducir una determinada manifestación de pensamiento como una voz fijada duramente: *vox mortua*. Por otro lado, el propio procesalista indica que documento en *strictu sensu* serán exclusivamente los "escritos" (léase aquello escrito en papel).[5] Interpretaciones y estudios procesales que permiten advertir la doble naturaleza del documento, asimismo, la separación que debe existir entre su capacidad de representación y el objeto material en sí mismo, sobre el cual se han plasmado hechos históricos que permiten acreditar que, en un momento específico, existieron hechos o actos de relevancia jurídica.

Derivado de las teorías tradicionalistas se ha determinado que los documentos pueden tener dos características: i) representativos y ii) declarativos, sin embargo, autores como José V. Acosta, señalan que gracias a los avances tecnológicos, podemos agregar una tercera clasificación: iii) transmisión. Ello permite fortalecer la distinción que existente entre un documento en sentido amplio y en sentido estricto, entre "escrito" y documento. Conforme a lo anterior, el Maestro Hernando Devis Echandía, señala:

> Se ha confundido en ocasiones el documento con la materia de que está formado, especialmente con el papel utilizado para los escritos o instrumentos privados y públicos, pero no sólo existen otras materiales utilizables para esta clase de documentos, como telas, maderas, cueros…sino que el documento es algo más que esa materia y principalmente está constituido por su contenido gráfico, escrito o figurativo o de otra clase (como en los discos y cintas magnetofónicas)…Un pedazo de tela, de cuero o de papel, sin ningún contenido declarativo o simplemente representativo, puede ser una pieza de convicción, que constituye un indicio, pero no es un documento…Además, se identifica erróneamente el contenido con el continente, siendo así que, incluso cuando se trata de escritos o instrumentos, la forma es la exterioridad del hecho o acto jurídico documentado [...][6]

---

[4] DEVÍS, Hernando. *Teoría General de la Prueba Judicial*. Tomo II. Sexta Edición. Pontificia Universidad Javeriana, Bogotá, Facultad de Ciencias Jurídicas. De la Prueba Por Documentos. Bogotá, 2002.

[5] Ob. Cit. 109

[6] Ob. Cit. 110

Afirmación que permite aclarar que en tanto los documentos cibernéticos, que referiremos a continuación, contengan un elemento declarativo o representativo de valor jurisdiccional, estos deben ser analizados bajo la categoría que les corresponda; en atención a lo que se pretende acreditar con el contenido de los mismos y no bajo el estricto examen del continente de dicho hecho o acto jurídico. Bajo la naturaleza del documento en sentido amplio, es que se permite la presencia de documentos tales como el cibernético e informático, en tanto que el documento electrónico y digital, cuentan con características que les permiten ser considerados dentro de la categoría de documento en sentido estricto; según lo describo a continuación.

XII. 2 Documento Cibernético e Informático

Al comprender la dicotomía que se presenta en el parágrafo anterior, es indispensable definir el marco de estudio de las ciencias que se aplican, multidisciplinariamente, al Derecho. Es decir, comenzaré por definir la Cibernética y la Informática, para posteriormente analizar la naturaleza de los documentos que se pudieren originar, en cada rama de estudio, para efectos de la ciencia jurídica.

En primer término, se define a la Cibernética, como la ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas –definición muy similar a la que aporta el Diccionario Legal de Black según la voz *cybernetics*-; creado y regulado mediante computadora.[7] En letras del Doctor Julio Téllez Valdés, la Cibernética es la ciencia que se encarga del estudio de la comunicación y control entre el hombre y la máquina, tal como lo concibe el matemático estadounidense Norbert Wiener (1948). Invita a reconocer a esta ciencia interdisciplinaria como aquella que estudia la forma en que el cerebro –humano- brinda instrucciones a las máquinas y, a su vez, reconoce la participación de la **Informática** en su estudio.[8] La Informática se define en el Diccionario de la Real Academia Española como el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras[9], en tanto que el Doctor Téllez Valdés la considera un neologismo conformado por los vocablos información y automatización, sugerido por Phillipe Dreyfus (1962); misma que describe como el conjunto de técnicas destinadas al tratamiento

[7] Diccionario de la Real Academia Española. *Cibernético, ca.* Puede consultar todas las acepciones a través del vínculo http://dle.rae.es/?id=98YYoXW Mismo que se consultó en línea el 10 de julio de 2017.

[8] TÉLLEZ Valdés, Julio. *Derecho Informático*. Cuarta Edición. Editorial McGrawhill. México 2009.

[9] Diccionario de la Real Academia Española. *Informática, co.* Puede consultar todas las acepciones a través del vínculo http://dle.rae.es/?id=LY8zQy3. Mismo que se consultó en línea el 10 de julio de 2017.

lógico y automatizado de la información para una adecuada toma de decisiones. Así las cosas, es inconcuso que la cibernética como ciencia interdisciplinaria se conforma, entre otras disciplinas, por la informática, por lo que es asequible afirmar que existen distinciones claras entre un documento de origen cibernético y otro de carácter informático.

El documento cibernético podría definirse como la acreditación intangible de la existencia de una instrucción de un usuario a una máquina integrada por circuitos, esto permitiría probar que, en un determinado momento, un sujeto encendió una computadora, la conecto a la corriente directa o bien, simplemente instaló, regeneró, copió o borró un disco duro. Conductas que podrían generar consecuencias jurídicas si se colocan estas hipótesis en situaciones similares a: i) No se cuenta con autorización para operar cierta computadora, ii) La computadora no se debía encender por instrucciones del ingeniero o iii) Se copió o borró información que pudiere tener calidad de confidencial o secreto industrial.

Ahora bien, los medios informáticos son las computadoras (máquinas integradas por circuitos) o herramientas dentro de las mismas (léase aplicaciones o programas de cómputo) creadas con el fin de automatizar la información. En consecuencia de lo anterior, el documento informático podría definirse como la acreditación cibernética, que advierte la existencia de la instrucción de un hombre hacia una computadora, para iniciar un proceso de automatización de información, sin que éste constituya la información automatizada *per se*. Es decir, el documento informático es la evidencia intangible a través de la cual, la computadora deja un rastro de la instrucción del inicio, progreso y fin de un proceso de automatización, sin que el resultado de ello sea considerado también informático, según se estudia en el parágrafo siguiente. Verbigracia, la hora de apertura de un procesador de texto (herramienta que permite automatizar un texto, en sentido contrario de lo que implicaría un proceso mecánico o manuscrito) y de forma más clara, la hora de última conexión que muestra *WhatsApp*. A su vez, los medios informáticos pueden dividirse en dos categorías según la forma en que los documentos pueden almacenarse y distribuirse: i) Electrónico y ii) Digital

XII. 3 Documento Electrónico y Digital

El Diccionario Legal de Black define a los medios electrónicos como cualquier dispositivo que almacena y permite la distribución o el uso de información electrónica (televisión, radio, Internet, fax, CD-ROM, DVD y cualquier otro medio electrónico)[10]. Por su lado, el Doctor Julio Téllez define al documento electrónico

[10] Diccionario de Black de Leyes. *Medios Electrónicos*. Puede consultar dicha acepción a través del vínculo http://espanol.thelawdictionary.org/medios-electronicos/ mismo que se revisó el pasado 10 de julio de 2017.

como el conjunto de impulsos eléctricos que recaen en un soporte de computadora y que, sometidos a un adecuado proceso, permiten su traducción a lenguaje natural mediante una pantalla o impresora, asimismo, resalta que para evitar las ambigüedades en el uso de electrónico o digital, prefiere denominarles documentos informáticos –no obstante lo sostenido en el parágrafo anterior-; en el entendido que éstos se crean con la intervención no ya de una computadora, sino de todo un sistema informático.[11] Definición que resulta consonante con lo que hasta ahora hemos expuesto, pero que no permite brindar las características esenciales de cada tipo de documento, en términos del objeto del presente capítulo. En atención de ello, es el propio Doctor Téllez Valdés, quien afirma que el documento electrónico puede ser concebido en un sentido amplio y en un sentido estricto: i) *Lato Sensu:* Es el que se forma por una computadora (dispositivo electrónico) a través de sus propios órganos de salida, y que es perceptible por el hombre sin la necesidad de máquinas traductoras; y ii) *Strictu Sensu:* El que aparece instrumentado sobre la base de impulsos electrónicos y no sobre un papel; es el conservado en forma digital en la memoria central de la computadora o en las memorias de masa, y que no puede ser leído o conocido por el hombre sino como consecuencia de un proceso de traducción que hace perceptible y comprensible el código de señales digitales.[12] Sin embargo, parece ser que la definición de documento electrónico en sentido estricto nos remite a una probable acepción de documento digital, en el entendido que éste es contenido que se comprimió digitalmente[13] para ser manipulado, distribuido, representado y transmitido a través de redes informáticas. Concepto que se logra fortalecer gracias a la definición que brinda el Diccionario Legal de Black: "…Lo digital son datos enviados en código de encendido y apagado, representado por 1 y 0 (código binario)".[14] Ello permite aproximarnos a una clasificación concreta respecto de la naturaleza particular de los documentos digitales frente a los documentos electrónicos, en tanto que los primeros dependen de la funcionalidad de los medios informáticos que permitan que la información sea representada mediante código binario –o cualquier otro código- para ser manipulada, distribuida, representada y transmitida a través de canales digitales; mientras que aquéllos de

[11] Ob. Cit. 204

[12] Ibídem.

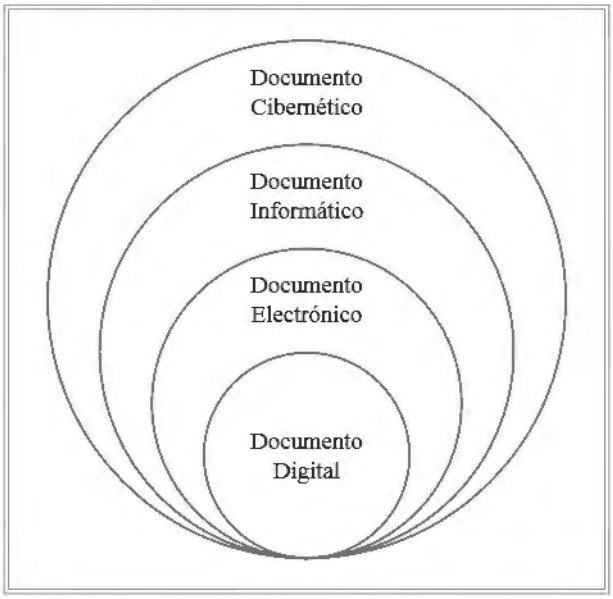
[13] TECHNET, Microsoft. ¿Qué son los medios digitales? En el mismo artículo, se analiza los formatos digitales que se encuentran disponibles para los productos de la familia Microsoft, tales como WMA, WMV, MP3, JPEG y AVI. En general, se considera que se pueden comprimir archivos de audio, video e imágenes, sin embargo, no se pneden descalificar los archivos de texto mismos. Puede consultar el texto íntegro a través de https://technet.microsoft.com/es-es/library/what-is-digital-media-2(v=ws.11).aspx, mismo que se analizó en línea el 10 de julio de 2017.

[14] The Law Dictionary. *What is Digital?* Puede consultar la acepción completa a través de http://thelawdictionary.org/digital/ Se consultó en línea el 10 de julio de 2017.

origen electrónico pueden estar presentes en distintos tipos de almacenamiento, lo que permite su consulta, reproducción y transmisión, sin necesidad que estos se encuentren codificados en un estado de unos y ceros. Si bien es cierto, ambos tipos de documentos pertenecen a la categoría de los documentos informáticos, la diferencia radical entre ambos yace en la calidad para formar parte de la red de redes, en atención a la naturaleza conforme la cual han sido concebidos –informatizados-. Siendo precisos con los medios electrónicos de comunicación que pudieren considerarse digitales, encontramos la televisión digital e Internet, por lo que es inconcuso que los documentos que se generan a través de estas plataformas pueden considerarse documentos electrónicos y particularizando, documentos digitales. Así las cosas, un documento electrónico puede considerarse un archivo de texto generado por un procesador que automatice caracteres (una contrato que se redacta en *Office Word*), mientras que un correo "electrónico" que contiene en archivo adjunto un contrato entre los usuarios, no debería considerarse documento electrónico, toda vez que éste, para su almacenamiento y consulta, depende de la codificación digital. Bajo esta hipótesis, el contrato de referencia mutaría la naturaleza bajo la cual se concibió, en el momento que se carga en el servidor *on line* [*Upload* (léase el capítulo sobre *Explotación digital de los derechos de autor,* dentro de la presente obra)] y ahora pertenece a la red de redes, requiriendo para su consulta, reproducción y comunicación, la interconectividad que sólo la *World Wide Web* permite; el documento electrónico muta en documento digital al momento que éste ingresa a la compleja telaraña de la autopista de la información, en tanto que el contrato que se redactó en el procesador de texto, en su origen no requiere de codificación alguna para su consulta y almacenamiento, sin embargo, dicha situación no perdura cuando adquiere calidad de digital y que por la simple mecánica de su envío a otro servidor, requiere ser transformado en paquetes (TCP/IP) y traducido al sistema binario (FTP). En sentido inverso, la calidad de documento digital no se pierde por realizar el proceso de Descarga/ *Download*, toda vez que esta acción no consiste en retirar el documento de Internet, sino un proceso de reproducción del documento digital para su almacenamiento en dispositivos que no necesariamente se encuentran conectados a la red de redes; así las cosas, este proceso de **descarga** permitirá almacenar una versión del documento bajo la modalidad de electrónico. Es imperativo resaltar que las diversas mutaciones, así como reproducciones que pudiere sufrir el documento, atentan contra el valor probatorio del mismo, toda vez que algunas versiones de éste pudieren vulnerar su integridad y autenticidad en el proceso (según las mismas se definen más adelanta).

Asimismo, se debe considerar la naturaleza de los documentos cibernéticos e informáticos desde la postura de los documentos en sentido amplio, mientras que los documentos en sentido estricto, permiten el ingreso de medios de convicción electrónicos y digitales por la "escritura" que se puede desprender de ellos, vestigio que resulta de trascendencia jurídica aunque ello no se desprenda de un medio tradicional

de probanza –tal como lo es un papel-. Hasta este punto, me permito proponer al lector el siguiente diagrama de Venn:



Según la teoría de conjuntos propuesta, es inconcuso afirmar que todo documento digital es un documento electrónico, a su vez informático y cibernético. Además, todo documento electrónico es informático y cibernético, sin embargo, no necesariamente será digital a pesar de contar con características para poder formar parte del universo de codificación digital. Por su lado, se advierte que todo documento informático es cibernético y éste, podría almacenarse y distribuirse a través de medios electrónicos y digitales, lo cual tendría por origen un documento electrónico o digital, según sea el caso.

Es importante resaltar a favor del lector, que el presente conjunto de Venn, únicamente resulta una propuesta para comprender las categorías de documento desde la perspectiva del análisis técnico jurídico que se brinda, sin que resulte limitante a las posturas legislativas que se presentan en cada país, ni las que a continuación se estudian, las cuales podrían erigirse sobre definiciones legislativas ambiguas que sostengan sinonimia entre informático, electrónico y digital.

XII. 4 Características de los documentos electrónicos y digitales

En diversas legislaciones alrededor del globo se adoptó el sistema de la sana crítica o el principio de libertad de prueba ["que consiste en otorgar libertad a los juzgadores

para determinar los medios de prueba, su eficacia probatoria y la manera de producirlos"] por lo que refiere a la valoración probatoria de soportes informáticos. Según lo expone el Doctor Julio Téllez, algunos soportes se enfrentan al desconocimiento jurídico para ser considerados como prueba dentro de procedimientos jurisdiccionales, con independencia que estos pudieren resultar benéficos en atención a la **durabilidad** y **fidelidad** al original que presentan, respecto de aquéllos de naturaleza tradicional.[15] Afortunadamente para el panorama procesal de las pruebas que actualmente estudiamos, el 30 de enero de 1997 se aprobó por la Comisión de las Naciones Unidades para el Derecho Mercantil Internacional en la Asamblea General de ONU, la Ley Modelo sobre Comercio Electrónico, un mandato con la finalidad de armonizar y unificar a los Países involucrados, en atención de permitir el progreso amplio del comercio internacional. Posteriormente, ésta traería a la vida el proyecto conocido como "Ley Modelo de la CNUDMI sobre Firmas Electrónicas". El mérito de la Ley Modelo en materia de comercio radica en la invitación internacional para dotar de valor probatorio a mensajes de datos que estuvieren contenidos en medios electrónicos, ópticos o similares –léase, digitales-, así como prescribir las reglas para su incorporación a un procedimiento, siempre que cumplieran con los principios contenidos en la propia normativa estandarizada. Inicialmente, conviene invocar el contenido del artículo segundo de dicha Ley, ya que la misma aporta definiciones fundamentales para el entendimiento del presente apartado:

> Artículo 2. — Definiciones Para los fines de la presente Ley: a) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el télex o el telefax; b) Por "intercambio electrónico de datos (EDI)" se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto; c) Por "iniciador" de un mensaje de datos se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él; d) Por "destinatario" de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje, pero que no esté actuando a título de intermediario con respecto a él; e) Por "intermediario", en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él;

[15] TÉLLEZ VALDÉS, Julio. *Derecho Informático*. Capítulo XVI. Valor probatorio de los soportes informáticos. Editorial Mc Graw Hill. Segunda edición. México, 1998. Puede consultar el texto íntegro a través del vínculo https://biblio.juridicas.unam.mx/bjv/detalle-libro/1941-derecho-informatico visto el 29 de noviembre de 2017.

f) Por "sistema de información" se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

Desde el punto de vista semántico, el artículo que reproduzco permite aclarar la unidad de medida mínima a estudiar en el presente capítulo, mismo que se denomina "mensaje de datos", a la cual se puede considerar el *contenido*. A su vez, fija el parámetro jurídico para calificar al soporte que se presentará como prueba dentro de un proceso, ya sea de naturaleza óptica, electrónica o digital; a éste se le considerará el *continente*. Por otro lado, dicta las reglas del juego electrónico, al colocar como sujetos de protección al "iniciador-intermediario-destinatario" que ocupan un sistema de información para generar, enviar, recibir, archivar o procesar un mensaje de datos. A modo de reflexión, la regla general en el proceso dicta que el mensaje informático (contenido) es aquel que se deberá ofrecer, desahogar y valorar dentro de un procedimiento, en tanto que el soporte (continente) debería fungir como el mecanismo, por excelencia, para que éste se fije en el procedimiento y se respeten cada uno de los principios que señala la Ley en cita. Como excepción, algunos Tribunales han optado por aceptar el mensaje de datos, pero no permiten su desahogo a través del soporte *ex profeso;* es decir, se inclinan por posturas de perfeccionamiento de la prueba (pruebas corroborantes) a través de certificaciones notariales, dictamen pericial, inspecciones oculares o cotejos, como si se tratare de pruebas tradicionales.

Si bien es cierto que la Ley Modelo UNCITRAL no resulta aplicable por razón de materia a otras ramas del Derecho, ésta ha servido como base doctrinaria para que los países partes, adapten sus legislaciones más allá del universo mercantil. Así las cosas, se popularizó la postura legislativa de retomar los principios de la Ley Modelo y flexibilizarlos a las diversas ramas del Derecho, siempre que los documentos electrónicos o digitales, respeten los principios y estándares que a continuación se detallan.

XII. 4. 1) Principios: Equivalencia funcional, no discriminación y neutralidad

La *Guía Para La Incorporación Al Derecho Interno* de la Ley Modelo de la CNUDMI sobre Comercio electrónico, tiene como finalidad orientar a los usuarios de los medios electrónicos de comunicación en los aspectos jurídicos de su empleo. Dicha guía reconoce la necesidad de vencer impedimentos al empleo de comercio electrónico y la admisibilidad de mensajes de datos a procesos, frente a conceptos ortodoxos como "escrito", "firma" y "original"; mismos que hemos ido destruyendo –o flexibilizando- en el recorrido de toda la Obra. En ese tenor, iuvita a los Estados incorporados a adaptar su funcionamiento a los nuevos avances técnicos de las comunicaciones. Así las cosas, la Comisión de las Naciones Unidas logró acuñar con

éxito el criterio de "equivalencia funcional", el cual no sólo aplicó a la presente Ley Modelo, sino a la relacionado con Arbitraje Comercial Internacional y el contenido del artículo 13 de la Convención de las Naciones Unidas sobre los Coutratos de Compraventa Internacional de Mercaderías. Bajo ese tenor, el principio de equivalencia funcional se puede definir como el análisis de los objetivos y funciones de uu requisito tradicional de presentación de un escrito consignado sobre papel contra aquél que pudiere presentarse en un soporte electrónico o digital, en atención a los siguientes estándares:

1. Proporcionar un documento legible para todos;
2. Asegurar la inalterabilidad de un documento a lo largo del tiempo;
3. Permitir la reproducción de un documento a fin que cada una de las partes disponga de un ejemplar;
4. Permitir la autenticación de los datos consignados suscribiéndolos con una firma; y
5. Proporcionar una forma aceptable para la presentación de un escrito ante las autoridades. [16]

A saber de quien escribe y de la Comisión de las Naciones Unidas en materia de Comercio, la documentación consignada en medios electrónicos no sólo brinda un grado de seguridad equivalente al de papel, sino superior, en la mayoría de los casos; ya que resulta superior si lo sometemos a un examen de **fiabilidad, originalidad** e **integridad**. Por otro lado, invita a no descartar medios de convicción por tratarse de un mecanismo no tradicional de probanza y en su caso, permitir la evaluación en igualdad de circunstancias de un documento digital frente a uno tradicional (**no discriminación y neutralidad**). Lo anterior resulta claro frente a escenarios procesales en los que alguna de las partes estima que el contenido de un documeuto tradicional fue alterado o no se suscribió por quién se manifiesta; para el caso de los documentos electrónicos y digitales, resulta un trabajo pericial complejo realizar cualquier modificación sobre el autor del documento, la cantidad y calidad del contenido (número de caracteres, espacios, fuente, tamaño e imágenes contenidas), así como la firma que pudiere contener, ya que, la firma consiste en un conjunto de caracteres alfa numéricos que se forjan como la huella digital de dicho soporte, cuya inalterabilidad se considera humanamente invencible; hipótesis que no se podrían defender respecto del documento tradicional. Empero, el principio de equivalencia funcional no debe ser interpretado como la búsqueda en la substitución jerárquica de los documentos tradicionales con aquéllos de naturaleza avanzada, sino como la invitación para la

[16] ONU. CNUDMI. *Guía para la incorporación al derecho interno de la Ley Modelo de la CNUNDMI sobre Comercio Electrónico*. Página 15. Visto el 27 de noviembre de 2017 a través del vínculo https://www.uncitral.org/pdf/spanish/texts/electcom/05-89453_S_Ebook.pdf

flexibilización de los requisitos mínimos que favorecen la incorporación de un mensaje de datos electrónico, cuando así resultare aplicable según el examen propuesto. Verbigracia, sería insostenible presentar a examen de equivalencia una probanza digital, cuando el argumento medular sobre un juicio sea la autenticidad de una firma autógrafa[17]; casos en los que resultaría indispensable la presencia del soporte físico *sub judice*. Al respecto, el Poder Judicial de la Federación, brinda un precedente aislado para el entendimiento de esta última aseveración:

> **DOCUMENTO ELECTRÓNICO. SI CUENTA CON CADENA ORIGINAL, SELLO O FIRMA DIGITAL QUE GENERE CONVICCIÓN EN CUANTO A SU AUTENTICIDAD, SU EFICACIA PROBATORIA ES PLENA.**
> De conformidad con el artículo 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo, la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología, constituye un medio de prueba que debe valorarse conforme a las reglas específicas contenidas en el propio precepto y no con base en las reglas generales aplicables a las copias simples de documentos públicos o privados impresos. Así, para establecer la fuerza probatoria de aquella información, conocida como documento electrónico, debe atenderse a la fiabilidad del método en que se generó, comunicó, recibió o archivó y, en su caso, si es posible atribuir su contenido a las personas obligadas e, igualmente, si es accesible para su ulterior consulta. En congruencia con ello, si el documento electrónico, por ejemplo, una factura, cuenta con cadena original, sello o firma digital que genere convicción en cuanto a su autenticidad, su eficacia probatoria es plena y, por ende, queda a cargo de quien lo objete aportar las pruebas necesarias o agotar los medios pertinentes para desvirtuarla.[18]

[17] Un ejemplo normativo de esta postura lo encontramos en el artículo 326, apartados 2 y 3 de la Legislación Consolidada de Enjuiciamiento Civil *Ley 1/2000, de 7 de enero* (España). Dichos apartados prescriben: "***Artículo 326. Fuerza probatoria de los documentos privados: … 2. Cuando se impugnare la autenticidad de un documento privado, el que lo haya presentado podrá pedir el cotejo pericial de letras o proponer cualquier otro medio de prueba que resulte útil y pertinente al efecto.*** *…3. Cuando la parte a quien interese la eficacia de un documento electrónico lo pida o se impugne su autenticidad, se procederá con arreglo a lo establecido en el artículo 3 de la Ley de Firma Electrónica.*" Por su lado, la *Ley 59/2003, de 19 de diciembre, de Firma Electrónica*, en la parte conducente dicta: "(…) **Artículo 3. Firma electrónica, y documentos firmados electrónicamente**…Si se impugna la autenticidad de la firma electrónica avanzada, con la que se hayan firmado los datos incorporados al documento electrónico, se estará a lo establecido en el apartado 2 del artículo 326 de la Ley de Enjuiciamiento Civil…9. No se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica." Visto el 04 de diciembre de 2017 a través del portal https://www.boe.es

[18] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. *Documento electrónico. Si cuenta con cadena original, sello o firma digital que genere convicción en cuanto a su autenticidad, su eficacia*

Por lo que refiere al panorama internacional y en afán de brindar una apreciación global de las características del documento electrónico, resultan aplicables los artículos 8° y 9° de la Ley Modelo UNCITRAL. Por ahora, únicamente estudiaremos el primero de ellos, ya que el segundo nos servirá de fundamento para fortalecer el parágrafo respectivo. El numeral octavo de referencia, prescribe:

> Artículo 8 Ley Modelo UNCITRAL. — Original 1) Cuando la ley requiera que la información sea presentada y conservada en su forma original, ese requisito quedará satisfecho con un mensaje de datos: a) Si existe alguna garantía fidedigna de que se ha conservado la integridad de la información a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos o en alguna otra forma; b) De requerirse que la información sea presentada, si dicha información puede ser mostrada a la persona a la que se deba presentar. 2) El párrafo 1) será aplicable tanto si el requisito en él previsto está expresado en forma de obligación como si la ley simplemente prevé consecuencias en el caso de que la información no sea presentada o conservada en su forma original. 3) Para los fines del inciso a) del párrafo 1): a) La integridad de la información será evaluada conforme al criterio de que haya permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de su comunicación, archivo o presentación; y 7 b) El grado de fiabilidad requerido será determinado a la luz de los fines para los que se generó la información y de todas las circunstancias del caso [...].

Conforme a los criterios que se reprodujeron, en consonancia con los preceptos invocados, parece claro que un documento electrónico y digital podría aspirar el valor probatorio pleno dentro de un proceso, siempre que cumpla con los **principios de equivalencia fnncioual, no discriminacióu y neutralidad** y no exista duda razonable sobre el cumplimiento en los estándares de **fiabilidad**, **integridad** y **auteuticidad** (en continente o contenido), sin importar si la duda surge en la psique del juzgador o en las intenciones del contrario. A esto, valdría sumar el estándar de **durabilidad** que cité con anterioridad.

---

probatoria es plena. Tribunales Colegiados de Circuito. Tesis XXI.1o.P.A.11 K (10a.)Décima Época. Semanario Judicial de la Federación y su Gaceta. Libro 47, Octubre de 2017, Tomo IV, Página 2434. Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/ el 02 de diciembre de 2017

Principio	Estándar (Parámetro de forma)	Se define como
Equivalencia Funcional: Son los criterios conforme a los cuales las comunicaciones electrónicas pueden equipararse a las comunicaciones sobre papel. Enuncia los requisitos concretos que deben cumplir las comunicaciones electrónicas para realizar los mismos fines y desempeñar las mismas funciones que se persiguen en el sistema tradicional basado en el papel.	Originalidad/ Fiabilidad	Proporcionar un documento legible para todos; permitir la reproducción de un documento a fin que cada una de las partes disponga de un ejemplar. Se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje.
	Integridad	Proporcionar una forma aceptable para la presentación de un escrito ante las autoridades. La fiabilidad de la forma en la que se haya conservado la integridad de la información, hasta su incorporación al proceso
	Autenticidad	Permitir la autenticación de los datos consiguados suscribiéndolos con una firma. Se habrá de tener en cuenta la forma en la que se identifique al iniciador del mensaje de datos
	Durabilidad	Asegurar la inalterabilidad de un documento a lo largo del tiempo
No discriminación		No se denegarán a un documento sus efectos jurídicos, su validez o su ejecutabilidad por la única razón que figure en formato electrónico.
Neutralidad		Es la obligación de los Estados de adoptar disposiciones cuyo contenido sea neutral respecto de la tecnología empleada. Su objetivo es dar cabida a toda novedad que se produzca en el futuro sin necesidad de emprender una labor legislativa

XII. 4. 2 Caso Mexicano: Fiabilidad, Atribución, Accesibilidad e Integridad

Según lo precisé en el parágrafo anterior, es prudente realizar la distinción entre Principios y Estándares que rigen las pruebas electrónicas y digitales. Para el caso mexicano, el Código Federal de Procedimientos Civiles fija los estándares que el juez en turno debe considerar para dotar de fuerza probatoria la información que

conste en medios electrónicos, ópticos o en cualquier otra tecnología. Estas condiciones se desprenden del artículo 210-A, mismo que de tenor literal prescribe:

> [...] **Artículo 210-A.**- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología.
>
> Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente **la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada** y, en su caso, **si es posible atribuir a las personas obligadas el contenido de la información** relativa y **ser accesible** para su ulterior consulta. Cuando la ley requiera que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, **se ha mantenido íntegra e inalterada** a partir del momento en que se generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.

En ese tenor, parece que el cuerpo de legisladores que adicionaron este precepto el 29 de mayo del año 2000, fijaron el principio de Equivalencia Funcional, a través de la tropicalización de los estándares que antes reproduje, en forma de ***fiabilidad, atribución, accesibilidad e integridad;*** empero, es importante destacar que este precepto atiende a un estudio "primordial", por lo que en uso de la sana crítica del juzgador, éste podría exigir mayores estándares para la incorporación de las pruebas digitales o electrónicas, en afán de dotarle de la fuerza probatoria adecuada. A su vez, señala el protocolo que debe seguir el juez cuando éste analiza la información contenida en un documento digital, como lo podría ser un correo electrónico; en primer lugar, deberá calificar la fiabilidad del método en que se generó, comunicó, recibió y archivo; posteriormente, analizará la posibilidad para atribuir identidad del emisor y remitente, asimismo, atenderá la accesibilidad para su consulta; estándares que podrían dictar el valor probatorio, indiciario o privilegiado del medio de convicción que se estudié. Por último, el precepto ordena la presentación original (en forma digital) de los documentos que así lo exija la ley, siempre que se satisfaga el estándar de integridad; hipótesis que podría resolverse en forma de certificado digital, como en el caso de las facturas electrónicas que contienen sellos digitales.

Sobre el estudio del artículo 210- A y su aplicación a pruebas que se generen en medios electrónicos u ópticos, el Poder Judicial de la Federación se ha pronunciado al respecto de correos electrónicos oficiales, que al cumplir ciertas condiciones, deben gozar pleno valor probatorio; a saber:

CORREO ELECTRÓNICO OFICIAL. LA INFORMACIÓN COMUNICADA A TRAVÉS DE DICHO MEDIO ENTRE LOS ÓRGANOS DEL PODER JUDICIAL DE LA FEDERACIÓN, SI ESTÁ CERTIFICADA LA HORA Y FECHA

DE SU RECEPCIÓN, ASÍ COMO EL ÓRGANO QUE LA REMITE POR EL SECRETARIO DE ACUERDOS DEL TRIBUNAL JUDICIAL QUE LA RECIBE, TIENE PLENO VALOR PROBATORIO. El artículo 210-A del Código Federal de Procedimientos Civiles, de aplicación supletoria a la Ley de Amparo en términos de lo previsto en el diverso numeral 2o. de esa ley, reconoce como medios de prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología, y establece que su fuerza probatoria está sujeta a la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Ahora bien, entre los medios de comunicación electrónica a que se refiere la legislación procesal civil de referencia, se encuentra el denominado correo electrónico, que es un medio de transmisión de datos mediante redes infonnáticas (Internet), por el que es factible el envío de infonnación que se recibe por el destinatario en fonna de mensaje de texto o como dato adjunto; de ahí que la información generada o comunicada en mensajes de texto o archivos adjuntos que se transmite por medio del correo electróuico oficial, eutre los órganos del Poder Judicial de la Federaciou, si su recepción está certificada por el secretario de Acuerdos del tribunal judicial al que se transmite, sobre la hora y fecha en que la recibió y la persona del órgano jurisdiccional federal que la remitió, tiene pleno valor probatorio, por ser confiable el medio en que fue comunicada, ya que tiene un grado de seguridad similar al de la documentación consignada en papel, además de que es identificable la persona a quien se atribuye su contenido y pueden verificarse tanto el origen del mensaje como el archivo adjunto que a través de éste se remita; pues en la actualidad los citados órganos se encuentran comunicados electrónicamente, por distintos medios, lo que permite corroborar los datos del mensaje de texto o dato adjunto recibido.[19]

Precedente que sostiene el valor probatorio del documento digital, bajo el estándar de cumplimiento sobre los principios de **fiabilidad, atribución** y **accesibilidad**, sin embargo, refiere la presencia de certificación por un fedatario público (Secretario de Acuerdos), lo que supone la existencia de un medio de perfeccionamiento, que no se invocó en la construcción del famoso 210-A, empero, al entender del Magistrado en turno, podría implicar el mecanismo idóneo para no dudar sobre la prueba digital que se invoca ante su psique. En afán de fortalecer lo anterior, más adelante haré referencia a la exigencia de "terceros" que perfeccionan la prueba digital.

[19] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. *Correo Electrónico Oficial. La Información comunicada a través de dicho medio entre los órganos del poder judicial de la Federación, si está certificada la hora y fecha de su recepción, así como el órgano que la remite por el Secretario de Acuerdos del Tribunal que la recibe, tiene Pleno Valor Probatorio.* Tribunales Colegiados de Circuito. Tesis I.3o.P. J/3 (10a.). Décima Época. Semanario Judicial de la Federación y su Gaceta. Libro 54, Mayo de 2018, Tomo III, Página 2178 Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/ el 02 de septiembre de 2018.

En seguimiento al criterio que invoqué, del Semanario Judicial de la Federación, se desprende el precedente Aislado XXI.1o.P.A.11 K (10a.), en el que también defiende la eficacia probatoria plena de un documento electrónico como el caso de las facturas, siempre que éstas cumplan con el estándar de autenticidad mediante sello o firma digital; que si bien es cierto, no hace referencia a la integridad de las mismas que también se acredita con dicha cadena, sí brinda un precedente plausible para nuestro Poder Judicial. Criterio que antes invoqué, cuyo rubro dicta: **DOCUMENTO ELECTRÓNICO. SI CUENTA CON CADENA ORIGINAL, SELLO O FIRMA DIGITAL QUE GENERE CONVICCIÓN EN CUANTO A SU AUTENTICIDAD, SU EFICACIA PROBATORIA ES PLENA**[20].

XII. 5 Incorporación procesal de pruebas electrónicas y digitales

En términos de los argumentos expuestos, resulta inverosímil aceptar cualquier tipo de ofrecimiento y desahogo (incorporación) de una prueba electrónica y digital fuera de los principios y estándares sostenidos, sin embargo, la realidad procesal provoca que en muchas de las ocasiones, los Tribunales no se encuentren debidamente capacitados para comprender la naturaleza *sui géneris* de nuevos medios de convicción y, en muchos de los casos, los abogados litigantes no cuentan con la capacitación técnica para precisar el alcance de la prueba *tecnológica* y porqué ésta debería incorporarse al proceso sin atentar contra su naturaleza digital. Es decir, no resulta admisible que el Tribunal de la causa exija a las partes desahogar una prueba electrónica o digital, a través de mecanismos tradicionales que pudieren afectar los principios de **no discriminación, neutralidad y equivalencia funcional;** verbigracia, un Juez que solicita a la parte oferente de un documento electrónico, que imprima las constancias de un mensaje de datos emitido a través del servicio de mensaje corto (SMS) y, en su caso, perfeccionar dicho medio de convicción a través de certificación notarial, atenta contra la naturaleza tecnológica de dicha probanza, por lo que debería ser permisible exhibir el propio mensaje dentro del equipo telefónico destino, o bien, solicitar el apoyo de la compañía telefónica para obtener un registro confiable de la emisión y recepción de dichos datos; de tal suerte que el mensaje que se pretende incorporar a un proceso no pierda su naturaleza, ni se valore conforme a principios tradicionales que mermen el valor probatorio asequible. En tales términos, no se deben admitir requerimientos caprichosos en

[20] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. *Documento Electrónico. Si cuenta con cadena original, sello o firma digital que genere convicción en cuanto a su autenticidad, su eficacia probatoria es plena.* Tribunales Colegiados de Circuito. XXI.1o.P.A.11 K (10a.). Décima Época. Semanario Judicial de la Federación y su Gaceta. Libro 47, Octubre de 2017, Tomo IV, Página 2434. Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/ el 02 de septiembre de 2018

perjuicio de la naturaleza tecnológica de cierto tipo de pruebas, tal como lo sostienen las Naciones Unidas en su Ley Modelo UNCITRAL, cuyo artículo 9° dicta:

> [...] **Artículo 9. — Admisibilidad y fuerza probatoria de los mensajes de datos**
>
> 1) En todo trámite legal, **no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos**:
>
> a) Por la sola razón de que se trate de un mensaje de datos; o
> b) Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.
>
> 2) **Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria**. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente **la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente**.
> **(El énfasis es añadido).**

El precepto de referencia permite afirmar que nuestras Naciones Unidas ya se preparaban para la aceptación de las pruebas tecnológicamente avanzadas y, en su caso, invitan a los Tribunales a admitir las mismas y brindarles un peso probatorio adecuado a sus circunstancias. Tan sólo del artículo recientemente transcrito, se advierte que el juzgador deberá atender a: i) **Equivalencia funcional.**- Por lo que refiere a no obstaculizar su ofrecimiento y, en todo caso, por ser el mensaje de datos "la mejor" prueba sobre una de carácter tradicional; ii) **Originalidad/ Fiabilidad.**- Por lo que refiere a la capacidad para determinar que el mensaje de datos que se aporta al procedimiento no sufrió ningún cambio desde su emisión, durante su archivo y hasta el momento de su incorporación a un procedimiento; iii) **Integridad.**- Por lo que refiere a la fidelidad del contenido del mensaje de datos; conforme al principio anterior, ni continente o contenido deberán sufrir alteraciones para ser incorporados a un procedimiento; y iv) **Autenticidad.**- Por lo que refiere a la posibilidad de acreditar la identidad de su iniciador/emisor –algunas legislaciones pudieren exigir la presencia de una firma electrónica o digital, empero, no debe considerarse que el certificado autenticador es un requisito *sine qua non* para considerar por satisfecho el presente requisito-; características que deberán interpretarse armónicamente con el artículo 8° del propio ordenamiento. Dicho fundamento no sólo brinda un parámetro para-procesal a las partes para conocer el éxito que podría tener su prueba dentro de un proceso, sino que fijan las reglas de admisibilidad que deberán seguir los juzgadores, según sus legislaciones procesales respectivas. Algunos tratadistas sobre la

materia incluyen el principio de "confidencialidad", así como el principio tradicional de **obtención lícita de la prueba** que invoca la Cuarta Enmienda de los Estados Unidos de América, el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos o bien, el artículo 29 de la Constitución Nacional de Panamá, según se explicará más adelante.

El caso mexicano es un paradigma ortodoxo en materia de incorporación de pruebas electrónicas y digitales. En el caso del contenido de las páginas web (o electrónicas), los Tribunales Colegiados de Circuito que dependen de nuestro Poder Judicial de la Federación, estiman que éste se debe incorporar a un proceso como "hecho notorio" y no como **documento digital**, que sería la calificación jurídica adecuada, según se expuso con anterioridad. A saber, el precedente jurisdiccional dicta:

> **PÁGINAS WEB O ELECTRÓNICAS. SU CONTENIDO ES UN HECHO NOTORIO Y SUSCEPTIBLE DE SER VALORADO EN UNA DECISIÓN JUDICIAL.**
> Los datos publicados en documentos o páginas situados en redes informáticas constituyen un hecho notorio por formar parte del conocimiento público a través de tales medios al momento en que se dicta una resolución judicial, de conformidad con el artículo 88 del Código Federal de Procedimientos Civiles. El acceso al uso de Internet para buscar información sobre la existencia de personas morales, establecimientos mercantiles, domicilios y en general cualquier dato publicado en redes informáticas, forma parte de la cultura normal de sectores específicos de la sociedad dependiendo del tipo de información de que se trate. De ahí que, si bien no es posible afirmar que esa información se encuentra al alcance de todos los sectores de la sociedad, lo cierto es que sí es posible determinar si por el tipo de datos un hecho forma parte de la cultura normal de un sector de la sociedad y pueda ser considerado como notorio por el juzgador y, consecuentemente, valorado en una decisión judicial, por tratarse de un dato u opinión común indiscutible, no por el número de personas que conocen ese hecho, sino por la notoriedad, accesibilidad, aceptación e imparcialidad de este conocimiento. Por tanto, el contenido de una **página** de Internet que refleja hechos propios de una de las partes en cualquier juicio, puede ser tomado como prueba plena, a menos que haya una en contrario que no fue creada por orden del interesado, ya que se le reputará autor y podrá perjudicarle lo que ofrezca en sus términos.[21]

[21] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. *Páginas Web o electrónicas. Su contenido es un hecho notorio y susceptible de ser valorado en una decisión judicial.* Tribunales Colegiados de Circuito. Tesis I.3°.C.35K. Décima Época. Semanario Judicial de la Federación y su Gaceta. Libro 26, Noviembre de 2013, Tomo II, Página 1373 Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/ el 02 de diciembre de 2017.

Algunos lectores podrían afirmar que el criterio que invocó no resulta perjudicial para el entendimiento y comprensión del valor probatorio de un documento digital como lo son las páginas web, sin embargo, la pobre incorporación que se propone pondría provocar la desaparición de la página antes de su valoración, así como su contenido. Sin embargo, parece ser que la décima época que vive nuestra Suprema Corte de Justicia, brinda luces esperanzadoras para el ofrecimiento, admisión y desahogo de pruebas electrónicas, a pesar de las limitantes que contiene el propio criterio, mismo que de tenor literal dicta:

PRUEBAS EN EL INCIDENTE DE SUSPENSIÓN DERIVADO DEL JUICIO DE AMPARO INDIRECTO. NATURALEZA Y CARACTERÍSTICAS DE LOS VIDEOS CONTENIDOS EN MEDIOS ELECTRÓNICOS PARA QUE PUEDAN PRODUCIR CONVICCIÓN PLENA.

La prueba es el instrumento con el que cuenta el Juez para verificar o confirmar las afirmaciones de los hechos expresados por las partes, cuyo esclarecimiento es necesario para la resolución del conflicto sometido a proceso. Así, cuando el instrumento probatorio consiste en una cosa, se le clasifica como una prueba real. En ese sentido, si la cosa es de naturaleza mueble, se trata de una prueba de documentos, y basta con que sea presentada al juzgador para que quede desahogada. En cambio, si es un inmueble y se requiere que el Juez o fedatario judicial se desplace hasta donde éste se sitúa, se habla de una prueba de reconocimiento judicial o inspección ocular (monumental). Por otra parte, el procedimiento del incidente de suspensión derivado del juicio de amparo indirecto es muy breve, pues debe resolverse por el órgano jurisdiccional con un trámite sencillo, sujeto a un plazo mínimo, al establecerse que una vez promovida la medida, debe celebrarse la audiencia incidental dentro de los cinco días siguientes; de ahí que la naturaleza sumaria de dicha vía no permite el desahogo de pruebas que puedan entorpecer u obstaculizar la resolución correspondiente, por el hecho de que requieran un trámite especial para ello, lo cual implica que, por regla general, las pruebas que pueden admitirse son las documentales y las monumentales. Es por esto que, en esta vía, las partes se enfrentan a una limitación al derecho de probar, pues sólo son admitidas las pruebas que pueden, por su naturaleza real, desahogarse en el momento en que se presentan al órgano jurisdiccional. En ese contexto, resulta imprescindible atender al avance actual de los conocimientos científicos y tecnológicos, pues los datos, imágenes, palabras o signos ya no constan solamente en documentos en papel, sino que pueden fácilmente contenerse en aparatos electrónicos; es por ello que, dada la facilidad que proporcionan para acudir a su contenido, estos medios se equiparan en su desahogo a un documento, ya que ilustran sobre los hechos captados mediante imágenes con o sin sonido y, en consecuencia, pueden ser llevados ante un Juez para formar en él una convicción sobre determinados hechos. **Para su presentación requieren de un equipo en el que pueda reproducirse la imagen y, en su caso, los sonidos que contenga; por lo que al igual que la prueba documental, una vez reproducido queda**

desahogado, en virtud de que no se requiere de una diligencia especial para ello, lo cual implica que su admisión no retrasaría la resolución del incidente. Por tanto, como prueba real, el video contenido en medios electrónicos es útil para coustituir un indicio, a fin de esclarecer los hechos uecesarios para resolver el conflicto; sin embargo, **si no es corroborado, como podría ser con la fe pública o con otros elementos de prueba, de que su contenido corresponde a hechos ocurridos en un lugar y tiempo determinados, no podría producir convicción plena**. En todo caso, el valor probatorio que debe otorgarse al contenido del video quedaría al prudente arbitrio judicial, en términos del artículo 217 del Código Federal de Procedimientos Civiles.[22]

(Énfasis añadido)

En materia Administrativa, el puesto jurisdiccional le corresponde al Tribunal Federal de Justicia Administrativa –otrora Fiscal y Administrativa-. Sobre el particular, la Sala Regional Especializada en materia de Propiedad Intelectual y la Décima Sala Regional Metropolitana, emitieron un precedentes aislados que podrían acreditar la posibilidad de incorporar el contenido de una página web al proceso, sin embargo, no es puntual sobre los mecanismos para su conservación forense, mucho menos para su incorporación. Máxime que sólo apuntan a brindar valor probatorio indiciario al contenido de una página web. A saber:

VALORACIÓN DE LA INFORMACIÓN CONTENIDA EN PORTALES DE LA RED MUNDIAL DE TERMINALES ENLAZADAS ENTRE SÍ (INTERNET).-De conformidad con los artículos 46, segundo párrafo de la Ley Federal de Procedimiento Contencioso Administrativo y 210-A del Código Federal de Procedimientos Civiles de aplicación supletoria a la materia, en relación con el 217 del último ordenamiento, se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecuología, por lo que la información contenida en las páginas de Internet, al ser aportaciones por los descubrimientos de la ciencia tienen un valor relativo que queda al prudente arbitrio del Juzgador. Cuando la información que plasme el Instituto Mexicano de la Propiedad Industrial en la resolución impugnada y la que tenga el Órgano Colegiado a la vista al momento de dictar el fallo correspondiente, se ha mantenido íntegra e inalterada a partir del momento en que se consulta por la autoridad administrativa, el valor otorgado a la información contenida en las páginas web que se encuentren en inglés es suficiente para motivar la negativa de un registro solicitado cuando el signo haya sido propuesto en

[22] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. *Pruebas en el incidente de suspensión derivado del juicio de amparo Indirecto. Naturaleza y Características de los videos contenidos en medios electrónicos para que puedan producir convicción plena.* Tribunales Colegiados de Circuito. Tesis I.8o.A.16 K (10a.)Décima Época. Semanario Judicial de la Federación y su Gaceta. Libro 47, Octubre 2017, Tomo IV. Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/ el 03 de diciembre de 2017.

ese idioma, al estar también dirigido tanto al público consumidor promedio de habla hispana como inglesa.[23]

PÁGINAS WEB. SU VALOR PROBATORIO.- Si bien es cierto que conforme al artículo 217 del Código Federal de Procedimientos Civiles de aplicación supletoria, las copias simples tienen un valor relativo que queda al prudente arbitrio del juzgador, también lo es que éste debe valorarlas en forma conjunta con otros elementos de prueba ofrecidos, por lo tanto, el sólo hecho de que se exhiban en copias sin certificar las páginas web, no les resta eficacia probatoria, toda vez que se debe tomar en consideración si las mismas se encuentran o no relacionadas o adminiculadas con otros elementos de prueba tendientes a demostrar la pretensión del oferente, resultando ilegal negarles en forma absoluta valor probatorio solamente por carecer de certificación, sino que deben tomarse como indicios atendiendo a los hechos que con ellas se pretende acreditar y a los demás elementos probatorios que obran en el expediente.[24]

XII. 5. 1 Perfeccionamiento, Perito Informático y Fedatario Informático

Los criterios expuestos ilustran dos elementos polares de mi exposición: i) El duro golpe a los principios de **neutralidad y discriminación** que implica el criterio de los jueces en turno. Tal como manifesté con anterioridad, en términos de la legislación internacional aplicable, no es admisible que el Tribunal de la causa exija mayores requisitos de ofrecimiento y desahogo sobre aquéllos que pudiere instar de un medio de convicción tradicional, máxime cuando dicho requerimiento pudiere atentar contra la naturaleza de la prueba e impedir analizar su "autenticidad y originalidad" en el proceso, no obstante que el uso de la fe pública se ocupe como medio de perfeccionamiento inadecuado para la causa; y ii) Existe un lado plausible, pues el vínculo existente entre *continente* y *contenido* permite al oferente y al juzgador, tener por desahogado un medio de prueba electrónico o digital, en el mismo dispositivo que generó, archivó o distribuyó el mensaje de datos, lo que brindaría un reconocido beneficio al principio de economía procesal e inmediación procesal. En ese sentido se

[23] TRIBUNAL FEDERAL DE JUSTICIA FISCAL Y ADMINISTRATIVA. *Valoración de la información contenida en portales de la red mundial de terminales enlazadas entre sí (Internet).* Sala Regional Especializada en materia de Propiedad Intelectual. México, 22 de septiembre de 2009. Tesis aislada. R.T.F.J.F.A. Sexta Época. Año III. No. 27. Marzo 2010. p. 405. Visto el 19 de agosto de 2018 a través del vínculo http://sctj.tfjfa.gob.mx/SCJI/assembly/detalleTesis?idTesis=36003

[24] TRIBUNAL FEDERAL DE JUSTICIA FISCAL Y ADMINISTRATIVA. *Páginas Web. Su valor probatorio.* Décima Sala Regional Metropolitana. México, 31 de octubre de 2003. Tesis aislada. R.T.F. J.F.A. Quinta Época. Año IV. No. 47. Noviembre 2004. p. 460. Visto el 19 de agosto de 2018 a través del vínculo http://sctj.tfjfa.gob.mx/SCJI/assembly/detalleTesis?idTesis=30648

pronunciaría un Tribunal Colegiado de Circuito en Materia Civil, del Poder Judicial de la Federación (México), tomando en consideración el peso normativo de la Ley Modelo UNCITRAL:

> **DOCUMENTOS Y CORREOS ELECTRÓNICOS. SU VALORACIÓN EN MATERIA MERCANTIL.** La doctrina explica que en la época contemporánea cuando se habla de prueba documental no se puede pensar sólo en papel u otro soporte que refleje escritos perceptibles a simple vista, sin ayuda de medios técnicos; se debe incluir también a los documentos multimedia, es decir, los soportes que permiten ver estos documentos en una computadora, un teléfono móvil, una cámara fotográfica, etcétera. En varios sistemas jurídicos se han equiparado totalmente los documentos multimedia o informáticos, a efectos de valoración. Esa equivalencia es, básicamente, con los privados, y su admisión y valoración se sujeta a requisitos, sobre todo técnicos, como la firma electrónica, debido a los problemas de fiabilidad de tales documentos, incluyendo los correos electrónicos, ya que es posible falsificarlos e interceptarlos, lo cual exige cautela en su ponderación, pero sin desestimarlos sólo por esa factibilidad. **Para evitar una pericial en informática que demuestre la fiabilidad del documento electrónico, pero complique su ágil recepción procesal, el juzgador puede consultar los datos técnicos reveladores de alguna modificación señalados en el documento**, aunque de no existir éstos, atenderá a la posibilidad de alteración y acudirá a la experticia, pues el documento electrónico puede quedar en la memoria RAM o en el disco duro, y podrán expedirse copias, por lo que para comprobar el original deberán exhibirse documentos asistidos de peritos para su lectura. Así es, dado que la impresión de un documento electrónico sólo es una copia de su original. Mayor confiabilidad merece el documento que tiene firma electrónica, aunque entre esa clase de firmas existe una gradación de la más sencilla a la que posee mayores garantías técnicas, e igual escala sigue su fiabilidad, ergo, su valor probatorio. Así, la firma electrónica avanzada prevalece frente a la firma electrónica simple, ya que los requisitos de producción de la primera la dotan de más seguridad que la segunda, y derivan de la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional sobre las Firmas Electrónicas. Esta propuesta de normatividad, al igual que la diversa Ley Modelo sobre Comercio Electrónico, fue adoptada en el Código de Comercio, el cual sigue el criterio de equivalencia funcional que busca equiparar los documentos electrónicos a los tradicionales elaborados en soporte de papel, mediante la satisfacción de requisitos que giran en torno a la fiabilidad y trascienden a la fuerza probatoria de los mensajes de datos. Por ende, conforme a la interpretación de los artículos 89 a 94, 97 y 1298-A del Código de Comercio, en caso de que los documentos electrónicos reúnan los requisitos de fiabilidad legalmente previstos, incluyendo la existencia de una firma electrónica avanzada, podrá aplicarse el criterio de equivalente funcional con los documentos que tienen soporte de papel, de manera que su valor probatorio será equivalente al de estos últimos. **En caso de carecer de esa firma y haberse objetado su**

> **autenticidad, no podrá concedérseles dicho valor similar, aunque su estimación como prueba irá en aumento si en el contenido de los documentos electrónicos se encuentran elementos técnicos bastantes, a juicio del juzgador, para estimar altamente probable su autenticidad e inalterabilidad, o bien se complementan con otras probanzas, como la pericial en informática que evidencie tal fiabilidad. Por el contrario, decrecerá su valor probatorio a la calidad indiciaria si se trata de una impresión en papel del documento electrónico, que como copia del original recibirá el tratamiento procesal de esa clase de documentos simples, y se valorará en conjunto con las restantes pruebas aportadas al juicio para, en función de las circunstancias específicas, determinar su alcance demostrativo**.[25]
>
> **(El énfasis en negritas y subrayado es añadido).**

A pesar que este último precedente no tiene poder vinculante para el resto de las autoridades juzgadoras en México, brinda un camino jurídico adecuado y más sólido conforme a los principios y criterios que sostienen las Naciones Unidas. En primer lugar, recuerda al juzgador la posibilidad de valorar por sí mismo las pruebas tecnológicas, siempre que no estime necesario llamar a un perito a su procedimiento, adicionalmente, lo invita a provocar el desahogo de un mensaje de datos a través de un soporte electrónico o digital, sin necesidad de mayor diligencia para ello. Sólo en caso que el mensaje o el soporte resulten dubitables, el propio juez tendrá facultades para invocar a un experto en la materia o solicitar que se ofrezcan otro tipo de medios de convicción para perfeccionar el ofrecido, empero, un documento electrónico con firma electrónica en él, pudiere alcanzar valor probatorio pleno si es que no existen elementos para creer que éste se emitió en contravención a los principios de la prueba tecnológicamente avanzada.

En ese tenor ha reaccionado el gobierno peruano, a través del Decreto Legislativo número 681 *Uso de tecnologías avanzadas en materia de Archivo*[26], cuyo fin es regular el uso de las "TIC's" en materia de archivos de documentos e información que se produce a través de mecanismos informáticos; en lo particular, faculta la participación de un **fedatario informático** que auxiliaría en la creación de *microformas* de documentos análogos (*strictu sensu)* y reconoce la validez de los *microarchivos* para acreditar el contenido de los documentos, aún ante la destrucción del soporte "original". Normatividad que, procesalmente, reconoce la fuerza probatoria de los

[25] Semanario Judicial de la Federación. CUARTO TRIBUNAL COLEGIADO EN MATERIA CIVIL DEL PRIMER CIRCUITO. 2002142. I.4o.C.19 C (10a.). Tribunales Colegiados de Circuito. Décima Época. Semanario Judicial de la Federación y su Gaceta. Libro XIV, Noviembre de 2012, Pág. 1856.

[26] ARCHIVO GENERAL DE LA NACIÓN. *Uso de tecnologías avanzadas en materia de archivo. Decreto Legislativo 681.* 11 de octubre de 1991, Perú. Visto a través del vínculo http://webapp.regionsanmartin.gob.pe/sisarch/LEGISLACION/6.%20TECNOLOGIA%20AVANZADA%20EN%20ARCHIVOS/DL_No_681.pdf Este Decreto fue reformado por Decreto Supremo el 6 de octubre de 2016, sin embargo, sostiene el vigor de las figuras jurídicas invocadas.

documentos electrónicos y prevé mecanismos particulares de su perfeccionamiento antes de su incorporación al juicio, en afán de omitir requerimientos ociosos o desnaturalizantes durante el desahogo de aquéllos.

Sin embargo, también existen legislaciones que además de los estándares de incorporación procesal, exigen la presencia de peritos especializados para permitir la comprensión del contenido de la prueba digital en el proceso. Verbigracia, en el caso de la normatividad española, la Ley de Enjuiciamiento Civil[27] rescata los estándares de integridad y autenticidad, además del principio de licitud en la obtención de la prueba; empero, añaden la calificación pericial de un técnico informático para **aclarar** –obligatoriamente- el contenido de la prueba digital a favor de las partes y el juzgador; en términos del artículo 346 de la Ley de Enjuiciamiento Civil. No obstante lo anterior, el diverso 326, inciso 3 de la propia Ley, recuerda que la eficacia de un documento electrónico dependerá de la integridad con la que se presenten, al tenor del artículo tercero de la Ley de Firma Electrónica (documentos privados firmados electrónicamente)[28]. Consideraciones que podrían permitir aducir a la fortaleza de los documentos electrónicos en el proceso, aún sin la presencia de un experto informático, en tanto se acredite la autenticación de los mismos.

Sobre el particular y la autenticación de documentos que incluyen firma electrónica, el artículo 342 apartado 6° del Código de Procedimientos de Chile, prescribe que se considerará como instrumento público en juicio a los documentos electrónicos suscritos mediante firma electrónica avanzada; precepto que se debe leer armónicamente con los artículos 4° y 5° de la Ley 19,799 *Sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.* En ese tenor, la jurisdicción chilena permite la impugnación y ofrecimiento de prueba complementaria de autenticidad, como una carga procesal adicional al impugnante, no como un estándar de admisibilidad de la prueba, tal como ocurre en el caso español; lo que a mi humilde parecer es la ruta procesal adecuada para desvirtuar el alcance o valor probatorio de una prueba electrónica o digital, que se emitió con los requisitos que exige la ley[29].

[27] JEFATURA DEL ESTADO, MINISTERIO DE LA PRESENCIA, RELACIONES CON LAS CORTES E IGUALDAD, GOBIERNO DE ESPAÑA. *Ley 1/2000*. 7 de enero, de Enjuiciamiento Civil. BOE número 7, de 8 de enero de 2000. Visto a través del Boletín Oficial del Estado en https://boe.es/buscar/act.php?id=BOE-A-2000-323

[28] JEFATURA DEL ESTADO, MINISTERIO DE LA PRESENCIA, RELACIONES CON LAS CORTES E IGUALDAD, GOBIERNO DE ESPAÑA. *Ley 59/ 2003*. 19 de diciembre, de firma electronica. BOE número 304, de 20 de diciembre de 2003, páginas 45329 a 45343. Visto a través del Boletín Oficial del Estado en https://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399

[29] MINISTERIO DE ECONOMÍA,. *Norma Ley 20217. Modifica el código de Procedimiento Civil y la Ley número 197999 sobre documento electrónico, firma electrónica y los servicios de certificación de dichas firmas.* 12 de noviembre de 2007, Chile. Visto a través de la Biblioteca del Congreso Nacional de Chile en https://www.leychile.cl/Navegar?idNorma=266348

El rumbo colombiano resulta un ejemplo de progreso legislativo y judicial, en términos de su Ley 527 de 1999, también conocida como Ley de Comercio Electrónico. En lo particular, sus artículos 10 y 11 brindan la posibilidad de otorgar valor probatorio a un mensaje de datos que se incorpore a un procedimiento, siempre que cumpla con las reglas de la sana crítica y los siguientes aspectos:

> ARTICULO 10. ADMISIBILIDAD Y FUERZA PROBATORIA DE LOS MENSAJES DE DATOS. Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil. En toda actuación administrativa o judicial, no se negará eficacia, validez o fuerza obligatoria y probatoria a todo tipo de información en forma de un mensaje de datos, por el sólo hecho que se trate de un mensaje de datos o en razón de no haber sido presentado en su forma original.
>
> ARTICULO 11. CRITERIO PARA VALORAR PROBATORIAMENTE UN MENSAJE DE DATOS. Para la valoración de la fuerza probatoria de los mensajes de datos a que se refiere esta ley, se tendrán en cuenta las reglas de la sana crítica y demás criterios reconocidos legalmente para la apreciación de las pruebas. **Por consiguiente habrán de tenerse en cuenta: la confiabilidad en la forma en la que se haya generado, archivado o comunicado el mensaje, la confiabilidad en la forma en que se haya conservado la integridad de la información, la forma en la que se identifique a su iniciador y cualquier otro factor pertinente.** [30]
>
> (El énfasis es añadido)

A su vez, los diversos 8° y 9° del propio ordenamiento fijan las reglas para el ofrecimiento y desahogo de un "mensaje de datos"; en lo esencial, obliga al juzgador a aceptar este medio de probanza siempre que i) Exista garantía confiable que se ha conservado la integridad de la información. La ley indica que la información se mantiene integra, siempre que esta haya permanecido completa e inalterada; y ii) Que el mensaje de datos y la información pueda mostrarse a la persona que se deba presentar (juez). Tal como se expuso en el capítulo respectivo de la presente obra, esta Ley reproduce la conducta normativa que exige la Ley Modelo UNCITRAL.

De forma similar, parece ser que el Cuerpo de Administradores Gubernamentales de Buenos Aires, Argentina, ha encontrado la guía jurídica para entender la evidencia digital.[31] La Ley número 25.506 de Firma Digital establece la validez legal del

[30] CONGRESO DE COLOMBIA. *Ley 527 de 1999*. República de Colombia. Publicada el 18 de agosto de 1999. Puede consultar el texto íntegro a través del vínculo http://www.cancilleria.gov.co/sites/default/files/tramites_servicios/apostilla_legalizacion/archivos/ley_527_1999.pdf

[31] RIVOLTA, Mercedes. *Construyendo el Estado Nació para el crecimiento y la Equidad. Panel: Gobierno Electrónico: Experiencias en el poder legislativo y judicial*. Cuarto congreso argentino de

documento electrónico, de la firma electrónica y de la firma digital, cuyos preceptos 6, 11 y 12 dictan:

Firma Digital. Ley 25.506

[…] **ARTÍCULO 6°** — Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

ARTICULO 11. — Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

ARTICULO 12. — Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permitan determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/o recepción […][32]

En seguimiento al caso Argentino, el artículo 131 del Código Procesal Penal de la provincia de Chubut, autoriza el uso de imágenes y sonidos o grabaciones digitalizadas para documentar total o parcialmente actos de prueba o audiencias; prohíbe toda forma de edición, tratamiento o modificación de los registros y requiere que se asegure su autenticidad e inalterabilidad.

XII. 5. 2 Conservación de Mensajes de Datos y Digitalización de Documentos

Tal como expuse con anterioridad, el gobierno peruano cuenta con el Decreto Legislativo número 681 *Uso de tecnologías avanzadas en materia de Archivo*; a través del cual se involucra al Estado en la digitalización y certificación de documentos digitales; de forma similar, el caso mexicano goza de la Norma Oficial Mexicana

administración pública. Buenos Aires, Argentina. 22-25 de agosto de 2007. Disponible a través del vínculo http://www.congresoap.gov.ar/sitio/objetivos.html

[32] CÁMARA DE DIPUTADOS DE LA NACIÓN DE ARGENTINA. *Firma Digital. Ley 25.506.* Promulgada el 11 de diciembre de 2001. Argentina. Visible el 04 de diciembre de 2017 a través del vínculo http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

NOM-151-SCFI-2016 *Requisitos que deben observarse para la conservación de mensajes de datos y digitalización,* misma que se publicó el 30 de marzo de 2017 en el Diario Oficial de la Federación[33]. Dicha norma cancela la anterior de 2002, a través de la cual se pretende armonizar correctamente el Código de Comercio mexicano, al uso de mensajes de datos en materia de Comercio Electrónico, según lo dispone la Ley Modelo CNUDMI. Sobre el particular, fija los requisitos que se deben observar para la conservación de mensajes de datos y la digitalización de documentos "originales" en términos de los artículos 33, 38 y 49 del Código de Comercio; destacando lo siguiente:

- **Tercero Certificador Autorizado.**- Así como lo dispone el Decreto peruano que referí, la NOM prescribe que el proceso de digitalización deberá ser controlado por un tercero legalmente autorizado, que constatará que la migración (material a digital) se realice íntegra e inalterablemente tal y como se generó por primera vez en su forma definitiva. El tercero legalmente autorizado deberá ser un Prestador de Servicios de Certificación acreditado para tales efectos.
- **Proceso de Digitalización.**- Consecuente al Decreto peruano, el proceso de digitalización de documentos requiere la presencia del Prestador de Servicios de Certificación, quien cotejará que el mensaje de datos permite asegurar la fidelidad e integridad conforme a los documentos amparados en soportes físicos. En todo caso, el mensaje de datos generado debe ser de alta calidad y debe tratarse con un intenso control de calidad.

XII. 5. 3 Obtención lícita y recolección en cadena de custodia

La Teoría de los "frutos del árbol envenenado", es conocida como la regla procesal en la que un Tribunal –de cualquier fuero, competencia y materia- está impedido para incorporar a la *litis* cualquier medio de convicción que fuere obtenido de manera ilícita, ya que el origen viciado del mismo podría provocar su nulidad y una indebida apreciación de la verdad jurídica. Esta doctrina tiene su origen en el Derecho anglosajón, específicamente en el caso *Silverthorne Lumber Company Inc V. USA* y la sentencia que dictó la Suprema Corte de los Estados Unidos en enero de 1920.[34] En el juicio criminal

[33] SECRETARÍA DE ECONOMÍA. *Norma Oficial Mexicana NOM-151-SCFI-2016 Requisitos que deben observarse para la conservación de mensajes de datos y digitalización.* México, 30 de marzo de 2017. Diario Oficial de la Federación. Visible el 19 de agosto de 2018 a través del vínculo http://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017

[34] Un extracto de la sentencia prescribe que la Cuarta Enmienda de los Estados Unidos protege a las empresas y sus oficinas de allanamientos no autorizados o compulsas en sus libros contables y papeles para el uso de los mismos en procedimientos criminales, cuando los últimos fueron obtenidos de forma ilegal. A saber: "…The Fourth Amendment protects a corporation and its officers from compulsory

de referencia, agentes del gobierno allanaron ilegalmente las oficinas de los imputados y se pretendió sustentar su culpabilidad en libros contables descubiertos durante dicha diligencia. En este caso, la Corte máxima declaró que los imputados sufrieron violaciones en su esfera, debido a un irregular comportamiento de la autoridad investigadora en términos de la Cuarta Enmienda de la Constitución de los Estados Unidos de América. Esta enmienda contiene el derecho de privacidad e intimidad y garantiza protección en las personas en sus casas, papeles y efectos, contra investigaciones no razonables, salvo que exista una causa probable; a su vez, las Cortes americanas han extendido la esfera de protección a escuela, lugar de trabajo y vehículo.[35] En el caso mexicano, la Constitución Política de los Estados Unidos Mexicanos prescribe una garantía similar en el primer párrafo del artículo 16, adicionalmente, protege las comunicaciones privadas en los párrafos trece, catorce, dieciséis y dieciocho (vigentes):

> Artículo 16. **Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones, sino en virtud de mandamiento escrito de la autoridad competente, que funde y motive la causa legal del procedimiento**. En los juicios y procedimientos seguidos en forma de juicio en los que se establezca como regla la oralidad, bastará con que quede constancia de ellos en cualquier medio que dé certeza de su contenido y del cumplimiento de lo previsto en este párrafo…
>
> 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**. 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. Exclusivamente la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, podrá autorizar la intervención de cualquier comunicación privada. Para ello, la autoridad competente deberá fundar y motivar las causas legales de la solicitud,

production of the corporate books and papers for use in a criminal proceeding against them when the information upon which the subpoenas were framed was derived by the Government through a previous unconstitutional search and seizure, planned and executed by its officials under color of a void writ, provided the defense of the Amendment be seasonably interposed, and not first raised as a collateral issue at the trial of the indictment…The rights of a corporation against unlawful search and seizure are to be protected even if it be not protected by the Fifth Amendment from compulsory production of incriminating document… The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court, but that it shall not be used at all." JUSTIA. *Silverthorne Lumber Co., Inc. v. United States, 251 U.S. 385 (1920).* Visible el 02 de diciembre de 2017 a través del vínculo https://supreme.justia.com/cases/federal/us/251/385/case.html

[35] US COURTS/ http://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0

expresando además, el tipo de intervención, los sujetos de la misma y su duración. La autoridad judicial federal no podrá otorgar estas autorizaciones cuando se trate de materias de carácter electoral, fiscal, mercantil, civil, laboral o administrativo, ni en el caso de las comunicaciones del detenido con su defensor…

Las intervenciones autorizadas se ajustarán a los requisitos y límites previstos en las leyes. Los resultados de las intervenciones que no cumplan con éstos, carecerán de todo valor probatorio…

La correspondencia que bajo cubierta circule por las estafetas estará libre de todo registro, y su violación será penada por la ley […]

(El énfasis es añadido)

Para fines ilustrativos, invocaré el contenido del artículo 29 de la Constitución Nacional de Panamá, que de forma similar protege el derecho a la intimidad, sobre todo en materia de comunicaciones y prevé las consecuencias de una indebida obtención de pruebas:

(…) ARTICULO 29. La correspondencia y demás documentos privados son inviolables y no pueden ser examinados ni retenidos, sino por mandato de autoridad competente y para fines específicos, de acuerdo con las formalidades legales… Todas las comunicaciones privadas son inviolables y no podrán ser interceptadas o grabadas, sino por mandato de autoridad judicial. **El incumplimiento de esta disposición impedirá la utilización de sus resultados como pruebas, sin perjuicio de las responsabilidades penales en que incurran los autores. (El énfasis es añadido)**

Tal como se advierte de la Constitución Política de los Estados Unidos Mexicanos, del artículo 29 de la Constitución Nacional de Panamá y de la Cuarta enmienda de la Carta Magna Americana, es un pilar en la obtención lícita de la prueba, el garantizar el bienestar de las personas y la seguridad a su privacidad; a su vez, prescriben la posibilidad de traspasar la misma siempre que se satisfagan los requisitos procedimentales que determina cada ordenamiento, sobre todo, en tratándose de intervención de comunicaciones privadas para la obtención de pruebas lícitas, que permitan su incorporación procesal. En el caso mexicano no basta la "causa probable" para solicitar la intervención de comunicaciones privadas, sino que se deben especificar las condiciones particulares y el objeto de ésta para que un juez de control la otorgue, de forma temporal y particularizada. En caso que alguna autoridad investigadora no cumpla con los requisitos constitucionales anteriormente expuestos, podría incurrir en la comisión de un delito y en consecuencia, "envenenar" cualquier medio de convicción que pretenda incorporar a un procedimiento por no contar con una debida "cadena de custodia".

La Cadena de Custodia se precisa en el Diccionario Jurídico mexicano como "el sistema de control y registro que se aplica al indicio, evidencia, objeto, instrumento o producto del hecho delictivo, desde su localización…hasta que la autoridad

competente ordene su conclusión".[36] En términos generales, la podemos concebir como los requisitos legales que permiten a la autoridad investigadora conservar la prueba pura hasta la incorporación de la misma a la *litis* y la valoración del juez.

En derecho comparado, los Tribunales argentinos en materia "criminal" han permitido la incorporación de comunicaciones privadas, aunque no se hubiese solicitado la intervención al juzgador o se notificara a la contraparte que la conversación se estuviere fijando, siempre que no exista una grabación ilegal y, como excepción, que un fedatario público (escribano público) certifique el contenido y hechos de la comunicación. La Cámara Criminal y Correccional Federal, Sala II, en el caso Argañaraz, Agustín s/Nulidad de noviembre de 2006, dictó que no se puede considerar que esto viola el derecho de la intimidad al presentar la comunicación como evidencia, ya que no se ocupa un elemento tecnológico para intervenir dicha comunicación. En el caso mexicano, esta hipótesis parece resolverse de una forma más clara, gracias al propio artículo 16 constitucional, ya que constitucionalmente faculta a uno de los participantes de la comunicación a "levantar la secrecía" sin que para ello fuere necesaria intervención alguna. Así lo reconoció la Primera Sala de nuestra Suprema Corte de Justicia como criterio vinculante, en los siguientes términos:

> **DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SE IMPONE SÓLO FRENTE A TERCEROS AJENOS A LA COMUNICACIÓN.**
>
> **La reserva de las comunicaciones**, prevista en el artículo 16, párrafos decimosegundo y decimotercero, de la Constitución Política de los Estados Unidos Mexicanos, **se impone sólo frente a terceros ajenos a la comunicación**. De tal forma que **el levantamiento del secreto por uno de los participantes en la comunicación no se considera una violación a este derecho fundamental**. Lo anterior no resulta óbice para que, en su caso, se configure una violación al derecho a la intimidad dependiendo del contenido concreto de la conversación divulgada.[37] (Énfasis añadido)

En términos de este último criterio, ninguna aportación de comunicaciones privadas puede aceptarse en menoscabo una esfera jurídica sensible o un bien jurídico tutelado superior al que se procura reparar, como lo podría ser la intimidad, un derecho de personalidad o un derecho humano, independientemente del mérito que

[36] DICCIONARIO JURÍDICO. *Cadena de custodia*. http://www.diccionariojuridico.mx/?pag=vertermino&id=1704

[37] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. *Derecho a la inviolabilidad de las comunicaciones privadas. Se impone sólo frente a terceros ajenos a la comunicación.* Primera Sala. Tesis 1a./J. 5/2013 (9a.). Décima Época. Semanario Judicial de la Federación y su Gaceta. Libro XIX, Abril de 2013, Tomo 1, Página 357 Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/ el 03 de diciembre de 2017.

podría brindar para favorecer la sentencia del juicio. Así las cosas, la regla general dicta que el ofrecimiento de comunicaciones privadas y su intervención debe seguir con los requisitos procesales o constitucionales que se fijen en cada legislación, por lo que cualquier desviación en los mismos podría constituir un delito; asimismo, la excepción a la regla pacta que dichas comunicaciones privadas habrán de aportarse sin necesidad de agotar requisitos de admisibilidad, si es que se forma parte de la comunicación, en tanto que no se afecta una esfera superior de derechos (excepción dentro de la excepción). En consecuencia de lo anterior, el Poder Judicial de la Federación mexicano, ha publicado los siguientes criterios relacionados:

> **PRUEBA ELECTRÓNICA O DIGITAL EN EL PROCESO PENAL. LAS EVIDENCIAS PROVENIENTES DE UNA COMUNICACIÓN PRIVADA LLEVADA A CABO EN UNA RED SOCIAL, VÍA MENSAJERÍA SINCRÓNICA (CHAT), PARA QUE TENGAN EFICACIA PROBATORIA DEBEN SATISFACER COMO ESTÁNDAR MÍNIMO, HABER SIDO OBTENIDAS LÍCITAMENTE Y QUE SU RECOLECCIÓN CONSTE EN UNA CADENA DE CUSTODIA.**
> El derecho a la inviolabilidad de las comunicaciones privadas, previsto en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, se extiende a las llevadas a cabo mediante cualquier medio o artificio técnico desarrollado a la luz de las nuevas tecnologías, desde el correo o telégrafo, pasando por el teléfono alámbrico y móvil, hasta las comunicaciones que se producen mediante sistemas de correo electrónico, mensajería sincrónica (chat), en tiempo real o instantánea asincrónica, intercambio de archivos en línea y redes sociales. En consecuencia, para que su aportación a un proceso penal pueda ser eficaz, la **comunicación debe allegarse lícitamente, mediante autorización judicial para su intervención o a través del levantamiento del secreto por uno de sus participantes pues**, de lo contrario, **sería una prueba ilícita**, por haber sido obtenida mediante violación a derechos fundamentales, con su consecuente nulidad y exclusión valorativa. De igual forma, dada la naturaleza de los medios electrónicos, generalmente intangibles hasta en tanto sou reproducidos en una pautalla o impresos, fácilmente susceptibles de manipulación y alteración, ello exige que para constatar la veracidad de su origen y contenido, **en su recolección sea necesaria la existencia de los registros condignos que a guisa de cadena de custodia, satisfagau el principio de mismidad que ésta persigue, o sea, que el contenido que obra en la fuente digital sea el mismo que se aporta al proceso.** Así, de no reunirse los requisitos mínimos enunciados, los indicios que eventualmente se puedan generar, no tendrían eficacia probatoria en el proceso penal, ya sea por la ilicitud de su obtención o por la falta de fiabilidad en ésta.[38]
>
> **(Énfasis añadido)**

[38] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. *Prueba electrónica o digital en el proceso penal. Las evidencias provenientes de una comunicación privada llevada a cabo en una red social, vía mensajería sincrónica (chat), para que tengan eficacia probatoria deben satisfacer como estándar*

DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SU ÁMBITO DE PROTECCIÓN SE EXTIENDE A LOS DATOS ALMACENADOS EN EL TELÉFONO MÓVIL ASEGURADO A UNA PERSONA DETENIDA Y SUJETA A INVESTIGACIÓN POR LA POSIBLE COMISIÓN DE UN DELITO. En términos del artículo 16 de la Coustitución Política de los Estados Unidos Mexicanos, para intervenir una comunicación privada se requiere autorización exclusiva de la autoridad judicial federal, a petición de la autoridad federal que faculte la ley o del titular del Ministerio Público de la entidad federativa correspondiente, por lo que todas las formas existentes de comunicación y las que son fruto de la evolución tecnológica deben protegerse por el derecho fundamental a su inviolabilidad, como sucede con el teléfono móvil en el que se guarda información clasificada como privada por la Primera Sala de la Suprema Corte de Justicia de la Nación; de ahí que el ámbito de protección del derecho a la inviolabilidad de las comunicaciones privadas se extiende a los datos almacenados en tal dispositivo, ya sea en forma de texto, audio, imagen o video. Por lo auterior, no existe razón para restringir ese derecho a cualquier persona por la sola circunstancia de haber sido deteuida y estar sujeta a iuvestigación por la posible comisión de un delito, de mauera que si la autoridad encargada de la investigaciou, al detenerla, advierte que trae consigo un teléfono móvil, está facultada para decretar su aseguramiento y solicitar a la autoridad judicial la intervención de las comunicaciones privadas conforme al citado artículo 16 constitucional; sin embargo, si se realiza esa actividad sin autorización judicial, cualquier prueba que se extraiga, o bien, la que derive de ésta, será considerada como ilícita y no tendrá valor jurídico alguno.[39]

PRUEBA ILÍCITA. NO LA CONSTITUYE LA OBTENCIÓN DE LA IMPRESIÓN FOTOGRÁFICA DEL PERFIL DEL IMPUTADO EN UNA RED SOCIAL (FACEBOOK) EN CUYAS POLÍTICAS DE PRIVACIDAD SE ESTABLECE QUE AQUÉLLA ES PÚBLICA (LEGISLACIÓN PARA EL DISTRITO FEDERAL). Conforme con la tesis aislada 1a. CLVIII/2011 de la Primera Sala de la Suprema Corte de Justicia de la Nación, visible eu el Semanario Judicial de la Federación y su Gaceta, Novena Época, Tomo XXXIV, agosto de 2011, página 217, de rubro: "DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. MEDIOS

mínimo, haber sido obtenidas lícitamente y que su recolección conste en una cadena de custodia. Tribunales Colegiados de Circuito. I.2o.P.49 P (10a.) Libro 38, Enero de 2017, Tomo IV

Página: 2609. Décima Época. Semanario Judicial de la Federación y su Gaceta. Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/ el 03 de diciembre de 2017.

[39] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. *Derecho a la inviolabilidad de las comunicaciones privadas. Su ámbito de protección se extiende a los datos almacenados en el teléfono móvil asegurado a una persona detenida y sujeta a investigación por la posible comisión de un delito.* 1 Tesis: 1a./J. 115/2012 (10a.). Primera Sala. Libro XVII, Febrero de 2013, Tomo Época: Décima Época. Semanario Judicial de la Federación y su Gaceta. Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/ el 03 de diciembre de 2017.

A TRAVÉS DE LOS CUALES SE REALIZA LA COMUNICACIÓN OBJETO DE PROTECCIÓN.", todas las formas existentes de comunicación y aquellas que sean fruto de la evolución tecnológica, deben quedar protegidas por el derecho fundamental a la inviolabilidad de las comunicaciones privadas. Ahora bien, constituye "prueba ilícita" cualquier elemento probatorio que se haya obtenido o incorporado al proceso en violación a derechos fundamentales, como son la inviolabilidad del domicilio o el secreto de las comunicaciones, de manera que cuando la prueba es obtenida mediante una conducta dolosa transgresora de derechos humanos, será espuria, y como tal, deberá privársele de todo efecto jurídico en el proceso penal en atención al respeto de las garantías constitucionales. Por otra parte, a toda persona asiste el derecho humano a la vida privada (o intimidad), cuya noción atañe a la esfera de la vida en la que puede expresar libremente su identidad, en sus relaciones con los demás, o en lo individual. Este derecho a la vida privada tiene vinculación con otros, como aquéllos respecto de los registros personales y los relacionados con la recopilación e inscripción de información personal en bancos de datos y otros dispositivos, que no pueden ser invadidos sin el consentimiento de su titular. En esta tesitura, partiendo de lo dispuesto en el artículo 135, párrafo penúltimo, del Código de Procedimientos Penales para el Distrito Federal, la información contenida en páginas de Internet, constituye un adelanto científico que puede resultar útil como medio probatorio, siempre que para su obtención no se utilicen mecanismos para violar la privacidad de las personas. Bajo tal contexto, y tomando en cuenta que dentro de las políticas de privacidad que se establecen en la red social (Facebook), si bien cada usuario es libre de administrar el contenido y la información que publica o comparte, no obstante, entre esos lineamientos se establece que la fotografía del perfil "es pública", por consiguiente, quien decide usar dicha red social, asume las "políticas de privacidad" que la misma determina, entre las cuales se encuentra la citada, y en ese orden, no puede calificarse como "prueba ilícita" la obtención de la impresión fotográfica del imputado cuando, para conseguirla, la ofendida no hizo otra cosa que acceder a la red social mencionada, e introducir versiones del nombre que recordaba de su probable agresor, comportamiento que bajo ninguna perspectiva puede calificarse como ilegal o violatorio de los derechos humanos del quejoso.[40]

La participación de estos criterios en la construcción del presente capítulo no es accidental, ya que pretende resolver dudas recurrentes en el lector. En la práctica académica me he enfrentado a la incógnita: Un mensaje que se emite a través de la

[40] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. *Prueba ilícita. No la constituye la obtención de la impresión fotográfica del perfil del imputado en una red social (facebook) en cuyas políticas de privacidad se establece que aquella es pública (legislación para el distrito federal).* Tesis: I.5o.P.42 P (10a.) Época: Décima Época. Libro 24, Noviembre de 2015, Tomo IV. Semanario Judicial de la Federación y su Gaceta. Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/ el 03 de diciembre de 2017.

plataforma *WhatsApp,* un mensaje directo a través de *Twitter* o bien, un "inbox" de *Facebook,* ¿pudiere ofrecerse como prueba dentro de un proceso? A parecer de quien escribe, la respuesta es "sí", ya que si bien se estos se consideran comunicaciones privadas y cuentan con dicha protección, estos son susceptibles de intervenirse –de ser legalmente necesario- o bien, de aportarse por el destinatario de los mensajes. Esto no debería complicarse derivado de la nacionalidad de las plataformas, ya que todas ellas cuentan con una representación en cada país en el que desean presencia comercial y mediática. Ahora bien, las "comunicaciones privadas" tampoco se verán violentadas de forma ilícita, si es que el titular de la información privada o sensible, ocupa dichas redes sociales para publicar datos personales que pudieren incorporarse a un proceso, sin que resulte necesario intervenir plataformas o revelar secreto alguno, puesto que la información cambió su categoría a "público", por así disponerlo y actuar a través de sus perfiles, lo que legalmente permitiría ofrecer su contenido dentro de un juicio sin "envenenar" su naturaleza. Caso de estudio diverso es, la imposibilidad de las autoridades investigadores de intervenir un equipo telefónico cuando se detiene a un ciudadano, ya que el mismo contará con la protección constitucional independientemente de los cargos que pudieren imputársele; salvo que el contenido del soporte electrónico sea indispensable para fijar la *litis* y determinar responsabilidad.

En tales términos, se puede afirmar que:

i) Las comunicaciones privadas son inviolables, como regla general;
ii) Para incorporar una comunicación privada a un proceso, ésta se debe obtener lícitamente y obrar en una cadena de custodia;
iii) Existen diversas vías para la obtención lícita de la prueba: a) Satisfacción constitucional o procedimental de los requisitos para su intervenciόu, b) Levantamiento de secrecía o, c) la información litigiosa sea torne de carácter público (Verbigracia, se publique en la red a través de redes sociales o se ponga a disposición de medios masivos de comunicación); y
iv) En caso de no cumplir con alguna de las hipótesis del inciso "iii)", la prueba se considerará ilícita por violar la privacidad e intimidad del contrario. Ello podría no sólo generar la nulidad de la prueba, sino de la sentencia que se pudiere dictar con fundamento en la misma.

Sin embargo, los precedentes del Poder Judicial de la Federación (México) no detienen su actividad en ese rubro, pues el Noveno Tribunal Colegiado en Materia Penal del Primer Circuito, en interpretación de los artículos 123, 123 Bis, 123 Ter y 123 Quáter del Código Federal de Procedimientos Penales, defienden que no es necesario fijar cadena de custodia sobre objetos informáticos que hubieren sido utilizados para cometer el delito; así se desprende del rubro "**CADENA DE CUSTODIA. SI EL OBJETO UTILIZADO POR EL IMPUTADO PARA COMETER EL**

DELITO CONSTITUYE UN SISTEMA INTANGIBLE QUE NO PUEDE EMBALARSE, CUSTODIARSE O RESGUARDARSE, AL TRATARSE DE UN SISTEMA INFORMÁTICO, ES LEGAL QUE NO SE LLEVE A CABO UN REGISTRO DE AQUÉLLA"; que en décima época se encuentra bajo el registro Tesis: I.9o.P.210 P (10a.).

XII.5. 4 Incorporación procesal de *WhatsApp*

El pasado mes de enero de 2017, el Segundo Tribunal Colegiado en Materia Penal del Primer Circuito, emitió un precedente interesante para los fanáticos de la prueba digital, así como del Derecho Informático. Mediante la tesis aislada I.2°.P.49 P (10ª.), cuyo rubro dicta: *PRUEBA ELECTRÓNICA O DIGITAL EN EL PROCESO PENAL. LAS EVIDENCIAS PROVENIENTES DE UNA COMUNICACIÓN PRIVADA LLEVADA A CABO EN UNA RED SOCIAL, VÍA MENSAJERÍA SINCRÓNICA (CHAT), PARA QUE TENGAN EFICACIA PROBATORIA DEBEN SATISFACER COMO ESTÁNDAR MÍNIMO, HABER SIDO OBTENIDAS LÍCITAMENTE Y QUE SU RECOLECCIÓN CONSTE EN UNA CADENA DE CUSTODIA*[41], el Tribunal afirmó que la comunicación privada que se origina a través de sistemas de correo electrónico, mensajería sincrónica (chat), en tiempo real o instantánea asincrónica, sistemas de intercambio de archivos en línea y redes sociales, puede incorporarse a un proceso de orden penal siempre que se obtenga lícitamente y cuya recolección respete el principio de mismidad mediante registros condignos que permitan acreditar el origen, contenido y fiabilidad entre la fuente digital y el mensaje de datos que se aporta al proceso. Por lo que refiere a este último requisito, el Tribunal Colegiado invita a la preservación de la comunicación privada en forma de "cadena de custodia", sin que procesalmente exista un protocolo mexicano universal para la preservación de pruebas consistentes en información de naturaleza digital. Independientemente del análisis que merece el derecho a inviolabilidad de comunicaciones privadas, consagrado en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos o la indiferente sinonimia en nuestro sistema respecto de pruebas informáticas, electrónicas y digitales; ocupa mi atención el progresista y al mismo tiempo insuficiente criterio del Poder Judicial de la Federación, ya que obliga al oferente a acreditar la licitud y recolección mediante una cadena de custodia, sin precisar algún protocolo a seguir, en afán de no atentar contra la licitud de la prueba. En ese tenor, ¿podríamos aportar legalmente cualquier comunicación que generamos a través de *WhatsApp*? ¿Qué cadena de custodia debe aplicarse sobre un mensaje de datos de esta naturaleza? Y ¿resulta aplicable el mismo criterio para otras materias?

[41] Segundo Tribunal Colegiado en Materia Penal del Primer Circuito. Amparo directo 97/2016 de 11 de agosto de 2016.

Tendremos que ir con pies de plomo para resolver dichas incógnitas. En primer lugar, es prudente comprender el concepto de cadena de custodia que rescata nuestro sistema jurídico, así como atender los Protocolos que existen al respecto. Posteriormente, analizaremos los artículos que obligan a la autoridad jurisdiccional a aceptar la incorporación de medios de convicción novedosos en el proceso; consecuentemente, enfrentaremos las vías procesales lícitas de obtención de comunicaciones privadas contra las políticas de la plataforma *WhatsApp Inc.,* con la humilde intención de ofrecer una ruta jurídicamente viable, a quien me honra con su lectura.

En primer lugar y como respuesta a la entrada en vigor del sistema de justicia penal acusatorio, el 12 de febrero de 2015, se publicó en el Diario Oficial de la Federación el Acuerdo A/009/15 por el que se establecen las directrices que deberán observar los servidores públicos que intervengan en materia de cadena de custodia, emitido por Jesús Murillo Karam, entonces Procurador General de la República. Dicho Acuerdo define la **cadena de custodia** como "…el sistema de control y registro que se aplica al indicio o elemento material probatorio, desde su localización, descubrimiento o aportación, en el lugar de intervención, hasta que la autoridad competente ordene su conclusión"; definición que resulta consonante con la prescrita en el artículo 227 del Código Nacional de Procedimientos Penales, del cual se desprende que una cadena de custodia deberá cumplir con los factores de: i) Identidad, ii) Estado Original, iii) Condiciones de recolección, iv) Preservación, v) Empaque y vi) Traslado, vii) Lugares y fechas de permanencia, viii) Cambios en cada custodia, y ix) Responsables y personas que tengan contacto con esos elementos.

Por su lado, el Pleno del Consejo de la Judicatura Federal, expidió el "Protocolo de actuación para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales"; publicado el 17 de junio de 2016 a través del Diario Oficial de la Federación, así como sus Lineamientos.[42] De estos instrumentos normativos destaca:

- Actuación en sitio.- Implica la obligación de la autoridad judicial de iniciar la investigación con al menos dos personas autorizadas de la Dirección General de Tecnologías de la Información.

  – Se realizará inventario de hardware, a través del "Registro de cadena de custodia" y "Formato de entrega-recepción de recursos informáticos y/o evidencia digital". El Protocolo define la evidencia digital como la "información almacenada de forma binaria que puede ser utilizada en una investigación o procedimiento".

[42] Poder Judicial de la Federación. Consejo de la Judicatura Federal. *Lineamientos para la obtención y tratamiento de los recursos informáticos y/o evidencias digitales.* Visible el 13 de febrero de 2018, a través del vínculo http://www.cjf.gob.mx/resources/index/infoRelevante/2016/pdf/LINEAMIENTOS_OBTENCION_TRATAMIENTO_RECURSOSINFORMATICOS.pdf

- Obtención de la información dinámica o en procesamiento.- Implica la obtención de datos en tiempo real así como de la información dinámica en procesamiento (aquella que se pierde al interrumpirse la alimentación eléctrica del recurso informático)
- Generación de imagen forense.- Implica el aseguramiento total del hardware y software que se considera relevante para la investigación. Esto tendrá forma de reporte y permitirá que el juez de control realicé su examen sobre el análisis de la Dirección general de tecnologías de la información. En términos del Protocolo, se define como la "copia bit a bit del dispositivo o medio electrónico de almacenamiento".
- Capacitación del informático forense.- Éste deberá ser licenciado en informática, ingeniero en electrónica, licenciado en sistemas computacionales, licenciado en administración de tecnologías de la información, ingeniero en sistemas electrónicos o perfil tecnológico afín. Adicionalmente, deberá contar con conocimiento mínimo en sistemas operativos Windows, Linux, Mac y prevención de pérdida de información, así como certificaciones ISO, ITL, *EnCase, Certified Ethical Hacking y Certified Forensic Examiner*, entre otras.

A su vez, la Procuraduría General de la República, en colaboración con el Instituto Nacional de Ciencias Penales, desarrollaron el texto "Protocolos de Cadena de Custodia. Dos grandes etapas: preservación y procesamiento".[43] Este manual contiene los métodos, técnicas de investigación y técnicas de fijación de evidencias en atención al tipo penal del que se trate, así como la naturaleza de la escena para el acordonamiento. En lo relativo a la preservación, distingue lugares abiertos y cerrados, en tanto que el procesamiento contiene la guía que permitirá una legal recolecta y la posibilidad de aportar tales medios de convicción a procedimientos de orden penal. En lo particular, el punto 4, "Tipos de muestras (indicios o evidencias)" contiene diversos medios a través de los cuáles se fija una prueba, entre los que destacan la i) cámara digital, ii) discos compactos, DVD o película fotográfica ya procesada y iii) documentos; sin embargo, estas hipótesis parecen atender únicamente a características análogas y contiene instrucciones que permiten embalar los dispositivos que almacenan nuestras pruebas informáticas.

Por lo que refiere a la admisibilidad de pruebas contenidas en medios electrónicos o digitales –siempre que respeten los protocolos antes citados-, la normatividad mexicana expande las facultades procesales del juzgador, a través del nuevo Código Nacional de Procedimientos Penales, cuyos artículos 381 y 382, prescriben de tenor literal:

[43] Procuraduría General de la República. *Protocolos de cadena de custodia. Dos grandes etapas: preservación y procesamiento.* México. Instituto Nacional de Ciencias Penales. 2012. Segunda edición. Visible el 13 de febrero de 2018 a través del vínculo http://www.inacipe.gob.mx/stories/publicaciones/descargas_gratuitas/ProtocolosdeCadenadeCustodia.pdf

Artículo 381. **Reproducción en medios tecnológicos**
En caso de que los datos de prueba o la prueba se encuentren contenidos en medios digitales, electrónicos, ópticos o de cualquier otra tecnología y el Órgano jurisdiccional no cuente con los medios necesarios para su reproducción, la parte que los ofrezca los deberá proporcionar o facilitar. Cuando la parte oferente, previo apercibimiento no provea del medio idóneo para su reproducción, no se podrá llevar a cabo el desahogo de la misma.

Artículo 382. **Prevalencia de mejor documento**
Cualquier documento que garantice mejorar la fidelidad en la reproducción de los contenidos de las pruebas deberá prevalecer sobre cualquiera otro.[44]

Preceptos que permiten al Juez de turno, aceptar medios de convicción que se hubieren fijado a través de medios tecnológicos, sólo condicionando al oferente a proporcionar el dispositivo para la reproducción y desahogo de la prueba. Por otro lado, el diverso 382 sostiene la posibilidad procesal de aceptar los documentos que mejoren la fidelidad en la reproducción, en cuyo caso, deberíamos descartar impresiones de pantalla o certificaciones notariales, que atentan contra la naturaleza de la prueba y la comunicación privada que se pudiere incorporar, en beneficio de exhibir el documento digital original en el dispositivo emisor o receptor, o bien, obtener registro condigno del proveedor del servicio.

A su vez, el Código Federal de Procedimientos Civiles exige el reconocimiento probatorio a la información que se generó o comunicó a través de medios electrónicos u ópticos, según se desprende del de artículo 210-A, cuyo texto vigente ordena:

ARTICULO 210-A.- Se reconoce como prueba la información generada o comunicada que conste en medios electrónicos, ópticos o en cualquier otra tecnología. Para valorar la fuerza probatoria de la información a que se refiere el párrafo anterior, se estimará primordialmente la fiabilidad del método en que haya sido generada, comunicada, recibida o archivada y, en su caso, si es posible atribuir a las personas obligadas el contenido de la información relativa y ser accesible para su ulterior consulta. Cuando la ley requiera **que un documento sea conservado y presentado en su forma original, ese requisito quedará satisfecho si se acredita que la información generada, comunicada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología, se ha mantenido íntegra e inalterada a partir del momento en que se**

[44] Cámara de Diputados del Congreso de la Unión. *Código Nacional de Procedimientos Penales.* Publicado el 17 de junio de 2016 en el Diario Oficial de la Federación. Visible el 13 de febrero de 2018 a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf

generó por primera vez en su forma definitiva y ésta pueda ser accesible para su ulterior consulta.[45]

(El énfasis es añadido)

Hasta este punto, parece adecuado afirmar que existeu aparatos normativos que regulan puntualmente la cadena de custodia sobre una recursos informáticos y evidencia digital, por lo que se tendrían que aplicar, prudentemente, las reglas generales contenidas en dichos ordenamientos y de esta forma conseguir la obtención de un valor probatorio privilegiado dentro del proceso, según lo prescriben los códigos adjetivos, penal y civil, que hemos invocado. Empero, parece ser que estos Protocolos de recolección y las reglas procesal no analizan el universo de los mensajes de datos cuya especial naturaleza, los lleva a tener una representación de carácter digital, por lo que es complejo su embalaje y en consecuencia, la obtención de la imagen forense sobre estos; particularmente, a la cadena de custodia de un mensaje privado de *WhatsApp* y su debida incorporación al proceso para ser considerado lícito y con posibilidad de obtener valor probatorio. A saber de algunos más sabios que yo, la forma adecuada de obtener un mensaje de datos cuyo origen yace en un sistema de mensajería instantánea, siempre ha de ser a través de la intervención constitucional de las comunicaciones. Sin embargo, ello no respeta la naturaleza digital de este tipo de comunicación, ya que, tal como refiero más adelante, algunos mensajes se encuentran encriptados o bien, podrían obtenerse legalmente a través de los servidores de la compañía WhatsApp Inc.

Conforme lo anterior, ¿podría considerarse "intervención de comunicaciones privadas" a la incorporación de un mensaje instantáneo al proceso? En su caso, el Juez de Control debe analizar el cumplimiento de los requisitos prescritos en los diversos 291, 292, 293 y 294 del Código Nacioual de Procedimientos Penales (en interpretación armónica con lo previsto en el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos):

> Artículo 291. **Intervención de las comunicaciones privadas**
> Cuando en la investigación el Ministerio Público considere necesaria la intervención de comunicaciones privadas, el Titular de la Procuraduría General de la República, o en quienes éste delegue esta facultad, así como los Procuradores de las entidades federativas, podrán solicitar al Juez federal de control competente, por cualquier medio, la autorización para practicar la intervención, expresando el objeto y necesidad de la misma. La intervención de comunicaciones privadas, abarca todo sistema de comunicación, o programas que sean resultado de la evolución tecnológica, que permitan el

[45] Cámara de Diputados del Congreso de la Unión. *Código Federal de Procedimientos Civiles*. Publicado el 09 de abril de 2012 en el Diario Oficial de la Federación. Visible el 13 de febrero de 2018 a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/6.pdf

intercambio de datos, informaciones, audio, video, mensajes, así como archivos electrónicos que graben, conserven el contenido de las conversaciones o registren datos que identifiquen la comunicación, los cuales se pueden presentar en tiempo real.

La solicitud deberá ser resuelta por la autoridad judicial de manera inmediata, por cualquier medio que garantice su autenticidad, o en audiencia privada con la sola comparecencia del Ministerio Público, en un plazo que no exceda de las seis horas siguientes a que la haya recibido. **También se requerirá autorización judicial en los casos de extracción de información, la cual consiste en la obtención de comunicaciones privadas, datos de identificación de las comunicaciones; así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, accesorio, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información, incluyendo la almacenada en las plataformas o centros de datos remotos vinculados con éstos**.

Si la resolución se registra por medios diversos al escrito, los puntos resolutivos de la autorización deberán transcribirse y entregarse al Ministerio Público. Los servidores públicos autorizados para la ejecución de la medida serán responsables de que se realice en los términos de la resolución judicial.

Artículo 292. Requisitos de la solicitud

La solicitud de intervención deberá estar fundada y motivada, precisar la persona o personas que serán sujetas a la medida; la identificación del lugar o lugares donde se realizará, si fuere posible; el tipo de comunicación a ser intervenida; su duración; el proceso que se llevará a cabo y las líneas, números o aparatos que serán intervenidos, y en su caso, la denominación de la empresa concesionada del servicio de telecomunicaciones a través del cual se realiza la comunicación objeto de la intervención. El plazo de la intervención, incluyendo sus prórrogas, no podrá exceder de seis meses. Después de dicho plazo, sólo podrán autorizarse nuevas intervenciones cuando el Ministerio Público acredite nuevos elementos que así lo justifiquen.

Artículo 293. Contenido de la resolución judicial que autoriza la intervención de las comunicaciones privadas

En la autorización, el Juez de control determinará las características de la intervención, sus modalidades, límites y en su caso, ordenará a instituciones públicas o privadas modos específicos de colaboración.

Artículo 294. Objeto de la intervención Podrán ser objeto de intervención las comunicaciones privadas que se realicen de forma oral, escrita, por signos, señales o mediante el empleo de aparatos eléctricos, electrónicos, mecánicos, alámbricos o inalámbricos, sistemas o equipos informáticos, así como por cualquier otro medio o forma que permita la comunicación entre uno o varios emisores y uno o varios receptores… El Juez podrá en cualquier momento verificar que las intervenciones sean realizadas en

los términos autorizados y, en caso de incumplimiento, decretar su revocación parcial o total **(El énfasis es añadido)**.

De los preceptos que invoqué, se advierte que la intervención de comunicaciones y la extracción de información son dos hipótesis diversas que atienden a la edad del mensaje de datos (fecha de creación) que se pudiera pretender invocar al proceso. Es decir, si la naturaleza de la evidencia que se desea captar para el proceso, consiste en acreditar las presunciones de la comisión de un hecho ilegal que se cometió, que se está cometiendo o que se cometerá, sin que se tenga conocimiento claro de la existencia de la misma, siempre resultará prudente la intervención de comunicaciones, en tanto que, si existen presunciones de la existencia de un mensaje de datos que pudiera acreditar la culpabilidad de un imputado, exonerarle o bien, simplemente favorecer las pretensiones del oferente –inclusive ante el riesgo de pérdida del mensaje de datos-, la vía jurídica adecuada será la extracción de información a que refiere al penúltimo párrafo del artículo 291.

Por su lado, *WhatsApp, Inc* se fundó en el año 2009 como un proyecto dedicado a tecnología Blackberry, sin embargo, pronto llamó la atención de grandes inversionistas y mudó sus oficinas a Estados Unidos de América. El progreso de la aplicación y la interoperabilidad con otros dispositivos, despertó el bolsillo de Mark Zuckerberg y sus accionistas; para febrero de 2014, *WhatsApp* pertenecería al grupo de filiales digitales de *Facebook*, por la cantidad de 19 mil millones de dólares.[46] Su ingreso al mundo de los titanes de las redes sociales le permitió reportar crecimientos inimaginables. Tan sólo para el 2017, la propia compañía anunció que supera los mil millones de usuarios activos al día, soporta más de 55 mil millones de mensajes diarios entre los que se incluyen los más de 4 mil 500 millones correspondientes a imágenes[47]. Sin duda, estos mensajes podrían contener conductas susceptibles de revisión judicial, por lo que Jan Koum –fundador- propone las siguientes directrices:

Información para las fuerzas del orden

...

WhatsApp ofrece mensajería, llamadas por Internet y otros servicios a usuarios alrededor del mundo...

[46] SUÁREZ, Eduardo. "Facebook compra WhatsApp por 19.000 millones de dólares". *El Mundo*. Edición España. Corresponsal en Nueva York, nota del 20 de febrero de 2014. Visto el 13 de febrero de 2018 a través del vínculo http://www.elmundo.es/economia/2014/02/19/53052f1e268e3eed5d8b456c.html

[47] TECHBIT. *EL UNIVERSAL*. "WhatsApp supera los mil millones de usuarios activos al día." Periódico en línea dol Universal. Redacción y Agencias. México, 28 de julio de 2017. Visible el 13 de febrero de 2018 a través del vínculo http://www.eluniversal.com.mx/articulo/techbit/2017/07/28/whatsapp-supera-los-mil-millones-de-usuarios-activos-al-dia

WhatsApp valora el trabajo que las fuerzas del orden realizan para mantener a las personas a salvo alrededor del mundo. Estamos dispuestos revisar, validar y responder a aquellas solicitudes de las fuerzas del orden de acuerdo a la legislación y política aplicable.

(...) los agentes de las fuerzas del orden pueden ponerse en contacto con WhatsApp para cualquier pregunta, así como en situaciones de emergencia (como se detalla más abajo).

(...)

Requisitos para procesos legales en EE. UU.

Sólo revelamos datos de las cuentas de acuerdo con nuestras condiciones del servicio y la legislación aplicable, **incluida** la **ley federal estadounidense de almacenamiento de datos ("Stored Communications Act", SCA), 18 USC, secciones 2701-2712**. En virtud de la legislación estadounidense:

- Se necesita una citación válida emitida en relación con una investigación criminal oficial para exigir la revelación de datos básicos del suscriptor...
- Se necesita una orden judicial emitida por un tribunal...
- Se necesita una orden de registro emitida según los procedimientos descritos en la normativa federal para procedimientos penales o según los procedimientos estatales equivalentes en el caso de que exista una causa probable para exigir la revelación de contenido almacenado en cualquier cuenta, en el que se pueden incluir la información de "Info", fotos de perfil, información de grupo, y directorio telefónico, si están disponibles. **WhatsApp no guarda mensajes una vez han sido entregados ni registros de transacción de esos mensajes entregados, y los mensajes no entregados son eliminados de nuestros servidores pasados 30 días. WhatsApp ofrece cifrado de extremo a extremo para nuestros servicios, el cual está activo por defecto**.

Conservación de la cuenta

Haremos lo posible por conservar los datos de las cuentas relacionadas con una investigación penal durante 90 días, en espera del proceso legal correspondiente...

Solicitudes de emergencia

En respuesta a una situación que implique un perjuicio inminente a un menor o riesgo de muerte o lesiones graves para cualquier persona, y que requiera la revelación de información de forma inmediata, un agente de las fuerzas del orden puede enviar una solicitud a través de un correo electrónico. Para acelerar el proceso de estas solicitudes, **recomendamos incluir la palabra "EMERGENCY"** en el asunto del mensaje.

Nota: No responderemos a las solicitudes enviadas por personas que no pertenezcan a las fuerzas del orden. **Por favor, envía tu solicitud de emergencia desde una dirección de correo electrónico oficial**. Los usuarios que tengan constancia de una situación de emergencia (...)

Correo electrónico

Los miembros de las fuerzas del orden deben enviar una solicitud desde una dirección de correo electrónico oficial a records@whatsapp.com. Los agentes de las fuerzas del orden que no pueden incluir el proceso legal en un correo electrónico, pueden notificarnos por correo electrónico de sus limitaciones para que podamos coordiuar el servicio del proceso.

...

Atención: WhatsApp Inc., Law Enforcement Response Team

El tiempo de respuesta será más largo si los miembros de las fuerzas del orden no envían su solicitud por correo electrónico. Enviar una solicitud en ambas formas, por correo electrónico y postal, puede incrementar el tiempo de respuesta.[48]

(El énfasis es añadido)

Sin embargo, estas no son las únicas condiciones a tomar en cuenta antes de pretender incorporar un mensaje de esta naturaleza al proceso, ya que existen mensajes "Cifrados de extremo a extremo", cuya especial naturaleza, no permitirían la participación activa de la plataforma para coadyuvar con la autoridad jurisdiccional; al menos por lo que refiere a mensajes que se emitieron después de febrero de 2014, cuando la plataforma fue adquirida por Facebook e hizo obligatoria la encriptación de comunicaciones. Esto se desprende del capítulo respectivo, de los Términos y Políticas de uso de *WhatsApp;* mismas que de tenor literal, indican:

Cifrado de extremo a extremo

La seguridad y privacidad de nuestros usuarios forman parte de nuestro ADN, por ello ofrecemos el cifrado de extremo a extremo en las versiones más recientes de nuestra aplicación. Con el cifrado de extremo a extremo tus meusajes, fotos, videos, meusajes de voz, documentos, actualizaciones de estado y llamadas están seguros.

El cifrado de extremo a extremo en WhatsApp asegura que sólo tú y el receptor puedan leer lo que se envía, y que nadie más, ni siquiera WhatsApp, lo pueda hacer. Tus meusajes se aseguran con un candado y sólo tú y el receptor cuentan cou el código/llave especial para abrirlo y leer los mensajes. Para mayor protección, cada mensaje que envías tiene su propio candado y código único. Todo esto pasa de manera automática; sin necesidad de realizar ajustes o de crear chats secretos para asegurar tus mensajes.

WhatsApp no tiene manera de ver el contenido de tus mensajes o de escuchar tus llamadas en WhatsApp. Esto es porque el cifrado y descifrado de los mensajes enviados a través de WhatsApp ocurre completamente en tu teléfono. Antes de

[48] *WhatsApp, Inc. Preguntas frecuentes. Información para las fuerzas del orden.*

que un mensaje salga de tu teléfono, se asegura con un candado criptográfico, y sólo el destinatario tiene la clave. Además, las claves cambian con cada mensaje enviado. Todo esto ocurre en segundo plano, pero puedes confirmar que tus conversaciones están protegidas si compruebas el código de verificación de seguridad en tu teléfono. Encontrarás más detalles sobre esto en nuestro documento.

En muchas ocasiones, la gente se pregunta qué implica el cifrado de extremo a extremo en relación al trabajo de las fuerzas del orden. WhatsApp valora el trabajo que las fuerzas del orden realizan para mantener a las personas a salvo alrededor del mundo. Revisamos, validamos y respondemos a aquellas solicitudes de las fuerzas del orden de acuerdo a la legislación y política aplicable, y damos prioridad a solicitudes de emergencia. [49]

(El énfasis es añadido).

Estas condiciones parecen ser adecuadas a los principios de seguridad informática que sostiene *WhatsApp:* i) Habla libremente, ii) Tus mensajes te pertenecen (protección de mensajes y cifrado de extremo a extremo), y iii) Compruébalo (cadenas de validación para garantizar la inviolabilidad de las comunicaciones). Hasta este punto, si llegamos a confrontar las reglas procesales contenidas en nuestro sistema jurídico, frente a los requisitos y condiciones que solicita la plataforma para colaborar con "las fuerzas del orden", sería prudente aseverar que estamos ante el complejo dilema del juzgador (o en su caso, los oferentes): 1) Optar por permitir la participación activa de *WhatsApp* Inc o bien, 2) Ocupar alguna de las vías procesales que brinda nuestro Código. En el primer escenario, nos veríamos ante la incómoda situación en la que, amigablemente, debamos solicitar al Juez de Control, que emita un correo electrónico, desde su cuenta oficial y cumplimentar cada uno de los requisitos que exige la plataforma, máxime, si no conocemos la ruta procesal adecuada para convencer el juez de turno sobre la legalidad de dicho acto y que ello no "envenenará" nuestra prueba y el proceso. Por otro lado, se debe atender a la especial naturaleza de los mensajes encriptados, bajo la modalidad "cifrado de extremo a extremo", en cuyo caso, no sería prudente obligar a la plataforma a la aportación de los mensajes objeto de prueba, ya que estos no se encuentran en su poder y únicamente se almacenan en el dispositivo a través del cual se emitieron o recibieron; esta consideración, parece dilucidar que no en todos los escenarios es prudente la intervención de comunicaciones o la extracción de información, como tampoco lo es, una regla absoluta el obtener apoyo internacional de la plataforma.

Es inconcuso que nos enfrentamos a un robusto sistema procesal penal que pretende proteger la garantía del debido proceso y licitud en la obtención de la

[49] WhatsApp Inc. *Privacidad y Términos. Cifrado de extremo a extremo.* Preguntas frecuentes. 2018. Visto el 28 de febrero de 2018 a través del vínculo https://faq.whatsapp.com/es/general/28030015

prueba, por lo que, indefectiblemente se deben seguir las reglas adjetivas que señala el Código Nacional de Procedimientos Penales que nos ocupa. En ese tenor, la autoridad jurisdiccional, en este caso, el Juez Federal de control deberá descubrir la forma jurídica más adecuada para cumplir con el procedimiento de solicitud de información previsto por la plataforma *WhatsApp*, sin que una operación tan simple como "enviar correo" pudiere ser considerada insuficientemente fundado y motivado para la incorporación lícita de la prueba en el proceso. A la luz del Código Nacional de Procedimientos Penales, parece que las figuras de Exhorto, Auxilio Procesal, Requisitorias o solicitudes urgentes son las vías más adecuadas para justificar la obtención de un mensaje instantáneo de aquella plataforma y no en todos los casos la intervención de comunicaciones, sin que se considere que se obtuvo de manera ilícita y sin la debida cadena de custodia. El artículo 24 de dicho ordenamiento resuelve esta incógnita, pues prevé la posibilidad de autorización judicial para diligencias urgentes, en cuyo escenario el Ministerio Público anuncia al Juez de control, las actuaciones que deberán efectuarse fuera de su jurisdicción y se tratare de diligencias que requieran atención urgente[50]. Hipótesis que podría ser aceptada por los postulantes más optimistas en la materia, ya que los elementos de **extraterritorialidad** y **urgencia** son características presentes en cualquier solicitud a la plataforma *WhatsApp*, quien, a su vez, cuenta con el procedimiento de **solicitud por emergeucia**[51], según lo hemos reproducido anteriormente. Empero, esto no puede considerarse la panacea de legalidad y debido proceso que buscamos, ya que sería igualmente válido afirmar, que el artículo 24 que nos ocupa resulta insuficiente para considerar que el acto procesal probatorio del Juez de Control, mediante el cual requiere información a la plataforma de mensajería por correo electrónico, se encuentra indebidamente fundado. En este intrincado mapa de colaboración informática o uso de poderes probatorios para intervención de comunicaciones, parece que nos enfrentamos a diversos escenarios igualmente válidos, como debatibles:

[50] El artículo 24 del Código Nacional de Procedimientos Penales, prescribe: "Artículo 24. Autorización judicial para diligencias urgentes El Juez de control que resulte competente para conocer de los actos o cualquier otra medida que requiera de control judicial previo, se pronunciará al respecto durante el procedimiento correspondiente; sin embargo, **cuando estas actuaciones debieran efectuarse fuera de su jurisdicción y se tratare de diligencias que requieran atención urgente**, el Ministerio Público podrá pedir la autorización directamente al Juez de control competente en aquel lugar; en este caso, una vez realizada la diligencia, el Ministerio Público lo informará al Juez de control competente en el procedimiento correspondiente"

[51] Dicha solicitud parece ser vinculante al caso urgente, derivado de un delito grave y riesgo de fuga que sostiene el artículo 16 de la Constitución Política de los Estados Mexicanos.

	Incorporación de mensajes emitidos a través de "*WhatsApp*"	
Sin la colaboración de *WhatsApp, Inc.* (Procedimiento Penal Federal)	**Fundamento**	• Intervención de comunicaciones en términos de los artículos 291, 292, 293 y 294 del Código Nacional de Procedimientos Penales • Extracción de información (obtención de comunicaciones privadas, datos de identificación de las comunicación, así como la información, documentos, archivos de texto, audio, imagen o video contenidos en cualquier dispositivo, acceso, aparato electrónico, equipo informático, aparato de almacenamiento y todo aquello que pueda contener información (Cuarto Párrafo del Artículo 291 del CNPP). • Levantamiento del secreto ("levantamiento de secrecía").- Implica la aportación voluntaria de la comunicación privada, por alguno de los particulares que participen en ella (Párrafo 12, del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos)
	Consideraciones	• Mensajes encriptados.- Los mensajes cifrados a través del mecanismo "cifrado de extremo a extremo", propone la seguridad de los mensajes de datos enviados a través de la plataforma y asegura que estos sólo se encuentren disponibles para el emisor y receptor, en el teléfono móvil respectivo. En ese tenor, la intervención resulta fútil; debiendo solicitar la extracción. (sobre todo en mensajes emitidos después de febrero de 2014) • **Cadena de custodia.**- Lo idóneo implicaría poseer el equipo telefónico o hardware que contenga el mensaje encriptado, sin embargo, se deben seguir las reglas de intervención o extracción de información • **Conservación forense.**- Debe prevalecer la urgencia para la obtención del hardware continente, ante el riesgo de desaparición del mensaje de datos; de otra forma, sólo la extracción legal de la información podría garantizar dicha preservación.

	Incorporación de mensajes emitidos a través de "*WhatsApp*"	
Con la colaboración de *WhatsApp, Inc.* (Solicitud Urgente)	**Fundamento**	• **Solicitud Urgente.**- Esta figura permite al juez de control, tomar las directrices necesarias para incorporar al proceso medios de convicción o bien, realizar los actos procesales necesarios para obtener el apoyo de autoridades o entidades privadas, inclusive, fuera de su jurisdicción (Artículo 24 del CNPP)
	Consideraciones	• Urgencia.- En atención a que no existen criterios vinculantes y precedentes que analicen la urgencia que propone la plataforma, es importante que el oferente, el agente investigador o el juez de control que emita el correo electrónico hacia la plataforma, motive adecuadamente un Estado de Urgencia: i) Perjuicio a un menor, ii) Riesgo de Muerte, o iii) Lesiones graves. Esta hipótesis no permitiría solicitudes urgentes en materia de delincuencia organizada, por ejemplo. • **Cadena de custodia.**- Implicaría obtener el mensaje de datos en los plazos prescritos por la plataforma, en tanto que ello permitiría advertir que aún existen y podrían ser susceptibles de cotejo. • **Conservación forense.**- El juez de control se vería obligado a solicitar el apoyo de la Dirección de Tecnologías para que realice la imagen forense del mensaje, sobre su correo electrónico oficial.

	Incorporación de mensajes emitidos a través de "*WhatsApp*"	
Con la colaboración de *WhatsApp, Inc.* (Colaboración internacional)	**Fundamento**	• **Auxilio Procesal.**- Implica la obligación de la autoridad jurisdiccional para dar cumplimiento al a) Exhorto, b) Mandamiento, o c) Comisión, para la realización de un acto procesal, en apego a los Tratados Internacionales celebrados en materia de persecución de delitos. En ese tenor, el Juez de Control tendría que solicitar el apoyo de su equivalente americano, para que éste, a su vez, dé seguimiento al protocolo que dicta la plataforma de mensajería instantánea (Exhortos y requisitorias/ Artículo 76 y Noveno Transitorio del Código Nacional de Procedimientos Penales)
	Consideraciones	• En caso de no acreditar las hipótesis de "EMERGENCY" que propone la plataforma, el juez de control tendría que optar por la vía en comento, para justificar debidamente su solicitud y la probable incorporación de este mensaje de datos al proceso. Sin embargo, esto es una interpretación semántica muy estricta que no podría resultar práctica en la especie. • **Cadena de Custodia.**- Toda vez que esta fórmula lleva de la mano el apoyo de autoridades ajenas al juez de control, tendríamos que atender a estándares internacionales como los propone la Organización de Estados Americanos. • **Conservación Forense.**- El mensaje de datos deberá garantizar su autenticidad e inalterabilidad desde su aceptación por la autoridad americana, hasta la recepción por parte del juez mexicano (ya sea en físico o digital, aunque lo ideal es la recepción a través de correo electrónico oficial).

Si hasta ahora he defendido la postura de la Plataforma respecto de solicitudes de información, sobre todo, en tratándose de procesos de orden criminal, ¿por qué exponer una hipótesis **sin la colaboración de *WhatsApp, Inc.***? Si bien es cierto, *WhatsApp* propone un procedimiento y formulario para las "fuerzas del orden", no menos cierto es que los mensajes y llamadas que pudiere tener almacenados en sus servidores sólo incluyen aquéllos que no han pasado por el proceso de "Cifrado de extremo a extremo"[52] que brinda el sistema. En este escenario, los usuarios (remitente y receptor) han generado un chat cifrado que garantiza su privacidad, por lo que se presume que todos los mensajes de datos que pudiere contener la comunicación privada entre estos, no es del conocimiento de la plataforma y, por ende, no tuvo posibilidad material de almacenarle. Bajo tales consideraciones, requerir apoyo de *WhatsApp* resultaría fútil por lo inverosímil del requerimiento. En se tenor, resulta imperativo que se realice la preservación de la información contenida en el hardware de los usuarios, así como la extracción de los mensajes de datos a través de la fórmula procesal que propone el artículo 291 del Código Nacional de Procedimientos Penales.

Ahora bien, es interesante analizar lo que ocurre en procesos ajenos al universo del Derecho Penal, es decir, aquellas materias del párrafo decimotercero, del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, que no admiten la intervención de comunicaciones: i) Electoral, ii) Fiscal, iii) Mercantil, iv) Civil, v) Laboral o, vi) Administrativo. En ese tenor, se propone la figura de "**levantamiento del secreto",** según se desprende del párrafo decimosegundo del artículo 16 de la Constitución Política que referimos, a través de la cual se faculta a los particulares para aportar comunicaciones privadas en las cuáles participen, de forma voluntaria y sin la necesidad de intervenir los mensajes privados, en términos del robusto proceso antes citado. Así las cosas, esta incorporación no se consideraría ilícita para los fines procesales. Empero, atiende a dos particularidades: i) Si la conversación que se pretende aportar al proceso se cifró, la preservación y procesamiento deberá ocurrir a la luz del equipo de cómputo (teléfono móvil) que lo contiene, sólo permitiendo el cotejo de su originalidad en confronta con la información que pudiere contener el otro equipo (emisor o receptor) o bien, ii) Si la conversación objeto de prueba no se cifró, esta podría validarse mediante requerimiento judicial con los servidores de la plataforma, si así lo estimare el Juez competente; sin embargo, es prudente señalar que

[52] Según lo describen los administradores de WhatsApp, el cifrado de extremo a extremo brinda seguridad y privacidad a sus usuarios: "… **En 2016, implementamos el cifrado de extremo a extremo para todos los mensajes y llamadas de WhatsApp, de manera que, ni siquiera nosotros, tenemos acceso al contenido de tus conversaciones**. Desde entonces, la seguridad digital se ha vuelto todavía más importante. Hemos visto muchos casos en los que piratas informáticos han obtenido una gran cantidad de información privada de manera ilegal y han abusado de la tecnología para provocar daños a la gente cuya información robaron. Por eso, según hemos ido incluyendo funciones en la aplicación, como videollamadas y Estados, también hemos implementado el cifrado de extremo a extremo en esas funciones."

WhatsApp defiende la integridad de sus testimonios, así como la autenticación de los mensajes que proporciona, rechazando cualquier dictamen pericial sobre estos:

> Testimonios
> WhatsApp no proporciona dictámenes periciales. Además, los registros de WhatsApp se autentican automáticamente con arreglo a la ley, **por lo que no debería ser necesario el testimonio de un conservador de documentos**. Si se requiere algún tipo especial de certificación, por favor, adjúntala a tu solicitud de registros.[53]

Postura que es justa, si lo sometemos a consideración de los principios que señalamos con anterioridad, ya que exigir cualquier validación científica de oficio, atentaría contra la neutralidad y equivalencia funcional de la prueba que nos ocupa. En resumen, un mensaje de este tipo, sí podría incorporarse a un procedimiento de orden civil, por ejemplo, sin necesidad de requerir intervención de comunicaciones, mediante el levantamiento del secreto y cuya validación o certificación tecnológica sobre los servidores de *WhatsApp*, sólo sería admisible en los casos que el mensaje de datos no se encuentre cifrado. A razón de lo anterior, el Poder Judicial de la Federación emitió la Jurisprudencia 1ª./J.5/2013 (9ª.), cuyo texto dicta:

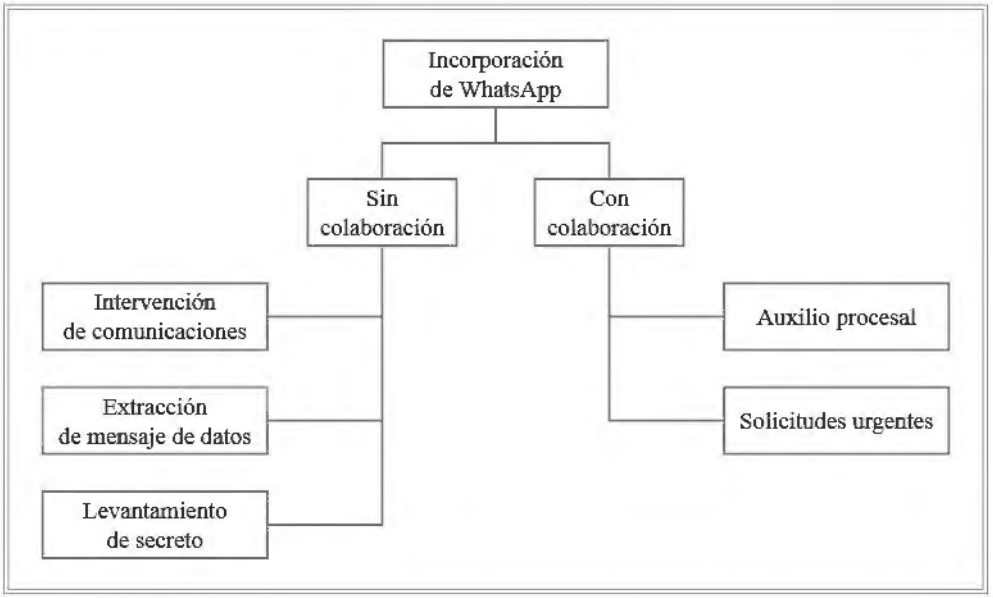
> **DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SE IMPONE SÓLO FRENTE A TERCEROS AJENOS A LA COMUNICACIÓN.**
> La reserva de las comunicaciones, prevista en el artículo 16, párrafos decimosegundo y decimotercero, de la Constitución Política de los Estados Unidos Mexicanos, se impone sólo frente a terceros ajenos a la comunicación. De tal forma que el **levantamiento** del **secreto** por uno de los participantes en la comunicación no se considera una violación a este derecho fundamental. Lo anterior no resulta óbice para que, en su caso, se configure una violación al derecho a la intimidad dependiendo del contenido concreto de la conversación divulgada.[54]

Razonamiento que pudiere aplicarse al universo del Derecho Penal, ya que cualquier mensaje de datos con valor procesal, al incorporarse voluntariamente por la víctima, no configura la hipótesis de intervención de comunicaciones y se debe atender a la naturaleza de la información y su encriptado. A consideración del lector y únicamente con fines pedagógicos, propongo el siguiente mapa conceptual:

---

[53] WhatsApp, Inc. *Información para las fuerzas del orden. Testimonios*. Visto el 13 de febrero de 2018, a través del vínculo https://faq.whatsapp.com/es/general/26000050

[54] Suprema Corte de Justicia de la Nación. Primera Sala. *DERECHO A LA INVIOLABILIDAD DE LAS COMUNICACIONES PRIVADAS. SE IMPONE SÓLO FRENTE A TERCEROS AJENOS A LA COMUNICACIÓN.* Semanario Judicial de la Federación y su Gaceta. Libro XIX, Abril de 2013, Tomo I, Página 357, Décima Época.



En afán de no confundir a mi lector, es prudente señalar dos consideraciones: 1) El presente capítulo responde a la práctica y necesidad que se experimenta en los tribunales mexicanos, por lo que únicamente es la humilde propuesta del autor y 2) Este criterio no puede ser universalmente aceptado y aplicado para todos los sistemas de mensajería instantánea. A la fecha de redacción del presente capítulo, la plataforma *Google Play*, reporta que existen al menos 65 mil aplicaciones ("APK") diversas para emitir mensajes instantáneos de forma coordinada o no, por lo que es prudente acercarse a los términos y condiciones de cada una para comprender la naturaleza del sistema, de los mensajes de datos que ahí existen, el protocolo de cadeua de custodia más adecuada y con ello, determinar la ruta procesal más adecuada para su obtenciónu.

XII. 6 Conservación Forense de la Prueba Electrónica y Digital

Una de las mayores complicaciones en materia de ofrecimiento de pruebas electrónicas y digitales, es la conversación de las mismas hasta la etapa procesal adecuada para que el juez la tenga por desahogada en el proceso y pueda otorgarle una correcta valoración. El Departamento de Seguridad Nacional de los Estados Unidos de América fue consciente de esta complicación y no sólo se detuvo a crear dependencias que se encargaran de regular su ciberespacio, sino que permitió el perfeccionamiento de buenas prácticas para la cadena de custodia informática, para brindar uno de los sistemas de conservación forense más eficientes del orbe. En el año 2007, la División

de Investigaciones Criminales del Servicio Secreto de los Estados Unidos de América, publicó el documento intitulado *Best Practices for Seizing Electronic Evidence v.3. A Pocket Guide por First Responders*[55], derivado de la política de ciberseguridad sostenida por el Departamento *Homeland Security* ("DHS" por sus siglas en inglés). Éste surgió como una guía legal para reforzar al personal con mejores prácticas para la conservación de evidencia electrónica derivado de crímenes tecnológicos. La guía actualmente cuenta con una versión "4.2" y fija las reglas puntuales para asegurar una cadena de custodia transparente y brindar una adecuada conservación forense. Con la finalidad de evitar reproducir todo el documento, únicamente traduciré y fijaré las "Reglas de Oro" del documento, así como algunas sugerencias del mismo, respecto a principios que deben seguir los "Primo-respondientes" cuando enfrentan un delito en que intervinieron computadoras o tecnología electrónica, a saber:

Reglas de Oro

1. Siempre que sea posible, es mejor contar con un Perito entrenado Informático o Analista, para recabar la evidencia electrónica;
2. Contar con los fundamentos legales para conservar la computadora (hardware);
3. Si existen dudas razonables para creer que una computadora se involucra en una investigación criminal, esta debe preservarse como evidencia;
4. Si la computadora se encuentra apagada, debe permanecer apagada. No tratar de encenderla;
5. Si la computadora se encuentra encendida y no existe un perito disponible en la escena, debe asegurar adecuada la computadora y preservar la evidencia;
6. Si tiene creencias razonables que la computadora destruye evidencia, debe apagar la misma inmediatamente desde su centro de poder;
7. En todos los escenarios, se debe documentar la localización y estado de la computadora, incluido los medios electrónicos que incluya;
8. En todos los escenarios, se debe fotografiar la computadora, su ubicación y cualquier mecanismo adjunto. Se debe fotografiar la pantalla; y
9. Considerar la protección legal de documentos contenidos en el equipo (datos personales, información confidencial).

Por lo que refiere a la conversación de dispositivos que se encuentran conectados a una red, el Manual indica que se deberá recolectar no sólo el equipo, sino los datos relativos a la conexión, tales como: i) Dirección IP, ii) Puertos abiertos, iii) Conexiones a

[55] U.S.SECRETE SERVICE *Best Practices for Seizing Electronic Evidence v.3. A Pocket Guide For First Responders*. US Dept of Homeland Security. 2007. http://www.listcrime.com/BestPracticesforSeizingElectronicEvidence.pdf

la red activas, y iv) Cualquier dato que estime el perito. La identificación de los puertos, así como las conexiones abiertas permitirían la ubicación de personas involucradas en el crimen que se investiga. En términos generales, la "guía de bolsillo" dicta las pautas de una debida cadena de custodia para los primeros respondientes ante un hecho que involucre soportes electrónicos o digitales y hasta ahora, ha permitido que la políticas detrás del *FinCEN* se traduzca en la capacitación activa de todas sus unidades para actuar conforme lo dictan las buenas prácticas en informática forense. Sin embargo, ello no resuelve enteramente lo que podría ocurrir en la web y portales que se pudieran encontrar "colgados" con información ilegal o ilícita, en su totalidad o parcialmente.

En el caso mexicano, la Segunda Sala de la Suprema Corte de Justicia ha fijado un criterio no vinculante para las autoridades en el país, a través del cual se prescribe la posibilidad de "Bloqueo de una página electrónica (Internet) [sic]" siempre que esta almacene contenido ilegal, independientemente de la libertad de expresión que pudiere afectarse en el caso particular. A saber, la Tesis Aislada de referencia dicta:

> **BLOQUEO DE UNA PÁGINA ELECTRÓNICA (INTERNET). DICHA MEDIDA ÚNICAMENTE ESTÁ AUTORIZADA EN CASOS EXCEPCIONALES.**
> Como lo ha sostenido el Consejo de Derechos Humanos de la Organización de las Naciones Unidas, **el bloqueo de una página de Internet implica toda medida adoptada para impedir que determinados contenidos en línea lleguen a un usuario final**. Al respecto, debe tenerse en cuenta que las restricciones al derecho humano de libertad de expresión no deben ser excesivamente amplias, por el contrario, deben referirse a un contenido concreto; de ahí que las prohibiciones genéricas al funcionamiento de ciertos sitios y sistemas **web**, como lo es el bloqueo, son incompatibles con el derecho humano de libertad de expresión, salvo situaciones verdaderamente excepcionales, las cuales podrían generarse cuando los contenidos de una **página** de Internet se traduzcan en expresiones prohibidas, esto es, tipificadas como delitos acorde con el derecho penal internacional, dentro de las que destacan: (I) la incitación al terrorismo; (II) la apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia -difusión del "discurso de odio" por Internet-; (III) la instigación directa y pública a cometer genocidio; y (IV) la pornografía infantil. Asimismo, la situación de excepcionalidad a la prohibición de restricciones genéricas al derecho de expresión también podría generarse cuando la totalidad de los contenidos de una **página web** resulte ilegal, lo que lógicamente podría conducir a su bloqueo, al limitarse únicamente a albergar expresiones no permisibles por el marco jurídico.[56]

[56] SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. *Bloqueo de una página electrónica (Internet). Dicha medida únicamente está autorizada en casos excepcionales.* Segunda Sala. Tesis 2ª. CIV/2017. Décima Época. Gaceta del Semanario Judicial de la Federación. Libro 43, Junio de 2017, Tomo II, Página 1429. Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/ el 02 de diciembre de 2017.

En el caso colombiano, los tratadistas Deisy Yanet Acevedo Surmary (Universidad del Externado de Bogotá) y Élber Enrique Gómez Ustaris (Universidad Santo Tomás, Bogotá), realizan un brillante estudio sobre el comportamiento judicial en su país y la interacción que tienen con la Asociación Colombiana de Ingenieros en Sistemas (entidad que fija y establece las normas de procedimiento de investigación frente a documentos electrónicos). Sostienen su premisa en el entendido que el juez no es perito en todas las materias, por lo que para emitir una sentencia justa podría requerir del consejo de un asesor informático que cuente con habilidades suficientes para conservar la prueba, ayudar a las partes a su incorporación procesal y por último, brindar las reglas básicas para su valoración. Al respecto, el perito emitiría un dictamen que no sólo reconozca la calidad tecnológica de la prueba, sino que éste "certificará" que la misma se obtuvo de una debida cadena de custodia, e inmediatamente procederá a rendir su opinión crítica en un lenguaje que sea comprensivo para el juzgador, en el cual debe informar cual fue el diseño utilizado en la prueba, la metodología de extracción, la técnica de análisis, el estado del arte en ingeniería forense y las conclusiones del perito. El juez Colombiano que pretenda hacer uso de esta herramienta procesal –el dictamen- podrá acudir a ACIS. El dictamen contendrá datos de relevancia y pertinencia jurídica tales como la fecha de su creación, de modificación, el tipo de formato, del tamaño del documento electrónico, e igualmente, de identificar quién fue su creador y receptor y si fue o no encriptado, lo que permite comprobar la seguridad del mismo.[57]

Por lo que refiere a conservación forense de un correo electrónico, el Director Nacional de Tecnología de la Información, Santiago Acurio del Pino, brinda un adecuado análisis sobre la naturaleza del correo digital y recuerda al primer respondiente, que el mensaje/carta se almacena en un servidor del intermediario o prestador del servicio, siendo pocas las ocasiones que el usuario almacena éste en su propio equipo:

> Al enviar un correo electrónico, la computadora se identifica con una serie de números al sistema del proveedor de servicios de Internet (ISP). Enseguida se le asigna una dirección IP y es dividido en paquetes pequeños de información a través del protocolo TCP/IP. Los paquetes pasan por una computadora especial llamada servidor (server) que los fija con una identificación única (Message-ID) posteriormente los sellan con la fecha y hora de recepción (Sello de tiempo). Más tarde al momento del envió se examina su dirección de correo para ver si corresponde la dirección IP de alguna de las computadoras conectadas en una red local (dominio). Si no corresponde, envía los paquetes a otros servidores, hasta que encuentra al que reconoce la dirección como una computadora dentro de su dominio, y los dirigen a ella, es aquí donde los paquetes su

[57] ACEVEDO, Deysi y GÓMEZ, Élber. *Los documentos electrónicos y su valor probatorio: En procesos de carácter judicial.* IUSTITIA Número 9. Diciembre de 2011. ISSN: 1692-9403

> unen otra vez en su forma original a través del protocolo TCP/IP. (Protocolo de Control de Transferencia y Protocolo de Internet). Siendo visible su contenido a través de la interface gráfica del programa de correo electrónico instalado en la máquina destinataria. Hay que tomar en cuenta que los correos electróuicos se mantieuen sobre un servidor de correo, y no en la computadora del emisor o del destinatario, a menos que el operador los guarde allí. Al redactarlos se transmiten al servidor de correo para ser enviados. Al recibirlas, nuestra computadora hace una petición al Servidor de correo, para los mensajes sean transmitidos luego a la computadora del destinatario, donde el operador la puede guardar o leer y cerrar. Al cerrar sin guardar, la copia de la carta visualizada en la pantalla del destinatario desaparece, pero se mantiene en el servidor, hasta que el operador solicita que sea borrada.[58]

Empero, la conservación forense de las pruebas tecnológicamente avanzadas no puede detener su camino en el aseguramiento de mensajes, equipos o, en su caso, requerir el apoyo de expertos que cuenten con el conocimiento adecuado para preservar la prueba informática; ya que más allá del proceso, las personas involucradas (usuarios) cuentan con herramientas suficientes para lograr la desaparición de la evidencia digital, inclusive con su presencia física en prisión preventiva; así las cosas, el juez de la causa deberá tomar las medidas necesarias para obtener contraseñas y nombres de usuario (en carácter de confidencial) necesarios para evitar que estos pudieren ser utilizados en perjuicio del proceso, única y exclusivamente para los fines que ocupe al juicio. Por otro lado, no es absurdo pensar que las entidades prestadoras de servicios de telecomunicación, mensajería o redes sociales están obligadas a cooperar con las instrucciones de los juzgadores, por lo que refiere a la conservación de la prueba digital, en tanto que deberían realizar todas las acciones, humanas e informáticas, que permiten la supervivencia de la evidencia digital hasta que la misma se incorpore al proceso, independientemente del método que el juez hubiere preferido para desahogar la probanza. A efecto de lo anterior, no sólo el dictaminador deberá conocer el camino procesal adecuado para requerir a estas instituciones virtuales, sino que las partes y sus abogados, se obligan a informarse sobre el origen, domicilio, razón social y medios de contacto para agilizar su participación activa en el procedimiento y que coadyuven en la cadena de custodia de la evidencia informática, electrónica o digital, su conservación forense, la incorporación de ésta al proceso, su desahogo y finalmente, su valoración en términos de la legislación aplicable.

[58] ACURIO DEL PINO, Santiago. *Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0.* Dirección Nacional de Tecnología de la Información. *Organization of American States.* Washington, D.C. Visto el 04 de diciembre a través del vínculo https://www.oas.org/juridico/spanish/cyber/cyb47_manual_sp.pdf

A nivel internacional[59], parece que el caso normativo más exitoso es el que brinda la *Scientific Working Group On Digital Evidence*, quienes en el año de 1998 reunieron al sector comercial, académico y jurídico para generar una guía y estándares para recuperación, preservación y examen de evidencia digital. El grupo fundado por miembros activos del *Federal Bureau of Investigation (FBI)* y el Servicio Secreto de los Estados Unidos de América, Mark M. Pollit (ex Presidente) Maruy Horvath (actual Presidente) y James Darnell (Vicepresidente), respectivamente, cuenta con comités conformados por sus casi 100 y exclusivos miembros, para abarcar ciencias relativas al Audio Forense, Computación Forense, Generación de imágenes, fotografía, estándares de calidad, video, membrecías y programas fantasma. A pesar que su mayor fortaleza política y criminalística yace en la Unión Americana, el Grupo ha comenzado a obtener fuerza a nivel internacional, inclusive, ha permitido que generar manuales de buenas prácticas para el FBI y la Unión Europea en materia de "evidencia digital de programas de laboratorio". Alrededor del globo, los particulares y juzgadores podrían ocupar los estándares de este sector científico, únicamente remitiendo una solicitud por escrito a la mesa directiva o, en su caso, requerir apoyo de la SWGDE para que participe de forma activa en la conservación de la evidencia digital a través del correo electrónico secretary@swgde.org.; ésta última hipótesis, en caso de no contar en la jurisdicción con peritos capaces para la recuperación de pruebas informáticas. Por lo que refiere a sus guías y mejores prácticas, actualmente cuenta con más de 66 escritos que expresan los resultados de los congresos que han celebrado desde su origen, empero, destacan los siguientes documentos por su aporte a la ciencia y a la presente obra:

a) *Mejores prácticas para la adquisición de videos como evidencia digital o multimedia que se almacena en la Nube (Cloud)*[60].- De este documento se desprenden los diferentes tipos de nube a los que se pueden enfrentar las partes: i) Nubes configuradas exclusivamente para el dispositivo que transmitió el video; ii) Nubes con múltiples ubicaciones y un almacenamiento centralizado; que resulta útil en el caso de ser imposible obtener la evidencia del dispositivo en que se grabó el video; iii) Nubes de transferencia, que permite obtener el video gracias a sistemas de compartimiento como *Dropbox* ™ y Google Drive.

[59] Sin que resulte óbice al presente párrafo, la existencia del Convenio de Budapest, ya que éste cuenta con un breve apartado en materia de conservación forense de evidencia digital y únicamente constituye un código normativo para que los Estados parte adapten sus legislaciones locales.

[60] SWGDE. *Best practices for digital & multimedia evidence video acquisition from Cloud Storage*. Estados Unidos de América. Versión 1.0. Octubre 17 de 2017. Disponible en línea a través del vínculo https://www.swgde.org/documents/Released%20For%20Public%20Comment/SWGDE%20Best%20Practices%20for%20Digital%20and%20Multimedia%20Evidence%20Video%20Acquisition%20from%20Cloud%20Storage visto el 6 de diciembre de 2017.

a. La guía sugiere prioridades: i) Determinar la ubicación física del dispositivo que grabó el video; ii) Obtener autorización legal; iii) En caso de no conocer las funciones del sistema, contactar al proveedor; y iv) Determinar la fecha, tiempo, cámara de interés y cuántos datos son necesarios.

b) *Mejores prácticas para examinar dispositivos GPS portátiles*[61].- Dicha guía parte de la premisa de que el dispositivo fue obtenido adecuada y legalmente a través de la cadena de custodia, posteriormente, invita a "parear" (conectar con otro dispositivo) el GPS, de tal suerte que se pueda conocer su funcionalidad y eficacia. Desconectarlo de cualquier cable, antena o red *wi-fi*. Para realizar un mejor examen, la SWGDE sugiere que el aseguramiento del equipo debe ocurrir con cables, memorias y documentos que se encuentren con él o que formen parte de él, ya que en algunas ocasiones éste pudiere contener mecanismos de identificación infranqueables, sin los accesorios adecuados.

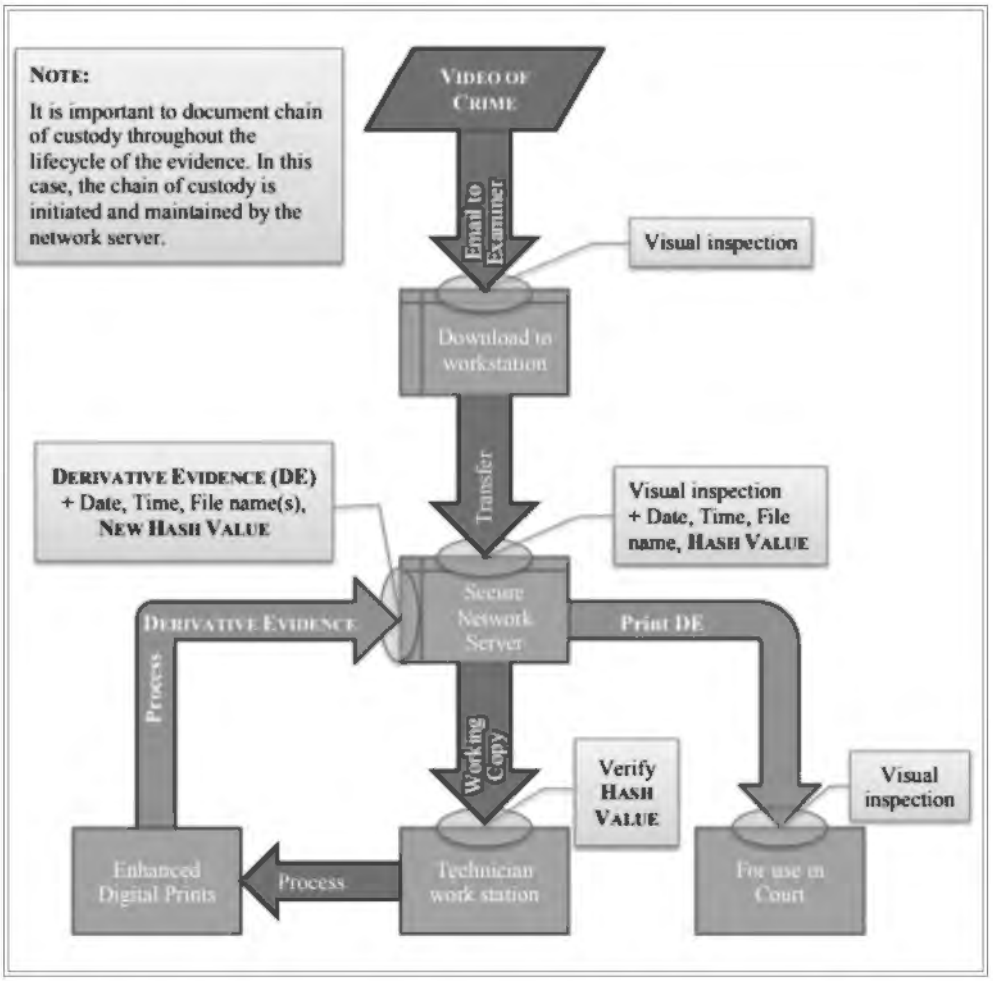
c) *Mejores prácticas para mantener la integridad de imágenes*[62].- La SWGDE es consciente de la importancia que tiene la "integridad" de una imagen, sobre todo de naturaleza digital, para ser incorporada a un proceso. Define "imagen" como la referencia o representación de un sujeto u objeto, que deriva de una imagen o video, digitales; asimismo, identifica cuatro etapas fundamentales en la conservación forense de este tipo de evidencia:

a. *Integridad de la imagen.*- La seguridad de que la imagen está completa e inalterada, desde el tiempo de la adquisición o generación al momento de su conservación. Al respecto, destaca la importancia de los metadatos que integran la imagen, los cuáles no son tan fácilmente eliminados de un equipo, pero sin los que sería imposible proveer la imagen al proceso
b. *Verificación de integridad.*- El proceso de confirmar que la imagen presentada está completa e inalterada, desde su adquisición hasta su generación;
c. *Autenticación.*- El proceso de sustraer el contenido de la imagen en un modelo representativo y adecuado para los fines del proceso sin alterar la integridad de la misma.
d. *Origen.*- Contar con una cadena de custodia que identifique el tiempo, lugar y motivo de la creación de la imagen.

[61] SWGDE. *Best practices for Portable GPS Device Examinations.* Estados Unidos de América. Versión 1.1. Septiembre 12 de 2012. Disponible en línea a través del vínculo https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Portable%20GPS%20Devices

[62] SWGDE. *Best practices for Maintaining the Integrity of Imagery.* Estados Unidos de América. Versión 1.1. Septiembre 12 de 2012. Disponible en línea a través del vínculo https://www.swgde.org/documents/Current%20Documents/SWGDE%20Best%20Practices%20for%20Portable%20GPS%20Devices

El grupo de científicos americanos también brinda guías y reglas básicas para la conservación de equipos telefónicos, *hardware* dañado, rastro de impresiones, autenticidad de impresiones que provengan de un dispositivo en particular y conservación de audio; asimismo, sugiere procesos de conservación que permitan una adecuada llegada de la evidencia digital a la corte; verbigracia, el referente a la valoración de videos que contengan hechos delictivos[63]:



Del diagrama que propone el grupo americano de peritos, se advierte la necesidad y suma importancia de la contar con servidor dedicado para la conservación forense de este tipo de evidencia digital; asimismo, la relevancia de contar con un grupo

[63] Supra. Cit. SWGDE.

policial o investigador debidamente capacitado en cadena de custodia digital; ya que la primera atención de la prueba podría determinar el valor o la carencia del mismo al ser valorado en la Corte.

En tenor de lo anteriormente expuesto, resulta meritorio citar al Maestro Oscar Manuel Lira Arteaga, Presidente de la Asociación Latinoamericana de Profesionales en Seguridad Informática, quien reconoce que los equipos de cómputo y las telecomunicaciones son uno de los mecanismos más populares, hoy en día, para conocer la existencia de un hecho delictivo, para cometerlo, planearlo y, en algunos casos, prevenirlo. Al respecto, propone que la criminalística, como ciencia forense que preserve los indicios digitales, podría intervenir en distintos niveles, según la tecnología aplicada[64]:

- Informática

  I. Identificación de acceso o uso no autorizado a equipos de cómputo
  II. Robo, alteración o copia de información contenida en equipos de cómputo
  III. Falsificación de documentos mediante equipos de cómputo
  IV. Ataques informáticos a servidores
  V. Robo de programas de cómputo
  VI. Identificación de correos electrónicos
  VII. Recuperación de información en dispositivos digitales de almacenamiento
  VIII. Ataques informáticos a redes de cómputo
  IX. Rastreo de servidores
  X. Recuperación de información publicada en Internet
  XI. Análisis de licitaciones, contratos en sistemas y equipos de cómputo
  XII. Clonación de bandas magnéticas o chips de tarjetas

- Telecomunicaciones

  I. Identificación de dispositivos o equipos de telecomunicaciones
  II. Recuperación de información almacenada en dispositivos
  III. Identificación de intervención de líneas telefónicas
  IV. Identificación de ataque o daño a una red de comunicación
  V. Identificación de robo de flujo electromagnético (TV, Cable)
  VI. Identificación de uso indebido de frecuencias de comunicación

[64] LIRA ARTEAGA, Óscar M. *Cibercriminalidad*. Instituto de Investigaciones Jurídicas. Instituto de Formación de la Procuraduría General de Justicia. México, 2012. Biblioteca Jurídica Virtual de la UNAM. Visto el 6 de diciembre de 2017, a través del vínculo https://archivos.juridicas.unam.mx/www/bjv/libros/7/3169/15.pdf

- Electrónica

  I. Identificación y funcionamiento de dispositivos electrónicos
  II. Identificación de principio y funcionamiento de circuitos electrónicos
  III. Análisis de diagramas esquemáticos
  IV. Alteración de cajeros automáticos

En lo esencial, el presente capítulo pretende brindar un panorama amplísimo sobre la posibilidad de incorporar pruebas electrónicas, informáticas o digitales a un proceso, gracias a la implementación de estándares y capacitación de las fuerzas forenses, sin los cuales, la prueba podría viciarse y resultar inútil para un juicio. Por otro lado, resulta evidente que las nuevas tecnologías podrían lucir fuera del alcance cognitivo de los juzgadores, empero, existen algunos elementos que forman parte de la cultura general e inclusive, que podrían calificarse como hechos notorios, que no provocarían la obligatoria presencia de un perito dentro del proceso, sin embargo, en caso que el Juez de turno requiera el consejo (dictamen) de alguno, es requisito *sine qua non* de la validez e integridad de la evidencia digital, que la misma sea obtenida por un perito capacitado y que tenga como apoyo estándares gubernamentales, los cuáles no existen en la mayoría de los casos.

XIII
CAPÍTULO

Delitos cibernéticos e informáticos

En septiembre de 2011, en Santa Ana, California, el hacker mexicano Luis Mijangos fue sentenciado por las autoridades federales del país americano, derivado de la implantación de un programa espía en al menos 100 computadoras, utilizadas por 230 personas, 44 menores entre ellas. Una vez que lograba tener el control de la computadora, extorsionaba a sus víctimas a través de amenazarles sobre divulgar información privada, sensible o bancaria, para evitar dicha difusión, los usuarios afectados debían enviar fotografías de índole sexual. Para junio de 2010 se logró el arresto del mexicano indocumentado y se le declaró culpable por los cargos de piratería cibernética, espionaje y ciber-terrorismo.[1] Algo similar ocurriría el pasado 6 de diciembre de 2017, cuando una corte en Suecia, condenó a Bjorn Samstrom a 10 años de prisión por haber abusado sexualmente de 27 menores de edad, a través de cámara web, bajo la amenaza de asesinar a seres queridos y publicar contenido en sitios web de pornografía. Algunos medios de comunicación no sólo trataron este hecho como "*sextorsión* online", sino como violación *on*

[1] *UNIVISION*. "Hacker mexicano condenado a seis años de cárcel por "sextorsión"". Medio Tiempo. Publicado el 01 de septiembre de 2011. Noticias. Visto el 7 de diciembre de 2017 a través del vínculo http://www.univision.com/noticias/hacker-mexicano-condenado-a-seis-anos-de-carcel-por-sextorsion

line, a pesar de no existir penetración o contacto físico.[2] Sin embargo, estas no son las únicas conductas que han generado complicaciones jurisdiccionales para los jueces encargados de resolver sobre la responsabilidad de los imputados. Quizá uno de los casos de mayor controversia a nivel mundial, es el de *Ross Ulbricht V. New York State*, también conocido como el caso de Silk Road y el Pirata Roberts; un proceso que tuviere inicio en 2011 con la detención del joven hacker, finalmente concluyó en mayo del 2017, cuando la Corte de apelación integrada por un panel de tres jueces, determinó que la pena de cadena perpetua resultó justa y emitida en estricto apego al Derecho; este precedente no sólo marcó las pautas de la existencia de la *Deep Web*, sino la compleja aplicación del derecho sobre un espacio en el que no se permite la intromisión gubernamental.[3] En referencia a la Deep Web, no sólo la venta de drogas y armas le ha ganado paupérrima reputación jurídica, sino la proliferación de grupos delictivos que atentan contra la esfera más delicada de la sociedad: La libertad sexual de los niños. Al respecto, ya existe preocupación de algunas naciones e instituciones especializadas en vigilancia cibernética para enfrentar a la red de pederastas que celebran cada 25 de abril, el *Día de Alicia (Alice's Day)*. Dicho festejo tiene su fundamento en el retorcido libro de Lewis Carrot, intitulado *Alicia en el país de las maravillas*. Así, cada 25 del mes de abril la *Deep Web* se transforma en el escenario perfecto para compartir pornografía infantil, videos de secuestros, trata de blancas y prostitución de menores; sin que en muchos de los casos, se tenga evidencia real sobre lo acontecido en esta capa oscura de la red. Por último, invocaré el hecho ocurrido el pasado mayo de 2017, cuando un grupo de piratas cibernéticos secuestraron los datos bancarios de millones de usuarios alrededor del mundo a través del software malicioso conocido como "*WannaCry*" y solicitaban el pago de US$300 dólares en *Bitcoin* para "desencriptar" los mismos. Las recomendaciones de las autoridades invitaban a no generar ningún pago, sin embargo, el miedo a perder datos confidenciales y de alto valor, llevó a gran parte de los cibernautas afectados a cumplir con la exigencia de los delincuentes.[4]

Por lo que refiere a los números detrás de los delitos que se comenten con uso de computadoras o programas de computadora, la Organización de los Estados

[2] *BBC MUNDO*. "El caso del primer hombre en el mundo condenado a prisión por "violación por Internet"". Redacción. 6 de diciembre de 2017. Visto el 7 de diciembre de 2017 a través del vínculo http://www.bbc.com/mundo/noticias-42252461

[3] GREENBERG, Andy. *Silk Road creator Ross Ulbricht Loses His Life Sentence Appeal*. WIRED. 31 de mayo de 2017. Visto el 7 de diciembre de 2017 a través del vínculo https://www.wired.com/2017/05/silk-road-creator-ross-ulbricht-loses-life-sentence-appeal/

[4] SYMANTEC SECURITY RESPONSE. *What you need to know about the WannaCry Ransomware*. Publicado el 23 de octubre de 2017. Visto el 9 de diciembre a través del vínculo https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

Americanos (OEA) en colaboración con la compañía *Symantec*™ estimaron para el 2014 que el cibercrimen ya costaba a América Latina al menos 113,000 millones de dólares, con un claro aumento para México de 113% en 2013 a 300%, no sólo por el aumento de hackers sino por la reducción en la brecha digital, lo que implica más usuarios y más dispositivos conectados a la red durante mayor cantidad de tiempo, lo que implica mayores amenazas y vulnerabilidades. Al respecto, el estudio *Tendencias de Seguridad Cibernética en América Latina y el Caribe*[5] permitió advertir las principales conductas criminales que ocurren en el ciberespacio: i) Violaciones de datos.- Más de 552 millones de identidades quedaron expuestas a causa de dichas violaciones, gracias al trabajo de *hacktivistas* y delincuentes; ii) *Spear-phising* (robo de identidad con objetivos específicos); iii) Estafas en redes sociales; iv) Troyanos bancarios consecuencia del *malware* dirigido a cajeros automáticos; v) Campañas de *malware* como "Darkmoon". Conforme a lo anterior, parece inconcuso que no sólo los costos comerciales deben generar alerta a las entidades gubernamentales que se encargan de la protección de los ciudadanos y cibernautas, sino que el creciente número de resoluciones judiciales que invocan desesperadamente la aparición de nuevos modelos de justicia que reconozcan las conductas delictivas que ocurren en la red, la forma de investigarlas y los mecanismos para prevenirlas.

XIII. 1 Aspectos epistemológicos y semánticos

En la mayor parte de los textos legislativos que estudiaremos en el presente capítulo, así como diversos doctrinarios de la materia ocupan de forma indistinta los conceptos de "ciberdelincuencia", "cibercrimen" y de forma más metódica, "delitos informáticos" y "delitos cibernéticos", empero, difícilmente se indica al lector el alcance de cada concepto, así como las consecuencias de Derecho que podrían conseguirse. En primer lugar, así como lo hemos manifestado en apartados diversos en la construcción de la presente obra, es meritorio recordar la diferencia entre Cibernética e Informática. El Doctor Julio Téllez, en su obra *Derecho Informático*, enfatiza el origen del vocablo "informática" como un neologismo que se funde de los términos "información" y "automatización", sugerido por primera vez por el Doctor Phillipe Dreyfus en el año 1962. A ésta se le conoce como "el conjunto de técnicas destinadas al tratamiento lógico y automático de la información para una mejor toma de

[5] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS/SYMANTEC. *Tendencias de seguridad cibernética en América Latina y el Caribe*. Publicado en junio de 2014. Visto el 9 de diciembre de 2017 a través del vínculo https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

decisiones"[6], a su vez, el Diccionario de la Real Academia Española la define [acepción 3) como el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras[7], por su lado, Mora y Molino cree que es la disciplina que dibuja los límite de las relaciones entre los medios, los datos y la información; y Mario Losano identifica a la informática como producto de la cibernética; corriente a la cual nos adherimos por el sentido tecnológico de la misma. Entonces, ¿podemos afirmar que la informática depende de la cibernética? Según el **Laboratorio de Cibernética,** con sede en Argentina, define a ésta como la ciencia interdisciplinaria que estudia el funcionamiento de las conexiones nerviosas en los seres vivos y los sistemas de comunicación, así como la regulación automática de los seres vivos con sistemas artificiales que simulan a los biológicos[8]; definición que parece consonante a la que brinda el Diccionario de la Real Academia Española, quienes la definen como la ciencia que estudia las analogías entre los sistemas de control y comunicación de los seres vivos y los de las máquinas.[9] A su vez, el Doctor Juan José Ríos Estavillo parecería brindar una composición de las aportaciones de Jagjit Sit y Neville Moray, al definirle como la inquisición interdisciplinaria hacia la naturaleza y base física de la inteligencia humana, con el propósito de reproducirla de forma sintética, asimismo, la considera la ciencia que relaciona las entradas y salidas del sistema, reconociendo dos conceptos fundamentales en su composición: comunicación y sistema.[10] Si bien es cierto, tratadistas como Fix Fierro reconocen que la informática es una ciencia integrada a la cibernética[11], se advierten diferencias substanciales que es meritorio invocar antes de avanzar en nuestro discurso:

[6] TÉLLEZ VALDÉS, Julio. *Derecho Informático.* Capítulo I. Fenómeno Informático. Editorial Mc Graw Hill. Segunda edición. México, 1998. Puede consultar el texto íntegro a través del vínculo https://biblio.juridicas.unam.mx/bjv/detalle-libro/1941-derecho-informatico visto el 29 de noviembre de 2017.

[7] Diccionario de la Real Academia Española. *Informática, co.* Definición. http://dle.rae.es/?id=LY8zQy3

[8] LABORATORIO DE CIBERNÉTICA. *Investigación y desarrollo en Procesamiento Inteligente de Señales.* Facultad de Ingeniería. Universidad Nacional de Entre Ríos. "Definición". Visto el 9 de diciembre de 2017 a través del vínculo http://www.bioingenieria.edu.ar/grupos/cibernetica/definicion.htm

[9] Diccionario Real Academia Española. *Cibernética, co.* Definición. http://dle.rae.es/?id=98YYoXW

[10] RÍOS ESTAVILLO, Juan José. *Derecho e Informática en México. Informática Jurídica y Derecho de la Informática.* Universidad Nacional Autónoma de México. México, 1997. Primera edición. Visto el 9 de diciembre de 2017 a través del vínculo https://biblio.juridicas.unam.mx/bjv/detalle-libro/147-derecho-e-informatica-en-mexico-informatica-juridica-y-derecho-de-la-informatica

[11] FIX FIERRO, Héctor y PONCE DE LEÓN, Luis. *Informática y documentación jurídica.* Boletín Mexicano de Derecho Comparado. Número 74. Instituto de Investigaciones Jurídicas. UNAM. México, Agosto 1992. Visto el 9 de diciembre de 2017 a través del vínculo https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/2965/3221

Cibernética	Informática
Se ocupa de los fenómenos de control y comunicación, lo que se traduce en la construcción de máquinas, inclusive de Inteligencia Artificial	Se ocupa de las tecnologías que desarrolla la cibernética, en lo relacionado a tratamiento, representación y manejo automático de la información.
Trata el empleo de métodos científicos para explicar fenómenos en la naturaleza o en la sociedad y la forma de representación del comportamiento humano de forma matemática en una máquina	Estudia las computadoras, sus principios básicos y utilización. Se ocupa de la programación, estructura de la información, lenguajes de programación, arquitectura de la computadora, así como ingeniería de software y hardware
Estudia la creación de instrumentos informáticos que simulen actividades del hombre	Es un instrumento de auxilio a la cibernética

En términos de las anteriores acepciones, parece prudente aseverar que la informática es una ciencia interdisciplinaria que pertenece a la cibernética; por lo que la primera únicamente podría operar como herramienta u objeto de auxilio para la segunda. En ese tenor, ¿qué es derecho informático y derecho cibernético? Siendo consecuentes con las anteriores definiciones, el propio Doctor Julio Téllez define al Derecho Informático como la rama de las ciencias jurídicas que contempla a la informática como instrumento (informática jurídica) y como objeto de estudio (derecho de la informática). A saber, nos resulta de utilidad la segunda división, a través de la cual el Doctor Téllez le define como "el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática".[12] Por su lado, el Diccionario Legal de Black, define al Derecho Cibernético, conforme su término en inglés "Cyberlaw", como el área de la ley que aplica a computadoras y a varias actividades relacionadas con Internet y conexiones. De esto se desprende la ausencia del término "derecho informático" en el sistema jurídico anglosajón, por lo que se debe ser paciente en la interpretación de textos en inglés que hablen al respecto. Por otro lado, podríamos definir al Derecho cibernético como el conjunto de normas jurídicas que regulan la interacción del hombre con la máquina, su construcción y las instrucciones que éste pudiere programar en ella; en el entendido, que en el momento que se estudie la automatización de dichas instrucciones, hablaremos estrictamente de Derecho Informático, para sistemas jurídicos latinoamericanos. Si bien es cierto, el *common law* brinda una salida semántica menos transitada, al prescindir de la "informática", el objeto del presente capítulo es pulir el lenguaje con el cual nos referimos a las conductas que se cometen en la red de redes o que tienen como objeto del ilícito, las computadoras.

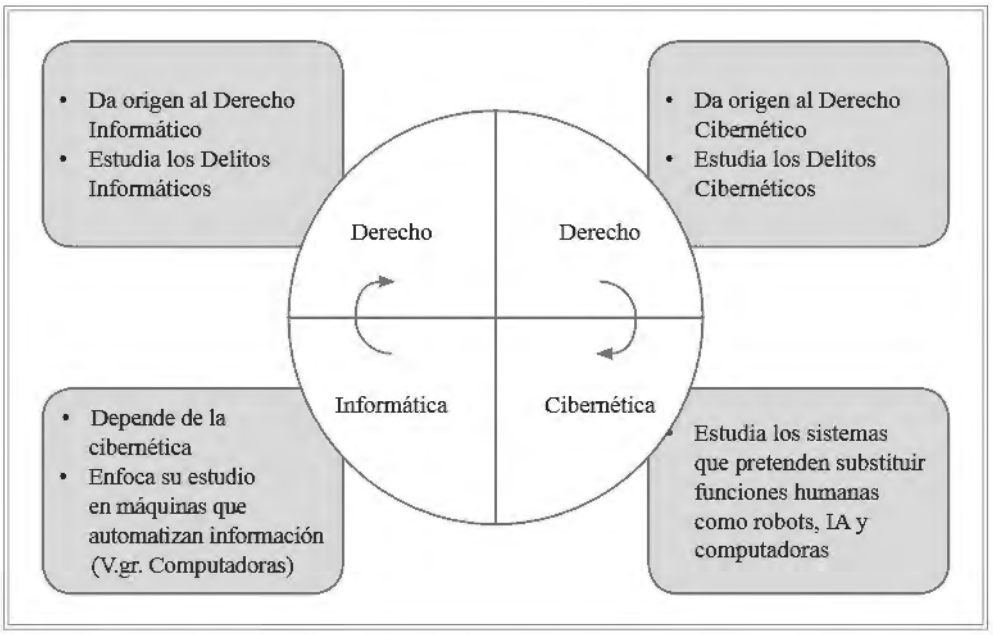
Hasta este punto, podemos afirmar que en los sistemas que se rigen por el *civil law*, tendrán la presencia de dos ramas del derecho interconectadas: Derecho

[12] Supra. Cit. Capítulo VIII. Derecho de la Informática en General.

cibernético y Derecho Informático; en tanto que los sistemas *common law* abarcan ambas ramas a través del concepto "Cyberlaw". En tenor de lo anterior, es prudente señalar que existirían diferencias entre los delitos cibernéticos e informáticos, no así en el universo anglosajón, por lo anteriormente referido. Los delitos cibernéticos estudian la fabricación, producción o concepción de máquinas, robots o inteligencia artificial que sirva para la comisión de conductas típicas, antijurídicas y antisociales, en tanto que los delitos informáticos son aquellos tipos penales que tienen su origen en un uso, tratamiento, disposición o manejo ilegal de la información automatizada a través de las computadoras.

No es óbice a las anteriores definiciones, precisar al lector que los conceptos de "ciberdelincuencia" o "cibercrimen", son resultado de desafortunadas traducciones de discursos anglosajones y aunque su uso se hubiese popularizado, no debería permitir confusión en los abogados digitales especializados.

Así las cosas, propongo al lector el siguiente esquema que permitiría advertir de forma más simple las acepciones que invocamos al presente parágrafo:



Una vez que tenemos claros los conceptos que deben ocupar el estudio jurídico, nos centraremos en definir las conductas que tienen mayor presencia en los diversos sistemas normativos, no sólo por vanguardia legislativa, sino porque las mismas ocupan un lugar de atención meritorio en su seguridad pública. Dentro de las conductas típicas, antijurídicas y antisociales que mayor presencia muestran en el derecho positivo podemos encontrar las siguientes:

- Acceso ilícito.- Se le considera como tipo penal al acceso sin autorización a un sistema informático, como consecuencia de la alteración o desactivación de un sistema de seguridad.

  – En el léxico digital podremos identificar este tipo penal a través de unodismos como "superzapping", que consiste en el uso no autorizado de programas de acceso universal o bien, "caballo de troya" que permite el acceso y codificación no autorizada. Ambas modalidades podrían provocar un concurso de delitos.

- Abuso de Dispositivos
- Daños causados a datos computarizados.- En términos generales, esta conducta ocurre gracias a las herramientas conocidas como *Malware (malicious software)*. Según el glosario en línea de Panda Security, se les define como "cualquier programa, documento o mensaje, susceptible de causar perjuicio a los usuarios de sistemas informáticos"[13].
- Distribución de virus informáticos
- Falsificación Informática.- Es imperativo considerar esta modalidad bajo las consecuencias que tuviere en el ámbito tradicional, ya que diversas legislaciones, así como el Consejo Europeo, consideran que se comete esta conducta por el aporte de datos, alteración, tachaduras o supresión de datos computarizados o programas de informática, siempre que las condiciones constituyan un delito de falsificación, cuando sea cometido en conexión a un objeto tradicional de tal delito.

  – En el léxico digital, esta conducta tiene su origen en usurpación de identidad digital (*phishing*).

- Fraude Informático.- Según el consejo europeo, se le considera al aporte de datos, alteración, tachaduras o supresión de datos computarizados o programas de informática, o cualquier otra interferencia durante el proceso de datos, que provoque pérdidas económicas o morales, con el objeto de obtener ganancia financiera ilegal, para sí o para terceros.

  – En el léxico digital, esta conducta tiene su origen en programas maliciosos o mensajes de datos que llevan al error y confusión al usuario, como en caso del *vhishing*; hipótesis en la que el usuario brinda información real a

[13] PS.S.L. *Panda Security*. 2013. Recuperado de: http://www.pandasecurity.com/spain/homeusers/security-info/glossary

un tercero que se ostenta como responsable o encargado del tratamiento de sus datos.

- Interceptación ilícita

  – En el léxico digital, se puede estudiar como "*botnets*". Consiste en el acto informático que permite acceso remoto de equipos o usuarios infectados. Asimismo, entra en esta categoría la conducta conocida como "*Spyware*"; misma que consiste en la recopilación ilegal de datos personales y envío a un tercero, sin consentimiento del titular.

- Interferencia en los datos.- Implica la infección y posterior encriptación de los datos de un sistema informático a través de un tipo de *Malware*. A este tipo de modalidad se le conoce como *Ransomware*. Según el glosario de definiciones de *Panda Security*, éste es un software malicioso que al infectar el equipo le da al ciberdelincuente la capacidad de bloquear un dispositivo desde una ubicación remota y encriptar los datos del equipo. De forma general, lanza una ventana emergente que exige el pago de un rescate, que se suele realizar en moneda virtual (V.gr. Bitcoin)[14]. En muchas ocasiones, la infección ocurre a través de un *Click-Bait*.
- Interferencia en el sistema
- Pornografía Infantil

  – Si bien esta conducta pertenece al ámbito tradicional, tiene graves repercusiones en el universo digital. En particular, el *Cibergrooming* se considera el método que los pederastas usan para contactar con menores de edad, en redes sociales, para después provocar encuentros sexuales en línea.

- Tráfico de claves informáticas
- Uso o Reproducción no autorizada de un programa informático.- Consiste en la conducta que atente contra los términos de la protección legal de la cual goza el programa de cómputo, siempre que no se encuentre en los estados de excepción para uso libre y gratuito que conceden las reglas del Derecho Internacional en materia de propiedad intelectual
- Uso no autorizado de una computadora.- *Per se*, podría considerarse un delito de índole cibernética, sin embargo, éste debe estudiarse en atención a los fines para los cuáles se utilizó y si en su caso, interviene el uso indebido de

[14] PANDA SECURITY, S.L. ¿Qué es un Ransomware? Malware. Mobile News. Noviembre 15 de 2013. Visto el 9 de diciembre de 2017 a través del vínculo https://www.pandasecurity.com/spain/mediacenter/malware/que-es-un-ransomware/

información, en cuyo caso, podría existir un concurso de delitos en materia cibernética e informática.

Independientemente del anterior listado, algunos tratadistas como Juan Diego Castro Fernández o el Doctor Oscar Manuel Lira, creen que los delitos informáticos se pueden adecuar a figuras tipificadas en el Código Penal Positivo, indicando los bienes jurídicamente afectados, lo que haría innecesaria la presencia de hipótesis delictivas digitales. A saber:

- Delitos contra las personas.- Conductas que realicen un mal uso de la Información que obre en registros computarizados que generen afectación en la vida o salud de las personas
- Delitos contra el honor.- Actos que podrían englobar por el uso de información automatizada que vulnere la dignidad, decoro, honra o reputación, independientemente del mecanismo informático que se ocupe para ello;
- Delitos contra la propiedad.- El Doctor Castro Fernández considera que gran parte de las afectaciones informáticas ocurren bajo las modalidades legislativas que los Códigos Penales establezcan para la protección de la propiedad.

Adquiere fortaleza la postura de los tratadistas que cito, en conductas como el ***Sexting*** y ***Ciberbullying,*** conductas que *per* se pueden vigilar su reparación en el universo del derecho tradicional en alguna de las hipótesis que antes reproduje, siempre que efectivamente exista un bien jurídico tutelado vulnerado, ya que el "sexo *on line*", así como las "intimidaciones" no suelen ser considerados como tipos penales a *prima facie*, independientemente de las consideraciones y agravantes que pudieren existir en cada hipótesis como lo es el ***"sexting revenge*** o **<<sextorsión>>".**

Tal como expresé con anterioridad, estas conductas se estudian de forma general y sin distinción de rama del Derecho, en sistemas *common law*, en cuyos países prefieren englobar el tratamiento de estos tipos penales en el *Cyberlaw* y así dirigir conductas precisas en contra de los "*cybercrimes*". En ese tenor, es que gran parte de los Tratados Internacionales y lectura de derecho comparado, prefiere el término de Delitos Cibernéticos, tal como el cuerpo normativo internacional que se estudiará a continuación.

XIII. 2 Legislación Internacional

El 23 de noviembre del año 2001, el Consejo de la Unión Europea tuvo clara la necesidad de homologar legislaciones en las diversas naciones que lo conforman, como medida de combate en contra de la "ciberdelincuencia" y permitir medios eficaces de investigación en materia de delitos informáticos. Ese mes y año se abrió

la Convención de Budapest sobre Ciberdelitos (*Convention on Cybercrimes)*[15] para incorporar a los países miembros del consejo y a otro no miembros, hasta el primero de junio de 2004 cuando finalmente entró en vigor. Se le considera el primer tratado internacional en estudiar los crímenes que se cometen gracias a Internet y las diversas conexiones de computadoras, para evitar violaciones en materia de derechos de autor, fraude computacional, pornografía infantil y violaciones a la seguridad de las redes. Su objeto principal es generar una política criminal común para proteger a la sociedad en contra del cibercrimen, especialmente, mediante la adopción de legislación apropiada y permitir la cooperación internacional. Este Tratado se compone de 48 artículos e invita a la legislación local, de al menos nueve tipos penales identificados por la Convención:

1. Acceso Ilícito (Artículo 2 de la Convención). Lo define cómo: "…el acceso deliberado o ilegítimo a todo o parte de un sistema informático…con la intención de obtener datos informáticos y otra intención delictiva…".

    a. Delito contra la confidencialidad, la iutegridad y la disponibilidad de los datos y sistemas informáticos

2. Interceptación Ilícita (Artículo 3 de la Convención). Lo define cómo: "…la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático…".

    a. Delito contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

3. Ataques a la integridad de los datos (Artículo 4 de la Convención). Lo define cómo: "…todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos…".

    a. Delito contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

4. Ataques a la integridad del sistema (Artículo 5 de la Convención). Lo define cómo: "…la obstaculización grave, deliberada e ilegítima del funcionamiento

[15] CONSEJO EUROPEO. *Convenio Sobre la Ciberdelincuencia.* Budapest, 23 de noviembre de 2001. Texto en español a través del vínculo https://rm.coe.int/16802fa41c Puede consultar el texto oficial en inglés, a través del vínculo https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561; ambos vistos el 9 de diciembre de 2017.

de un sistema informático mediante la introducción…alteración o supresión de datos informáticos…".

a. Delito contra la confidencialidad, la iutegridad y la disponibilidad de los datos y sistemas informáticos

5. Abuso de dispositivos (Artículo 5 de la Convención). Lo define como la enajenación o puesta a disposición de un dispositivo, medio informático o contraseñas que permiten acceso total o en parte a un sistema informático o bien para cometer cualquiera de los anteriores cuatro tipos penales. La posesión de dicho dispositivo o contraseña también es considerado dentro de esta hipótesis normativa.

a. Delito contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

6. Falsificación Informática (Artículo 6 de la Convención).- Lo define cómo: "… la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos…"

a. Delito informático

7. Fraude informático (Artículo 7 de la Convención).- Lo define cómo: "…los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante falsificación informática o interferencia en el funcionamiento del sistema informático…".

a. Delito informático

8. Delitos relacionados con la pornografía infantil (Artículo 9 de la Convención). En general, lo podemos definir como la producción, oferta, difusión, transmisión, adquisición o posesión de pornografía infantil en un sistema informático.
9. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (Artículo 10 de la Convención). A saber del Consejo Europeo, constituyen delitos en contra de la PI, aquellos actos que se cometen deliberadamente, a escala comercial y por medio de un sistema informático, que atenten en contra de los derechos consagrados en el Convenio de Berna (Acta de París de 24 de julio de 1971); el Tratado de la OMPI sobre Derecho de Autor; la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión

(Convención de Roma); el Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio; y el Tratado de la IMPI sobre interpretación o ejecución y fonogramas.

El Tratado que nos ocupa también reconoce la posibilidad de sancionar la tentativa, la complicidad y designar responsabilidad a las personas jurídicas/morales. Asimismo, destaca que brinda al menos 3 categorías de delitos cibernéticos: i) Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, ii) ***Delitos Informáticos en sentido estricto***, y iii) Delitos por su contenido.

En un ejercicio legislativo similar, la Secretaría General del *Commonweatlh* publicó en octubre de 2002 la Ley Modelo para crímenes relacionados con computadoras y crímenes computacionales (*Model Law On Computer And Computer Related Crime)*[16], la cual incluye tipos penales similares a los del Convenio de Budapest, pero destaca en las reglas de preservación de evidencia digital y una política de cooperación internacional en materia de conservación forense de los datos informáticos. A nivel institucional, no sólo la Unión Europea ha forjado su camino a través del Convenio de Budapest. En el caso de América, independientemente del esfuerzo local que cada Estado realiza, la Organización de los Estados Americanos construyó el Portal Interamericano de Cooperación en materia de Delito Cibernético y de vuelta al viejo continente, en Ucrania existe un esfuerzo colosal por parte de un grupo no gubernamental de investigadores que se denominan *Computer Crime Research Center About Computer Crime Research*, quienes cuentan con una de las bases de datos más grandes de la web por lo que refiere a noticias de relevancia y legislación en materia de Delitos Cibernéticos.

XIII. 3 Marcos jurídicos nacionales sobre delitos cibernéticos e informáticos

Una vez que hemos definido los alcances internacionales del Convenio de Budapest, inclusive la posibilidad de ingreso para países no miembros de la Unión Europea, deberemos atender al tratamiento que han brindado algunos Estados Nación, referente a delitos cibernéticos e informáticos. Al respecto, es meritorio mencionar que el derecho positivo parece no mantener una línea homogénea respecto de las definiciones que se deben ocupar en este rubro, sin embargo, las conductas apuntan a similitudes

[16] COMMONWEALTH SECRETARIAT. *Model La won Computer and Computer Related Crime.* Vista el 9 de diciembre de 2017 a través del vínculo http://www.thecommonwealth-ilibrary.org/commonwealth/governance/2002-meeting-of-commonwealth-law-ministers-and-senior-officials/model-law-on-computer-and-computer-related-crime_9781848598188-16-en

sustantivas en cada Estado. Para brindar un panorama, relativamente breve, nos remitiremos al compendio que brinda la Organización de Estados Americanos (*Organization of American States)* y, en su caso, nos enfocaremos en legislación de orden penal/criminal, así como algunas referencias a leyes administrativas que contemplan tipos penales relativos a conductas de cibercrímenes o delitos informáticos.

- **México.**- La *OAS* reconoce el trabajo del Estado mexicano en la regulación de conductas que castigan los cibercrímenes, así como referencias en leyes diversas como la Ley de Propiedad Industrial, Ley de Vías Generales de Comunicación, Ley de Instituciones de Crédito, Ley Federal del Derecho de Autor y Ley Federal de Comunicaciones, sin embargo, todo apunta a una correcta (aunque breve) aproximación a los delitos informáticos en los artículos 200, 211 bis, 211 bis 1, 211 bis 2, 211 bis 3, 211 bis 4 y 211 bis 5, del Código Penal Federal, mismos que de tenor literal prescriben:

  – Artículo 211 bis. A quien revele, divulgue o utilice indebidamente o en perjuicio de otro, información o imágenes obtenidas en una intervención de comunicación privada, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa. Artículo 211 bis 1. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa. Artículo 211 bis 2. Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa. Artículo 211 bis 3. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de dos a ocho años de prisión y de trescientos a novecientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática del Estado, indebidamente copie información que contengan, se le impondrán de uno a cuatro años de prisión y de ciento cincuenta a cuatrocientos cincuenta días multa. Artículo 211 bis 4. Al que sin autorización modifique, destruya o provoque pérdida

de información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática de las instituciones que integran el sistema financiero, protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Artículo 211 bis 5. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente modifique, destruya o provoque pérdida de información que contengan, se le impondrán de seis meses a cuatro años de prisión y de cien a seiscientos días multa. Al que estando autorizado para acceder a sistemas y equipos de informática de las instituciones que integran el sistema financiero, indebidamente copie información que contengan, se le impondrán de tres meses a dos años de prisión y de cincuenta a trescientos días multa. Las penas previstas en este artículo se incrementarán en una mitad cuando las conductas sean cometidas por funcionarios o empleados de las instituciones que integran el sistema financiero.

- **Es meritorio señalar que México es observador permanente del Convenio de Budapest, que se estudió con anterioridad.**

- **Antigua y Barbuda.**- El país de referencia no sólo cuenta con previsiones específicas en materia de "crímenes electrónicos", como acceso ilegal, intercepción, interferencia de datos y sistemas, sino que ha creado una progresiva y eficiente legislación preventiva en materia de pornografía infantil; sino que ha designado un marco normativo exclusivo para los tipos penales cibernéticos y, en su caso, para la investigación y procesamiento de los mismos, en términos de su "Electronic Crimes Act, 2013".
- **Argentina.**- La ley 11.179 que reforma el Código Penal de la Nación, así como las modificaciones a través de la Ley 26.388 insertan al marco normativo argentino los siguientes tipos: Acceso ilícito, Intercepción Ilícita, Interferencia de Datos, Interferencia de Sistemas, Abuso de los Dispositivos, Falsificación Informática, Fraude Informático, Pornografía Infantil e Infracciones de Propiedad Intelectual y derechos afines.
- **Las Bahamas.**- El acta "Computer Misuse"[17] de 2003 es un documento que contiene provisiones en materia de seguridad computacional, en contra de accesos no autorizados, para modificaciones o conexiones ilegales. Al respecto,

[17] LAS BAHAMAS. *Computer Misuse Act 2003.* Aprobada el 11 de abril de 2003 y entrada en vigor el 16 de junio del mismo año. Vista el 7 de diciembre de 2017 a través del vínculo http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf

tipifica el acceso ilegal, intercepción ilegal, interferencia de datos, interferencia de sistemas y fraudes computacionales. Dicha Acta también incluye las reglas procesales para su substanciación en juicio.

- **Barbados.**- La ley de Barbados que resulta aplicable a los delitos cibernéticos es la conocida como "Computer Misuse Act, 2005-4"[18]. La cual fija los malos usos de las computadoras a través de catorce conductas prohibidas: Comunicaciones maliciosas, pornografía infantil, Acceso no autorizado a programas de computadoras o datos, Ofensas relativas a sistemas de computadoras restringidos, Revelación no autorizada de códigos de acceso, Acceso con intención de ofensa, Dispositivos ilegales (uso de), Intercepción ilegal de datos, interferir con programas computacionales, interferir con datos y acceso ilegal.
- **Belice.**- Esta Nación sólo tiene provisiones específicas en materia de intercepciones ilegales, contenida en la sección 3, 4 y 13 del Acta número 25 del 2010.
- **Bolivia.**- El código penal del Estado boliviano prevé la figura de manipulación informática y alteración, acceso y uso indebido de datos informáticos, en términos de los artículos 363 bis y 363 ter. Esto en su capítulo XI denominado "Delitos Informáticos". Éste se incorporó al Código Penal a través de la Ley 1768 del 10 de marzo de 1997.[19]
- **Canadá.**- El gobierno canadiense cuenta con un "Criminal Code"[20] que prohíbe, sanciona y dicta las reglas de persecución de ciertas conductas típicas, antijurídicas y antisociales. En lo particular, sus artículos 163, 183, 184, 318, 319, 322 y 430, regulan lo respectivo a pornografía infantil, intercepción de comunicaciones, propaganda de odio y su publicación digital, robo a través de un sistema de computadora y mal uso de datos de computadora (destrucción, reproducción no autorizada u obstrucción [interrupción o interferencia]), respectivamente.
- **Chile.**- El país andino promulgó la Ley número 19.223 relativa a Delitos Cibernéticos/Informáticos[21], el 28 de mayo de 1993. En este ordenamiento se tipifican conductas relativas a la informática. Únicamente incluye cuatro artículos que prohíben el acceso ilícito, la intercepción ilícita, la interferencia

[18] GOVERNMENT OF BARBADOS. *Computer Misuse Act 2005.* Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_bbs_computer_misuse_2005.pdf

[19] BOLIVIA. *Código Penal aprobado por DL 10426 de 23/08/1972, elevada al rango de Ley por Ley 1768 de 10/03/1997.* Vigente a partir del año 1973. Visto el 7 de diciembre de 2017 a través del vínculo https://bolivia.infoleyes.com/norma/1401/codigo-penal-cp

[20] CANADÁ. *Criminal Code R.S.C. 1985.* Con enmienda del pasado 18 de octubre de 2017. Visto el 7 de diciembre de 2017 a través del vínculo http://laws-lois.justice.gc.ca/eng/acts/C-46/

[21] Congreso Nacional de Chile. *Ley 19223.* Biblioteca del Congreso Nacional. Promulgada el 28 de mayo de 1993 y publicada el 7 de junio del mismo año por el Ministerio de Justicia. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_chi_ley_19223.pdf

de datos e interferencia de sistemas. Lo relacionado con pornografía infantil ocupa su propio espacio en el Código Penal, artículos 366 quinquies y 374 bis.

- **Colombia.-** Este país se destaca por no sólo regular de forma sustantiva los delitos informáticos y cibernéticos, sino por brindar reglas de cadena de custodia y procesales para un debido estudio en juicio. Por lo que refiere a lo último, cuenta con un procedimiento para investigación de delitos informáticos en el Código de Procedimientos Penales Ley 906 de 2004, asimismo, regula la orden de presentación, registro y confiscación de datos informáticos almacenados, específicamente en los artículos 236 y 244 del propio ordenamiento procesal. Por lo que refiere a la parte sustantiva, el Estado colombiano promulgó la Ley 1273 del 5 de enero de 2009, por la que se modifica el Código Penal para insertar un nuevo bien jurídico tutelado conocido como "protección de la información y de los datos". Específicamente, incorpora a su código los tipos relacionados con Acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales, hurto por medios informáticos y semejantes y transferencia no consentida de activos.[22]
- **Costa Rica.-** Así como lo fue el caso colombiano, este país cuenta con reglas sustantivas, procesales y forenses en materia de delitos informáticos. Por lo que refiere a las últimas, los artículos 198 y 199 del Código Procesal Penal y primero de la Ley sobre Registro, Secuestro y Examen de documentos privados e intervención de las comunicaciones, contiene las reglas para una cadena de custodia legal y transparente. En materia sustantiva, el Código Penal Nacional tipifica la interceptación ilícita, interferencia de datos, interferencia en el sisteua, falsificación informática y fraude informático.
- **Ecuador.-** En el caso de esta Nación, no cuenta con una disposición enteramente de carácter criminal como se expuso en casos anteriores, al respecto, su Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos Número 2002.67[23] incluye disposiciones específicas en materia de delitos informáticos, tales como acceso ilícito, interferencia de datos, interferencia en el sistema, abuso de dispositivos, falsificación informática, fraude informático y pornografía infantil. A saber del lector, es meritorio destacar que esta ley tiene

[22] REPÚBLICA DE COLOMBIA/ GOBIERNO NACIONAL. *Ley 1273/2009.* Bogotá, 5 de enero de 2009. Ministerio del Interior y Justicia. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_col_ley1273.pdf

[23] CONGRESO NACIONAL DE ECUADOR. *Ley de comercio electrónico, firmas electrónicas y mensajes de datos (Ley 2002-67).* Registro oficial 557-S, 17-IV-2002. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf

como base la Ley Modelo UNCITRAL que se mencionó con anterioridad, en el cuerpo de la presente obra.

- **El Salvador.**- Las cinco conductas típicas y antijurídicas que existen en esta nación se prohíben en el Código Penal de la Nación. Tipifica conductas de acceso ilícito, interferencia de datos, interferencia en el sistema, fraude informático y pornografía infantil.
- **Estados Unidos de América.**- Éste podría ser el caso normativo más extenso por lo que refiere a su regulación sustantiva, procesal e institucional. Al respecto, el título 18 del Código Criminal Federal de los Estados Unidos[24] contiene provisiones específicas relacionadas con acceso ilegal, intercepción ilegal, interferencia de datos, interferencia de sistemas, mal uso de dispositivos, robo de identidad, fraude computacional y pornografía infantil. Adicionalmente, dicta las reglas para la intercepción de comunicaciones aéreas, orales y electrónicas y reglas para preservación y obtención de comunicaciones archivadas. Mención aparte son las infracciones que pudieren cometerse en materia de derechos de autor y derechos conexos, debido al mal uso de sistemas y programas computacionales, también regulado en el título 18 del Código Criminal Federal.
- **Guyana.**- Al respecto, esta Nación únicamente tipifica la intercepción ilegal de comunicaciones y regula la intercepción necesaria para procedimientos de orden penal, a través de su Acta Número 21 el 2008.[25]
- **Honduras.**- Su código Penal Nacional tipifica las conductas relativas a la interferencia de datos y abuso de dispositivos.
- **Jamaica.**- El Acta 2010 sobre Cibercrímenes[26] contiene provisiones específicas sobre acceso ilegal, interferencia de datos, interferencia de sistemas, mal uso de dispositivos, falsificación relacionada con computadoras y pornografía infantil. Este ordenamiento también contiene las reglas procesales para incorporar evidencia digital, así como las pautas de la cadena de custodia.
- **Nicaragua.**- Los artículos 175, 197, 198, 229, 245, 246 y 275 del Código Penal del Estado de Nicaragua contienen prohibiciones específicas respecto al acceso ilícito, interferencia de datos, pornografía infantil, fraude informático y falsificación informática.

[24] ESTADOS UNIDOS DE AMÉRICA. *U.S. Code Part I- Crimes- Title 18.* Vista el 7 de diciembre de 2017 a través del vínculo https://www.law.cornell.edu/uscode/text/18/part-I

[25] GUYANA. *Interception of communication Act 2008.* Acta 21 de 2008. Autorizado por la Asamblea Nacional el 17 de octubre de 2008. Vista el 7 de diciembre a través del vínculo http://www.oas.org/juridico/mla/en/guy/en_guy_Inter_Commun_Act_2008.pdf

[26] JAMAICA. *Acta 2010 sobre Cibercrímenes.* Aprobada por la casa de representantes el 16 de febrero de 2010. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/PDFs/jam_act2010.pdf

- **Panamá.**- El código penal panameño prohíbe conductas relacionadas con delitos informáticos, a saber, el acceso ilícito, interceptación ilícita, interferencia en el sistema, falsificación informática, fraude informático y pornografía infantil. A su vez, el Código Judicial del país determina las reglas del procedimiento para la investigación de este tipo de delitos, así mismo, fija normas para el registro y confiscación de datos informáticos almacenados.
- **Paraguay.**- Además de regular las conductas infractoras en materia de derechos de autor y derechos conexos (Código Penal), la Ley 1160/97 incorporó al Código Penal Paraguayo[27] las conductas relativas a delitos informáticos. Específicamente, se prohíbe y sanciona la interceptación ilícita, interferencia en los datos, interferencia en el sistema, falsificación informática, fraude informático y pornografía infantil. Adicionalmente, mediante Ley número 2861/2001 sobre represión del comercio y difusión comercial de material pornográfico, utilizando la imagen u otra representación de menores o incapaces, Paraguay pretende fijar las políticas públicas y policiales para evitar la comisión de este tipo de conductas.
- **Perú.**- La Ley 30096 sobre Delitos Informáticos incorpora al sistema normativo peruano las conductas de acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema, abuso de los dispositivos, falsificación informática, fraude informático, pornografía infantil e infracciones en materia de propiedad intelectual.
- **República Dominicana.**- Su Ley 53-07 sobre Crímenes y Delitos de Alta Tecnología[28] prescriben sanciones a aquéllos que cometan conductas relativas al acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema, abuso de dispositivos, falsificación informática, fraude informático, pornografía infantil e infracciones en materia de Propiedad Intelectual.
- **Sant Kitts y Nevis.**- Esta Nación cuenta con un Acta sobre delitos electrónicos de 2009, que tipifica el acceso ilegal, interceptación ilegal, interferencia de datos, interferencia de sistemas, abuso de dispositivos y pornografía infantil. Asimismo, existen provisiones relativas a la obtención y conservación de evidencia digital.
- **Santa Lucía.**- Tipifica los fraudes computacionales y la pornografía infantil a través de su código criminal.

[27] PARAGUAY. *Código Penal de Paraguay Ley 1.160/97.* Visto el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_par_cod_penal.pdf

[28] REPÚBLICA DOMINICANA. *Ley 53-07 Crímenes y delitos de alta tecnología.* Promulgada el 23 de abril de 2007 por el presidente Leonel Fernández. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

- **San Vicente y Granadinas**[29].- El acta 2007 sobre Transacciones Electrónicas tipifica delitos informáticos relativos al acceso ilegal, interceptación ilegal, interferencia de datos, interferencia de sistemas, abuso de dispositivos, fraude computacional, pornografía infantil e infracciones relativas a derechos de autor.
- **Uruguay.**- A pesar de no contar con regulación en materia de cibercriminalidad, sí estudia la posibilidad que se cometan conductas a través de medios tecnológicos en perjuicio de la integridad sexual, en particular, aquella de los niños.
- **Venezuela.**- A través de la Gaceta Oficial de la República Bolivariana de Venezuela se publicó la Ley Especial Contra Delitos Informáticos, a través de la cual se prohíben conductas de acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema, abuso de dispositivos, falsificación informática, fraude informático y pornografía infantil.[30]

XIII. 4 Mejores prácticas

El estudio profundo y jurídico de las conductas delictivas que ocurren en el ciberespacio o con el auxilio de un ordenador, no bastará para enfrentar el alza en sus números y que los estudios recientes apunten a aumentos insospechados frente a los delitos de orden tradicional/material. Al respecto, los gobiernos deberán implementar un conjunto de "Mejores prácticas" que se conviertan en reglas de conducta en sus ciudadanos cibernautas y que resulten tan naturales como respirar, comer y vestir. A saber, la compañía desarrolladora *Symantec* ™ brinda algunas reglas que podrían considerarse valiosas como medida que combate la delincuencia informática y cibernética, no sólo como mecanismo gubernamental, sino como actuar individualizado.

1. Estrategias de defensa profunda.- En muchas ocasiones, el usuario pretende evitar instalar sistemas de protección en sus computadores para no afectar el rendimiento de sus equipos sin saber que ello podría colocarlo en un alto índice de vulnerabilidad. Al respecto, es recomendable contar con *firewalls* actualizados, antivirus vigentes, sistemas de detección de intrusiones y programas de escaneo de vulnerabilidades de sitios web. Estos sistemas deberán colaborar de forma paralela y superpuesta.

[29] SAINT VINCENT AND THE GRENADINES. *Electronic Transactions Act 2007.* Aprobada por la asamblea de representantes en 2007. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_svg_electronic_act_2007.pdf

[30] VENEZUELA. *Ley Especial contra los delitos informáticos.* Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_ven_LEY%20ESP_CON_DELI_INFOR.pdf

2. Monitoreo para detección de intentos de incursión en la red, vulnerabilidades y abuso de marca.- La consulta periódica a revistas especializadas podría significar la diferencia entre contar con un equipo protegido y uno efectivamente vulnerable. El mantenerse al tanto de los mecanismos más usados para afectar usuarios permite activar los filtros necesarios de seguridad, así como buscar las mejores opciones de protección contra virus informáticos. Por otro lado, el conocimiento de las tendencias digitales, permite conocer qué marcas están sufriendo de suplantación de identidad, como mecanismo para cometer conductas infractoras.
3. Antivirus robusto más allá de los *endpoints*.- No basta contar con la última versión del antivirus si éste no vigila el comportamiento total del usuario y las probables intromisiones. Al respecto, se sugiere permitir acceso total al antivirus para detectar intrusiones, revisar ataques complejos en la web, funciones de prevención conductual, control de aplicaciones y *plug-in,* y limite en el uso de dispositivos USB que se utilizarán.
4. Proteger sitios web contra "Man in the Middle". - Implica activar la protección del sitio y su configuración, a través de los certificados *SSL* con validación extendida que permite el propio espacio digital.
5. Proteger claves privadas y aplicar política de contraseña eficaz.- Además de asegurarse que su contraseña exceda los 8 caracteres, combine letras y números; el usuario debe evitar reutilizar contraseñas en distintos sitios web y modificarlas cada 90 días, en tratándose de firmas digitales o electrónicas, se debe procurar que las mismas se resguarden en hardware diferente al equipo de uso diario.
6. Educar al cibernauta.- Parecería absurdo, pero según reportes de desarrolladores americanos, al menos un 80% de las vulneraciones al sistema se hubiesen evitado si el usuario reaccionara de forma diferente. Se sugiere encriptar datos personales sobre todo los de naturaleza sensible, hacer copias de seguridad regularmente, no abrir datos adjuntos inesperados o provenientes de fuentes no confiables, prevenir clic en URL de reputación dudosa, evitar descarga de software desconocido.

Países como Argentina, Brasil, Chile, Colombia, San Vicente y las Granadinas, Trinidad y Tobago y Uruguay, han logrado superar la cobertura de servicio de conexión a Internet, por más del 50% de su población en su espacio físico y aéreo. Una tarea muy alejada para otras naciones como México y Perú, que no superan el 40%, según reportes de la OEA. En ese tenor, parece claro que los Estados deben prender alertas serias, no sólo de política y demagogia, en atención a los millones de usuarios que se conectan diariamente a la red de redes y que se encuentran vulnerables ante una indebida educación digital y por la ausencia de medidas preventivas gubernamentales, independientemente de la tipificación que pudiere existir respecto de los

delitos cibernéticos e informáticos, pues más que la semántica que defendimos en el presente capítulo, también somos justos ante el bien jurídico tutelado que no puede esperar "nombre y apellido" en los códigos penales para verse protegido y, en su caso, reparado.

Referencias

Referencias Bibliográficas

ACEVEDO, Deysi y GÓMEZ, Élber. *Los documentos electrónicos y su valor probatorio: En procesos de carácter judicial.* IUSTITIA. Número 9. Diciembre de 2011.

ACOSTA Romero, Miguel. *Teoría General del Acto Jurídico*. Primera Parte. Porrúa. México.

BELLO, Luisa Isabel. "Modelo Argumentativo de Toulmin en la escritura de artículos de investigación educativa". *Revista Digital Universitaria.* Volumen 5. Número 1. Universidad Nacional Autónoma de México. 21 de enero de 2004.

BLACK'S LAW DICTIONARY. *The Law Dictionary*.

BRIZZIO, Claudia. *La informática en el nuevo derecho*. Abeloa Perrot. Buenos Aires, Argentina. 2000.

CÁMPOLI, Gabriel Andrés. *La Firma Electrónica en el Régimen Comercial Mexicano*. Porrúa. México. 2004. Página 3.

CARREÓN GALLEGOS, Ramón. *Derechos humanos, garantías individuales y derechos fundamentales*. Los derechos humanos en el momento actual. Instituto de Investigaciones Jurídicas. Universidad Nacional Autónoma de México. 2012.

Conferencia de la Haya de Derecho Internacional Privado. Electronic Commerce and International Jurisdiction–Ottawa, 28/2-1/3/00. Preliminary Document N° 12. Agosto de 2000.

DEVÍS, Hernando. *Teoría General de la Prueba Judicial*. Tomo II. 6ª edición. Pontificia Universidad Javeriana. Bogotá. Facultad de Ciencias Jurídicas. De la prueba por documentos. Bogotá, 2002.

Diccionario de Inglés de Oxford. Oxford Dictionaries. 2010

DOMÍNGUEZ MARTÍNEZ, José Alfredo. *Derecho Civil, parte general, personas, cosas negocio jurídico e invalidez*. Porrúa. 11ª edición. Página 215, México, 2008.

Enciclopedia Jurídica Mexicana.

FERRAJOLI, Luigi. *Los fundamentos de los derechos fundamentales.* Primera Vista. Editorial Trotta. Madrid, 2001. Edición de Antonio de Cabo y Gerardo Pisarello.

GÓMEZ NAVARRO, Soledad. *Testamento y tiempo: historia y derecho en el documento de última voluntad*. Universidad de Córdoba. Revistas Científicas de la Universidad de Cádiz. España, 1999.

GÓMEZ ROBLEDO, Alonso. *Protección de Datos Personales en México: el caso del Poder Ejecutivo Federal.* México, Instituto de Investigaciones Jurídicas UNAM, 2006.

GUADAMUZ, Andrés. *Artificial Intelligence and copyright.* WIPO. Octubre de 2017. Revista de la OMPI. 05/2017.

GUZMÁN, Ángeles. *Hábeas Data. Diccionario de Derecho Procesal, Constitucional y Convencional.* Tomo II. Instituto de Investigaciones Jurídicas. Serie Doctrina Jurídica. Número 693.

Jane Reno, Attorney General of the United States *et al.* appellans vs. American Civil Liberties Union, *et al.*, sentencia del 26 de junio de 1997.

JEWELL, Catherine. *Mycelia: una nueva configuración del panorama musical.* División de comunicaciones de la OMPI. OMPI Revista. Abril de 2016.

KELSEN, Hans. *Crítica a la Teoría Pura del Derecho.* Editorial EUDEBA. Buenos Aires, 1989.

LABARDINI INZUNZA, Adriana. *Del derecho a la protección de los consumidores y a su organización.* Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas, Suprema Corte de Justicia, Fundación Konrad Adenauer. México, 2013.

LIMÓN, Jaime (coordinador). *Antología Iberoamericana sobre Propiedad Intelectual. Daddy's Car: Inteligencia Artificial como herramienta auxiliar en la creación de derechos de autor.* México, 2018. Tirant Lo Blanch

LIRA ARTEAGA, Óscar M. *Cibercriminalidad.* Instituto de Investigaciones Jurídicas. Instituto de Formación de la Procuraduría General de Justicia. México, 2012.

LÓPEZ MONROY, José, *et al. Diccionario Jurídico Mexicano. Legado.* Universidad Nacional Autónoma de México. Instituto de Investigaciones Jurídicas. Tomo VI L-O. Segunda Parte. México, 1982.

PALLARES, Eduardo. *Diccionario de Derecho Procesal Civil.* Editorial Porrúa. Vigésima Octava Edición. México, 2005

R. PUCCINELLI, Oscar. *Protección de Datos de Carácter Personal.* Argentina 2004, Editorial Astrea.

REYES KRAFT. Alfredo A. *La firma electrónica y las entidades de certificación.* Porrúa. México, 2003.

RÍOS ESTAVILLO, Juan José. *Derecho e Informática en México. Informática Jurídica y Derecho de la Informática.* Universidad Nacional Autónoma de México. México, 1997.

ROJAS, Pedro. *Reclutamiento y Selección 2.0. La nueva forma de encontrar talento.* Editorial UOC. España, 2010.

SANTAMARÍA Ramos, Francisco José. *Identidad y Reputación Digital. Visión Española de un Fenómeno* Global. Revista Ambiente Jurídico. Número 17. Enero 2015.

SHARIFF, Azim, *et al.* "The social dilema of autonomous vehicles". *Science.* 24 de junio de 2016. Volumen 352. Páginas 1573-1576.

TÉLLEZ VALDÉS, Julio. *Contratos Informáticos. Contratos, Riesgos y seguros informáticos.* "Capítulo II. Contratos Informáticos". Universidad Nacional Autónoma de México. México, 1988.

TÉLLEZ VALDÉS, Julio. *Derecho Informático*. "Capítulo XIII. Contratos Informáticos". Mc Graw Hill. 2ª edición. México, 1998.

TÉLLEZ, Julio. *La protección jurídica de los programas de cómputo*. Universidad Nacional Autónoma de México. México, 1989. 2ª edición.

WALLERSTEIN, Immanuel. *El Universalismo Europeo. El discurso del Poder*. Inglaterra, 2004. Editorial Siglo xxi. Primera edición en inglés 2006, primera edición en español 2007.

Referencias hemerográficas y electrónicas

24 HORAS. "Joven demanda a Instagram tras ser usada como meme". *Diario 24 horas*. Julio 2014. Puede consultar la nota completa a través del vínculo http://www.24horas.cl/tendencias/espectaculosycultura/joven-demanda-a-instagram-tras-ser-usada-como-meme-1321986

ABC España. *Vale, ¿pero cuánto cobran los famosos por un "tuit"?* 24 de enero de 2017. Madrid, España. Visto el 18 de noviembre de 2017, a través del vínculo http://www.abc.es/tecnologia/redes/abci-vale-pero-cuanto-cobran-famosos-tuit-201701240234_noticia.html

AGENCIA DE GOBIERNO ELECTRÓNICO Y DE LA SOCIEDAD. *YouTube*. AGESIC. 20 de junio de 2011. http://youtu.be/qDvuC5GH_pI, visto el 1 de abril de 2016.

INSTITUTO GLOBAL DE ALTOS ESTUDIOS EN CIENCIAS SOCIALES. *Youtube*. Editado por FUNGLODE Media. FUNGLODE Multimedia. 17 de diciembre de 2012. http://youtu.be/PoYqNlnBoy4. Visto el 1 de abril de 2016.

ALLEN Green, David. *Copyright: No time to monkey around*. WIPO MAGAZINE. Versión en línea para consulta a través del vínculo http://www.wipo.int/wipo_magazine/en/2014/05/article_0004.html

AMAZON. *Contrato de licencia y condiciones de uso del Kindle de Amazon.es*. Última actualización de 28 de septiembre de 2011. Consultado en línea el 11 de noviembre de 2017, a través del vínculo https://www.amazon.es/gp/help/customer/display.html?nodeId=201283840&tag=xataka-21

AMIPCI. *Estudio sobre los hábitos de los usuarios de internet en México 2014*. México, 2014. Visto el 10 de diciembre de 2017 a través del vínculo http://www.amipci.org.mx/estudios/habitos_de_internet/Estudios_Habitos_del_Internauta_Mexicano_2014_V_MD.pdf

APPLE. *Términos y Condiciones de los Servicios de Contenido Multimedia de Apple*. Legal. 13 de septiembre de 2016. Consultado en línea el 11 de noviembre de 2017, a través del vínculo https://www.apple.com/legal/internet-services/itunes/es/terms.html

ASAMBLEA GENERAL DE LAS NACIONES UNIDAS. Comisión de las Naciones Unidas para el Derecho Mercantil Internacional. *Jurisprudencia de los*

Tribunales sobre Textos de la CNUDMI (CLOUT). Visto el 27 de noviembre de 2017 a través del vínculo https://documents-dds-ny.un.org/doc/UNDOC/GEN/V10/546/15/PDF/V1054615.pdf?OpenElement

ASOCIACIÓN DE INTERNET.MX/ INFOTEC. 13° Estudio sobre los hábitos de los usuarios de Internet en México 2017. Mayo 2018. Consultado en línea a través del vínculo https://www.infotec.mx/work/models/infotec/Resource/1012/6/images/Estudio_Habitos_Usuarios_2017.pdf el pasado 31 de mayo de 2017

AUDIBLE MAGIC. Help Desk. *Registering Your Content with Audible Magic*. 13 de noviembre de 2017. Visto el 24 de noviembre de 2017 a través del vínculo https://audiblemagic.zendesk.com/hc/en-us/articles/201232220-Registering-my-content-with-Audible-Magic

BARRANCO FRAGOSO, Ricardo. ¿Qué es Big Data? DeveloperWorks. IBM. 18 de junio de 2012. Aprenda/ Information mgmt. Visto el 13 de diciembre de 2017 a través del vínculo https://www.ibm.com/developerworks/ssa/local/im/que-es-big-data/index.html

BBC MUNDO. *El caso del primer hombre en el mundo condenado a prisión por "violación por internet"*. 6 de diciembre de 2017. Visto el 7 de diciembre de 2017 a través del vínculo http://www.bbc.com/mundo/noticias-42252461

BBC MUNDO. *El gobierno de Donald Trump pone fin a las normas que aseguraban la neutralidad de internet en Estados Unidos*. 14 de diciembre de 2017. Recuperado el 15 de diciembre de 2017 a través del vínculo http://www.bbc.com/mundo/noticias-internacional-42359904

BCC MUNDO. *Tay, la robot racista y xenófoba de Microsoft*. 25 de marzo de 2016. Consultado en línea el pasado 11 de noviembre de 2017 a través del vínculo http://www.bbc.com/mundo/noticias/2016/03/160325_tecnologia_microsoft_tay_bot_adolescente_inteligencia_artificial_racista_xenofoba_lb

BITCONNECT. *What is Bitcoin?* Visto el 01 de diciembre de 2017 a través del vínculo https://bitconnect.co/bitcoin-information/2/what-is-bitcoin

BRIGHT, Sam. *After Trump, "big data" firm Cambridge Analytica is now working in Kenya*. BCC Trending. 3 de agosto de 2017. Recuperado el 13 de diciembre de 2017 a través del vínculo http://www.bbc.com/news/blogs-trending-40792078

BUENROSTRO MERCADO, Héctor. CONACYT/ INFOTEC. ¿Es gratuito el software libre? Centro de investigación e Innovación en Tecnologías de la Información y Comunicación. Sistema de centros Públicos de Investigación. México. Puede consultar el artículo completo en el vínculo https://centrosconacyt.mx/objeto/softwarelibre/ visto el 15 de noviembre de 2017

BUSTILLOS, María. *The bitcoin Boom*. The New Yorker. Elements. 1 de abril de 2013. Visto el 01 de diciembre de 2017 a través del vínculo https://www.newyorker.com/tech/elements/the-bitcoin-boom

CASAÑAS, María Elena. ¿Qué es el software libre? CASANAS. COM. AR. Puede consultar el texto íntegro a través del vínculo http://www.casanas.com.ar/attachments/Que_es_-_A_-_Conc_tecnicos.pdf. Visto el 14 de noviembre de 2017

CATTAN, Nacha. *Trump's Big Data Gurus Scout Presidential Candidate In Mexico.* Bloomberg. Politics. Estados Unidos de América, 19 de Julio de 2017. Visto el 13 de diciembre de 2017 a través del vínculo https://www.bloomberg.com/news/articles/2017-07-19/trump-s-big-data-gurus-scout-presidential-candidate-in-mexico

CISCO. *The Zettabyte Era- Trends and Analysis*. Documento que forma parte del CISCO® Visual Networking Index (VNI). Consultado en línea el 31 de mayo de 2017 a través de http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/vni-hyperconnectivity-wp.html

CISCO. *Visual Networking Index (VNI) IP Traffic Chart.* Consultada en línea a través del vínculo http://www.cisco.com/cdc_content_elements/networking_solutions/service_provider/visual_networking_ip_traffic_chart.html

COMISIÓN EUROPEA. *Mergers: Commision fines Facebook 110 million for providing misleading information about WhatsApp takeover.* Press Release. Bruselas, 18 de mayo de 2017. Recuperado el 16 de diciembre de 2017 a través del vínculo http://europa.eu/rapid/press-release_IP-17-1369_en.htm

Commemorating the 1956 founding ad Dartmouht College of AI as research discipline. http://www.dartmouth.edu/~ai50/homepage.html

CONDUSEF. ¿Qué son las *fintech?* Educación Financiera. Proteja su dinero. Gobierno de la República Mexicana. Visto el 13 de diciembre de 2017 a través del vínculo http://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/educacion-finauciera/763-que-son-las-fintech

CONSEJO SOBRE NORMAS DE SEGURIDAD DE LA PCI, LLC. *Normas de Seguridad de Datos de la Industria de tarjetas de pago.* Abril de 2016. Versión 3.2. Recuperado el 11 de diciembre de 2017 a través del vínculo https://es.pcisecuritystandards.org/_onelink_/pcisecurity/en2es/minisite/en/docs/PCI_DSS_v3-2_es-LA.pdf

CONTACT GROUP OF THE DATA PROTECTION AUTHORITIES. *Common Statement.* 16 de mayo de 2017. Recuperado el 16 de diciembre de 2017 a través del vínculo https://sontusdatos.org/wp-content/uploads/2017/05/Common_Statement_16_May_2017.pdf

CORELLA RAMÍREZ, David, et al. *Modalidades de Fraude en la compra-venta de artículos de aplicaciones electrónicas*. Universidad Autónoma del Estado de Hidalgo. Boletín ICEA Número 9. Disponible en línea a través del vínculo https://www.uaeh.edu.mx/scige/boletin/icea/n9/e1.html

CREATIVE COMMONS. *Sobre las licencias. Lo que nuestras licencias hacen.* Visto el 16 de noviembre de 2017 a través del vínculo https://creativecommons.org/licenses/

DAKEVYCH, Alex. *The Australian Teen suing for mullet memes*. BBC Trending. BBC News. Noviembre 2016. Puede consultar la nota completa a través de vínculo http://www.bbc.com/news/blogs-trending-37838197

DAVIDSON, Stephen J. *Estudio sobre los programas informáticos de código abierto para empresarios y abogados* Organización Mundial de Propiedad Intelectual. Estados Unidos, 2004. Puede consultar el texto íntegro, a través del vínculo http://www.wipo.int/sme/es/documents/opensource_software_primer.htm

DAVIDSON, Stephen J. *Estudio sobre los programas informáticos de código abierto para empresarios y abogados* Organización Mundial de Propiedad Intelectual. Estados Unidos, 2004. Puede consultar el texto íntegro, a través del vínculo http://www.wipo.int/sme/es/documents/opensource_software_primer.htm

DELL. *Términos de licencia del software de Microsoft. Windows Vista Home Basic, Windoes Vista Home Premium, Windows Vista Ultimate.* Puede consultar las políticas íntegras, a través del vínculo http://www.dell.com/downloads/global/products/vostrodt/es/UseTerms_OEM_Vista_HomeBasicHomePremiumUltimate.pdf

Derechos en Acción, primavera 2017. Universidad Nacional de la Plata, Buenos Aires, Argentina. Visible a través del vínculo https://revistas.unlp.edu.ar/ReDeA/article/view/4083/4034

DIARIO CRÍTICO. *Tellmebye, el primer testamento digital ante notario*. Emprendedores 2020. España, Mayo de 2015. Puede consultar la nota completa a través del vínculo https://www.diariocritico.com/noticia/479213/emprendedores-2020/tellmebye-el-primer-testamento-digital-ante-notario.html

EFE/ 20 Minutos. *El partido Nacional de Nueva Zelanda deberá compensar a Eminem por derechos de autor*. Música. España. 25 de octubre de 2017. Visto el 24 de noviembre a través del vínculo http://www.20minutos.es/noticia/3169586/0/nueva-zelanda-partido-nacional-compensar-eminem-derechos-autor/

EL FINANCIERO. *Ley Mordaza, de última hora.* Opinión. México, 15 de diciembre de 2017, visto a través del vínculo http://www.elfinanciero.com.mx/opinion/ley-mordaza-de-ultima-hora.html

EL FINANCIERO. Redacción. ¿Te imaginas un abogado robot? Aquí te lo presentamos. TECH. México, 14 de noviembre de 2017. Visto el 24 de noviembre de 2017 a través del vínculo http://www.elfinanciero.com.mx/tech/los-robots-quieren-ganarle-a-los-abogados-y-lo-estan-logrando.html

EL FINANCIERO. *Senado aprueba la Ley Fintech.* Notimex. Economía. México, 5 de diciembre de 2017. Recuperado el 13 de diciembre de 2017 a través del vínculo http://www.elfinanciero.com.mx/economia/senado-aprueba-la-ley-fintech.html

EL MUNDO. *Una inteligencia artificial se vuelve racista, antisemita y homófoba en menos de un día en Twitter.* Madrid. 28 de marzo de 2016. Consultado en línea

el pasado 11 de noviembre de 2017, a través del vínculo http://www.elmundo.es/tecnologia/2016/03/28/56f95c2146163fdd268b45d2.html

EL NACIONAL. *Facebook llega a 1,500 millones de usuarios.* Histórico. 03 de agosto de 2015, actualizado el 09 de diciembre de 2016. Colombia. Visto el 24 de noviembre de 2017 a través del vínculo http://www.el-nacional.com/noticias/historico/facebook-llega-1500-millones-usuarios_45960

ELGUEA, Javier. *Inteligencia artificial y psicología: la concepción contemporánea de la mente humana, Breve Historia de la Inteligencia Artificial.* Instituto Tecnológico Autónomo de México. Estudios sobre filosofía-historia y letras. |1987. Consultable en línea, a través del vínculo http://biblioteca.itam.mx/estudios/estudio/estudio10/sec_16.html

ESCAMILLA, Viridiana. ¿Quién pierde con los fraudes en e-*commerce?* Portada. Emprendedores. FORBES MÉXICO. Agosto 1 de 2013. Disponible a través del vínculo https://www.forbes.com.mx/quien-pierde-con-los-fraudes-en-e-commerce/

Invertimos en los creadores y Derechos de Autor. Consultado en línea a través del vínculo https://www.youtube.com/yt/press/es/statistics.html el 19 de abril de 2017

ESTEVEZ, María. "El valor de la marca Beckham se dispara hasta los 1 000 millones de euros". ABC. Gente y estilo. Consulta en línea a través de http://www.abc.es/estilo/gente/abci-valor-marca-beckham-dispara-hasta-1000-millones-euros-201601140020_noticia.html

FACEBOOK. ¿Qué es un contacto de legado de Facebook? https://www.facebook.com/help/1568013990080948

FACEBOOK. *Declaración de Derechos y Responsabilidades. Compartir el contenido y la información.* Última versión de 30 de enero de 2015. Visto el 21 de noviembre de 2017, a través del vínculo https://www.facebook.com/legal/terms

FACEBOOK. *Rights Manager.* Visto el 24 de noviembre de 2017 a través del vínculo https://rightsmanager.fb.com/

FERNÁNDEZ FLORES, Ricardo. *La ejecución de los contratos click-wrap y browse wrap en Derecho español.* Economist & Jurist. Inicio. Artículos destacados. Difusión jurídica y temas de actualidad, S.L. España, 2017. Visto el 29 de noviembre de 2017 a través del vínculo http://www.economistjurist.es/articulos-juridicos-destacados/la-ejecucion-de-los-contratos-click-wrap-y-browse-wrap-en-derecho-espanol/

FERRADA Cubillos, Mariela. *Términos de uso frecuente en la Web Social. Glosario*. Departamento de Gestión de Información. Universidad Tecnológica Metropolitana. Serie bibliotecología y gestión de información número 81, abril 2013. Mismo que se puede consultar en línea a través del vínculo http://eprints.rclis.org/19182/1/Serie%20N%C2%B081%20Mariela%20Ferrada.pdf

FIX FIERRO, Héctor y PONCE DE LEÓN, Luis. *Informática y documentación jurídica.* Boletín Mexicano de Derecho Comparado. Número 74. Instituto de Investigaciones Jurídicas. UNAM. México, Agosto 1992. Visto el 9 de diciembre

de 2017 a través del vínculo https://revistas.juridicas.unam.mx/index.php/derecho-comparado/article/view/2965/3221

FLORIO, Luis. *Bitcoin de récord: ¿es todo una estafa?* La Vanguardia. Economía. El futuro de las divisas. España, 30 de noviembre de 2017. Visto el 13 de diciembre de 2017 a través del vínculo http://www.lavanguardia.com/economia/20171130/433291143335/comprar-bitcoin-invertir-estafa.html

FORBES México. *Las 20 empresas tecnológicas más importantes del mundo.* Forbes Staff. Portada. Agosto 18 de 2013. Puede consultar el listado completo en el vínculo https://www.forbes.com.mx/las-20-empresas-tecnologicas-mas-importantes-del-mundo/ visto el 14 de noviembre de 2017.

FORBES. *Hawkers propone a Checo Pérez crear una fundación con su nombre.* Portada. Últimas Noticias. Forbes Staff. Noviembre 17 de 2016. Se puede consultar en línea a través del vínculo https://www.forbes.com.mx/hawkers-propone-a-checo-perez-crear-una-fundacion-con-su-nombre/ Mismo que se revisó el 03 de junio de 2017.

FORBES. *Top predictions for 2014 by VCs. Think of Bitcoin as a commodity, not a currency.* 2014. Visto el 01 de diciembre de 2017 a través del vínculo https://www.forbes.com/pictures/ekij45gjle/think-of-bitcoin-as-a-commodity-not-a-currency-2/#6c13c6002a78

FOS MEDINA, Juan Bautista. *El testamento en la historia: aspectos morales y religiosas.* Biblioteca digital de la Universidad Católica Argentina. Suplemento de filosofía número 30, Argentina, 2015. Puede consultar el artículo completo, en el repositorio institucional en el vínculo http://bibliotecadigital.uca.edu.ar/repositorio/investigacion/testamento-historia-morales-religiosos.pdf

FOX SPORTS. *Entérate cuánto sale aparecer en un tweet de Cristiano Ronaldo.* Columnistas. La Liga. Fox Sports. Junio de 2017. Buenos Aires. Visto el 18 de noviembre a través del vínculo https://www.foxsports.com.mx/blogs/view/310064-enterate-cuanto-sale-aparecer-en-un-tweet-de-cristiano-ronaldo

FRESNEDA, Carlos. "Un ordenador logra superar por primera vez el test de Turing". *El Mundo.* 10 de junio de 2014. Publicado en el periódico español en línea a través del vínculo http://www.elmundo.es/ciencia/2014/06/09/539589ee268e3e096c8b4584.html

FTC. *Información para consumidores.* Seguridad Informática. Visto el 11 de diciembre de 2017 a través del vínculo https://www.consumidor.ftc.gov/articulos/s0009-seguridad-informatica

GATT, Adam. *Electronic Commerce. Click Wrap Agreements.* The Enforceability of Click Wrap Agreements. University of Melbourne, Australia. Computer Law & Security Report, Vol. 18, No. 6. 2002. Visto el 29 de noviembre de 2017 a través del vínculo https://edisciplinas.usp.br/pluginfile.php/2056275/mod_resource/content/1/enforceability%20of%20clickwrap%20%28Adam%20Gatt%29.pdf

GNU. *Visión General del Sistema GNU.* El sistema operativo GNU. Última modificación el 10 de septiembre de 2017. Visto a través del vínculo https://www.gnu.org/guu/gnu-history.html el 16 de noviembre de 2017.

GOOGLE. *Administrador de cuentas inactivas. https://myaccount.google.com/inactive*

GREENBERG, Andy. *Silk Road creator Ross Ulbricht Loses His Life Sentence Appeal.* WIRED. 31 de mayo de 2017. Visto el 7 de diciembre de 2017 a través del vínculo https://www.wired.com/2017/05/silk-road-creator-ross-ulbricht-loses-life-sentence-appeal/

GUADAMUZ GONZÁLEZ, Andrés. OMPI. *Propiedad Intelectual y Software.* Revista de la OMPI. Diciembre de 2008. Puede consultar el texto íntegro a través del vínculo http://www.wipo.int/wipo_magazine/es/2008/06/article_0006.html

GUTIÉRREZ, Fernando. *Diputados aplazan discusión de Ley Fintech; podría irse hasta 2018.* El Economista. México, 12 de diciembre de 2017. Visto el 13 de diciembre de 2017 a través del vínculo https://www.eleconomista.com.mx/sectorfinanciero/Diputados-aplazau-discusion-de-Ley-Fintech-podria-irse-hasta-2018-20171212-0117.html

HILEMAN, Garrick y RAUCHS, Michel. *Global cryptocurrency benchmarking study.* Cambridge Centre for Alternative Finance. University of Cambridge. Judge Business School. With the Support of *VISA*. Reino Unido, 2017. Visible el 01 de diciembre de 2017 a través del vínculo https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-global-cryptocurrency-benchmarking-study.pdf

HOFFMAN, Ivan. *Scenes a faire Under Copyright Law*. Estados Unidos, 2003. Puede consultar el texto íntegro a través del vínculo http://www.ivanhoffman.com/scenes.html , visto el 18 de noviembre de 2017.

HUDAK, Steve. *FinCEN Fines BTC-e Virtual Currency Exchange $110 million for facilitating ransomware, Dark Net Drug Sales*. United States Department of the Treasury. FinCEN. 27 de julio del 2017. Visto el 01 de diciembre de 2017 a través del vínculo https://www.fincen.gov/news/news-releases/fincen-fines-btc-e-virtual-currency-exchange-110-million-facilitating-ransomware

HUDAK, Steve. *FinCEN Publishes Two rulings on Virtual Currency Miners and Investors*. FinCEN. Washington, Enero 20 del 2014. Visto el 01 de diciembre de 2017 a través del vínculo https://www.fincen.gov/news/news-releases/fincen-publishes-two-rulings-virtual-currency-miners-and-investors

IBM. News Room. News Releases. *IBM and Audible Magic Team to protect video content*. California, 23 de octubre de 2008. Visto el 24 de noviembre de 2017 a través del vínculo https://www-03.ibm.com/press/us/en/pressrelease/25741.wss

INTELLECTUAL PROPERTY OFFICE & PRS for Music. *Stream-Rippin: How it works and its role in the UK music piracy ladscape.* Reino Unido. Julio de 2017. Consultado en línea el 25 de agosto a través del vínculo https://s3.amazonaws.com/documentos-ia/pdf/KANTAR_E_INCOPRO_STREAM-RIPPING_REPORT.pdf

JANÉ, Carmen. *Testamento digital: ¿qué pasará con tu Facebook cuando hayas muerto? El Periódico.* Sociedad. Barcelona. 28 de febrero de 2017. Puede consultar el texto completo a través del vínculo http://www.elperiodico.com/es/sociedad/20170228/testamento-digital-ley-catalunya-5865493

JUSTIA. Naruto *v. David John Slater et al, No. 3:2015cv04324 - Document 45 (N.D. Cal. 2016). ORDER GRANTING MOTIONS TO DISMISS by Judge William H. Orrick granting 24 Motion to Dismiss and 28 Motion to Dismiss for Lack of Jurisdiction. Defendants' motions to dismiss are GRANTED.* Puede consultar la sentencia íntegra a través del vínculo http://law.justia.com/cases/federal/district-courts/california/candce/3:2015cv04324/291324/45/

KARP, Hannah. *Music Industry's Latest Piracy Threat: Stream Ripping.* The Wall Street Journal. Estados Unidos de América. Septiembre 12 de 2016. Puede consultarse el artículo completo –previo pago de suscripción-, a través del vínculo https://www.wsj.com/articles/music-industrys-latest-piracy-threat-stream-ripping-1473718919. Visto el pasado 22 de agosto de 2017.

KUTSENKO, Ekaterina. *Waves Platform, with the support of leading market players, is founding new self-regulatory body to set standars for ICO's (Initian Coin Offering).* DELOITTE CIS. Rusia, Moscú, 11 de diciembre de 2017. Visto el 13 de diciembre de 2017 a través del vínculo https://www2.deloitte.com/content/dam/Deloitte/ru/Documents/about-deloitte/pressrelease/waves-platform-en.pdf

LAVENDA, David, The Battle of intelligence, publicado el 22 de septiembre de 2016, en la revista en línea *Computer News Middle East* (CNME) y consultado el pasado 01 de octubre de 2016, a través del vínculo http://www.cnmeonline.com/insight/the-battle-of-intelligence/

LIEU, Ted. *Overview of the MMA.* Estados Unidos de América, Septiembre de 2018. Congresista del 33ª Distrito de California. Visto el 21 de octubre de 2018 a través del vínculo https://lieu.house.gov/sites/lieu.house.gov/files/Overview%20of%20the%20Music%20Modernization%20Act.pdf

LIMÓN, Jaime. *El Origen del mundo: Crítica al Sistema Normativo en Facebook.* Foro Jurídico. Diciembre de 2016. Se puede consultar la obra primigenia a través del vínculo https://www.forojuridico.org.mx/origen-del-mundo-critica-al-sistema-normativo-facebook/

LIMÓN, Jaime. *El Proceso de Autorregulación Autoral en Youtube.* Publicado originalmente el 05 de mayo de 2017, en la edición impresa de mayo y en la edición digital de la revista Foro Jurídico. Consultable en línea a través del portal https://www.forojuridico.org.mx/proceso-autorregulacion-autoral-youtube/

LIMÓN, Jaime. *Las 10 profesiones que desaparecerán con la Inteligencia Artificial.* México, Octubre 2018. Foro Jurídico. Política. Visto el 21 de octubre de 2018 a través del vínculo https://forojuridico.mx/las-10-profesiones-que-desapareceran-con-la-inteligencia-artificial/

LÓPEZ VARAS, Mariana. *Regulación Jurídica de la Contratación Electrónica en el Código Civil Federal*. Instituto de Transparencia y Acceso a la Información Pública del Estado de México y Municipios. Primera Edición. México. Septiembre 2010. Puede consultar el texto íntegro a través del vínculo http://www.infoem.org.mx/sipoem/ipo_capacitacionComunicacion/pdf/pet_tesis_001_2009.pdf

LÓPEZ, Yair. *Las Empresas pierden hasta 10% de sus ventas por fraude electrónico.* CNN México. Tecnología. Miércoles 19 de julio de 2017. Visto el 27 de noviembre de 2017 a través del vínculo http://mexico.cnn.com/tecnologia/2017/07/19/las-empresas-pierden-hasta-10-de-sus-ventas-por-fraude-electronico

MANDJEE, Tara. *Bitcoin, its Legal Classification and its regulatory framework.* Journal of Business and securities law. Michigan State University. College of Law. Digital Commons at Michigan State. Volume 15. Issue 2. Article 4. 2015. Disponible a través del vínculo https://digitalcommons.law.msu.edu/jbsl/vol15/iss2/4

MÁRQUEZ VILLÉN, Francisco. *Testamento Digital. Nuevas tecnologías y derecho.* Publicaciones de IN DIEM. Abogados. Madrid, Sevilla. Enero, 2016. Visto el 16 de diciembre de 2017 a través del vínculo https://www.in-diem.com/wp-content/uploads/2016/01/CUADERNOS-IN-DIEM-Abogados-Testamento-Digital.pdf

MECINAS MONTIEL, Juan. *The Digital Divide In Mexico: A mirror of Poverty.* Mexican Law Review. Universidad Nacional Autónoma de México. Julio-Diciembre de 2016. Número 1, Volumen IX. México. Visible el 10 de diciembre de 2017 a través del vínculo https://revistas.juridicas.unam.mx/index.php/mexican-law-review/article/view/10432

MIGLIANO, Simon. *Dark web Market Price Index (US Edition).* TOP 10 VPN. Privacy Central. Estados Unidos de Anérica. 27 de febrero de 2018. Visto el 08 de agosto de 2018 a través del vínculo https://www.top10vpn.com/privacy-central/privacy/dark-web-market-price-index-feb-2018-us/

MIT Media Lab. *Moral Machine*. Massachusetts Institute of Technology. Consultable en línea a través del vínculo http://moralmachine.mit.edu/

MONROY, Jorge. "Aprueban que SE emita NOM para regular ecommerce". *El Economista*. México. 15 de noviembre de 2017. Visto el 27 de noviembre de 2017 a través del vínculo https://www.eleconomista.com.mx/empresas/Aprueban-que-SE-emita-NOM-para-regular-ecommerce-20171115-0049.html

MORENO, V. "El testamento digital, una herencia conflictiva". *Expansión.* España, Portada, Jurídico. Abril de 2013. Puede consultar la nota completa a través del vínculo http://www.expansion.com/2013/04/18/juridico/1366302969.html

MOZUR, Paul, MARKOFF. "China es el nuevo líder en el campo de la inteligencia artificial". *The New York Times ES.* Noticias. Tecnología. 2 de junio de 2017. Puede consultar la declaración e investigación completa a través del vínculo https://www.nytimes.com/es/2017/06/02/china-inteligencia-artificial/

NATIONAL TAXPAYERS UNION. *Milton Frieadman Full Interview on Anti-trust and Tech. YouTube.* Entrevista de 1999 publicada el 09 de agosto de 2012. Puede consultar la entrevista completa, a través del vínculo https://www.youtube.com/watch?v=inlwxdyLnMXM&feature=youtu.be

NAVETTA, David. *Legal implication of Big Data.* ISSA Journal. Marzo 2013. Visto el 13 de diciembre de 2017 a través del vínculo https://c. ymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0313.pdf

NOÉ. *Nature See You.* Cerebro Digital. Enero 2016. Puede consultar la traducción del video, en la versión titulada "Koko el gorila que habla con humanos, tiene un mensaje urgente". El mismo se publicó en el marco de la Cumbre de París sobre cambio climático (COP21 SUMMIT). https://www.youtube.com/watch?v=rXkvKXaZRws

OATH, Inc. *Yahoo provides notice to additional users affected by previously disclosed 2013 data thef.* Nueva York, Octubre 3 de 2017. Recuperado el 16 de diciembre de 2017 a través del vínculo https://www.oath.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/

OBAMA, Barack. *Memorandum on Transparency and Open Government. Administration of Barack H. Obama, 2009.* Transparencia y gobierno abierto. Memorándum para los jefes de los departamentos ejecutivos y agencias. Estados Unidos de América. 21 de enero de 2009. Visto el 16 de diciembre de 2017 a través del vínculo https://www.archives.gov/files/cui/documents/2009-WH-memo-on-transparency-and-open-government.pdf

OJO, Adegboyega/ MILLARD, Jeremy. *Government 3.0- Next Generation Government Technology Infraestructure and Services.* Editorial Springer. Suiza, 2017. Puede consultar la versión digital a través del vínculo https://books.google.com.mx/books?id=VaI7DwAAQBAJ&lpg=PA297&ots=Rgh4_0pSHZ&dq=bitcoin%20wipo&hl=es&pg=PR7#v=onepage&q=bitcoin%20wipo&f=false

OMPI. *Un nuevo sistema de gestión de licencias en línea facilita la reedición de las publicaciones de las organizaciones intergubernamentales.* Génova, 6 de diciembre de 2013. Comunicados de Prensa. Visto el 16 de noviembre de 2011 a través de http://www.wipo.int/pressroom/es/articles/2013/article_0026.html

OMPI. *Uso de licencias de Creative Commons para organizaciones Intergubernamentales.* Política de acceso abierto de la OMPI. 15 de noviembre de 2016. Visto el 16 de noviembre de 2017 a través del vínculo http://www.wipo.int/export/sites/www/tools/es/cc_igo_licenses.pdf

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS/SYMANTEC. *Tendencias de seguridad cibernética en América Latina y el Caribe.* Publicado en junio de 2014. Visto el 9 de diciembre de 2017 a través del vínculo https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

OSLAK, Oscar. *Ideas sobre gobierno abierto.* Gobierno Abierto. El valor social de la información Pública. Isa Luna Pla y José Antonio Bojórquez Pereznieto, Coordinadores. Instituto Tabasqueño de Transparencia y Acceso a la Información Pública. Instituto de Investigaciones Jurídicas, UNAM. México, 2015. Visible el 16 de diciembre de 2017 a través del vínculo https://archivos.juridicas.unam.mx/www/bjv/libros/9/4016/17.pdf

PALACIO, Guillermo. *Presidente de la Fundación de Software Libre de Europa: a Facebook le quedan 3 años (sic).* Hipertextual. Economía y empresas. Internet. 29 de julio de 2013. Visto el 24 de noviembre de 2017 a través del vínculo https://hipertextual.com/2013/07/opinion-de-karsten-gerloff-sobre-facebook

PATENTSCOPE/WIPO. *Search International and National Patent Collections. Bitcoin Technology.* 24 de febrero de 2015. Visto el 02 de diciembre de 2017 a través del vínculo https://patentscope.wipo.int/search/en/detail.jsf;jsessionid=1A75938928EB9E338D4E14DB8AB2C578.wapp2nB?docId=GB176139235&recNum=1&office=&queryString=bitcoin+&prevFilter=&sortOption=&maxRec=1817

PÉREZ CAZARES, Martín. *El Habeas Data o Derecho a la Intimidad en el Derecho Informático.* Orden Jurídico Nacional. Gobierno Federal de los Estados Unidos Mexicanos. Recuperado el 15 de diciembre de 2017 a través del vínculo http://www.ordenjuridico.gob.mx/Congreso/pdf/98.pdf

PINZÓN, Carlos. *Diferencia entre identidad digital y reputación on-line.* INVENIO PRO. Social Media. INVENIO PRO, Blog de Marketing Online. Consultado en línea a través del vinculo http://www.inveniopro.es/diferencia-entre-identidad-digital-y-reputacion-on-line/

PIÑERO, Laura. *Un abogado sevillano demanda a "Apple" inspirado por Bruce Willis (sic).* Cadena SER. Madrid, España, 2012. Puede consultar la nota íntegra, a través del vínculo http://cadenaser.com/programa/2017/01/20/la_ventana/1484935223_530716.html

PORCELLI, A. "Los bienes digitales y el derecho de autor en internet. La denominada 'piratería informática'". *Revista del Departamento de Ciencias Sociales*, Volumen 2, Número 3. 258.294. Revista electrónica del Departamento de Ciencias Sociales de la Universidad Nacional de Luján. Puede consultar el texto íntegro a través del vínculo http://www.redsocialesunlu.net/wp-content/uploads/2015/06/RSOC009-16-ARTICULO-PORCELLI.pdf

PROCESO. *Hackers roban datos personales de 57 millones de clientes y choferes de Uber. Bloomberg.* Redacción. México, 21 de noviembre de 2017. Visto el 16 de diciembre de 2017 a través del vínculo http://www.proceso.com.mx/512086/hackers-roban-datos-personales-57-millones-clientes-choferes-uber-bloomberg

PS.S.L. *Panda Security*. 2013. Recuperado de: http://www.pandasecurity.com/spain/homeusers/security-info/glossary

R3D. ¡Ganamos! Tribunal anula resolución del INAI sobre el faso "derecho al olvido". México, 24 de agosto de 2016. Visto el 14 de diciembre de 2017 a través del vínculo

REINBERG, Consuelo. ¿Están los tweets protegidos por derechos de autor? Revista de la OMPI. Número 4/2009. Julio de 2009. Visto el 18 de noviembre de 2017 a través del vínculo http://www.wipo.int/wipo_magazine/es/2009/04/article_0005.html

REUTERS. *Russia demands Internet Users show ID to access public Wifi.* Business Insider. Moscú, 8 de agosto de 2014. Visto el 16 de diciembre de 2017 a través del vínculo http://www.businessinsider.com/r-russia-demands-internet-users-show-id-to-access-public-wifi-2014-08

REY RUIZ, Ramón. "Testamento Digital Inverso, ¿una forma de ejercicio del derecho al olvido?" *Diario Jurídico*. España, 23 de octubre de 2014. Visto el 16 de diciembre de 2017 a través del vínculo http://www.diariojuridico.com/testamento-digital-inverso-una-forma-de-ejercicio-del-derecho-al-olvido/

RIQUELME, Rodrigo. "La suprema corte de Justicia confirma sentencia contra Google en México". *El Economista*. México. 6 de diciembre de 2017. Recuperado el 14 de diciembre de 2017 a través del vínculo https://www.eleconomista.com.mx/empresas/La-Suprema-Corte-confirma-sentencia-contra-Google-en-Mexico-20171206-0075.html

RIVOLTA, Mercedes. *Construyendo el Estado Nació para el crecimiento y la Equidad. Panel: Gobierno Electrónico: Experiencias en el poder legislativo y judicial*. Cuarto congreso argentino de administración pública. Buenos Aires, Argentina. 22-25 de agosto de 2007. Disponible a través del vínculo http://www.congresoap.gov.ar/sitio/objetivos.html

SAMSUMG. Soluciones para dispositivos Móviles. Encriptación de datos. Consultado el 01 de junio de 2017 a través del vínculo http://www.samsung.com/es/business/solutions-services/mobile-solutions/security/encryption

SAN MARTIN, José Ignacio. *Marcas y nombres de dominio: solución de controversias*. ELZABURU. Abril de 2016. Consulta en línea a través del vínculo http://www.oepm.es/export/sites/oepm/comun/documentos_relacionados/Ponencias/101_03_II_Jornadas_Sobre_Propiedad_Intelectual_e_Industrial.pdf

SAUER, BEATE. *Central bank behaviour concerning the level of bitcoin regulations as a policy variable*. Athens Journal of Business and Economics. Athens Institute for Education & Reasearch (A World Association of Academics and Researchers. Grecia. Octubre de 2015. Visto el 01 de diciembre de 2017 a través del vínculo http://www.athensjournals.gr/business/2015-1-4-1-Sauer.pdf

SEMANA 25. *Testamento Digital*. Tecnología. Colombia, diciembre de 2014. Puede consultar la nota completa a través del vínculo http://www.semana.com/vida-moderna/articulo/testamento-digital/395286-3

SHINEN, Brock. *The Misunderstandings of Ownership*. Twitter Logical. Shinen Law Coporation. 2009. Visto el 18 de noviembre de 2017, a través del vínculo http://canyoucopyrightatweet.com/

SILLS, Anthony. *ROSS and Watson tackle de Law*. Cognitive Enterprise. Watson. IBM. 14 de enero de 2016. Visto el 24 de noviembre de 2017 a través del vínculo https://www.ibm.com/blogs/watson/2016/01/ross-and-watson-tackle-the-law/

SOFTDOIT. ¿Qué es el código fuente? Puede consultar el texto íntegro, a través del vínculo https://www.softwaredoit.es/definicion/definicion-codigo-fuente.html visto el 15 de noviembre de 2017.

SOMONITE, Tom, et al. *Tenemos que hablar de internet como un derecho humano*. MIT TECHNOLOGY REVIEW. Abril de 2017. Puede consultar el texto íntegro de la entrevista al inventor de internet, a través del vínculo https://www.technologyreview.es/s/7615/tenemos-que-hablar-de-internet-como-un-derecho-humano Visto el 25 de junio de 2017.

STALLMAN, Richard. *Por qué el código abierto pierde de vista lo esencial del software libre*. El sistema operativo GNU. Patrocinado por Free Software Foundation. Última actualización 11 de octubre de 2017. Visto el 16 de noviembre a través del vínculo https://www.gnu.org/philosophy/open-source-misses-the-point.es.html El texto original en inglés se intitula *Why Open Source misses the point of Free Software*.

SUÁREZ MAGALLANES, Amanda. *El senado de EEUU aprueba por unanimidad la Music Modernization Act*. España, 24 de septiembre de 2018. Instituto de Derecho de Autor. Derechos PI, Legislación, Legislación internacional. Visto el 21 de octubre de 2018 a través del vínculo http://www.institutoautor.org/es-ES/SitePages/EstaPasandoDetalleActualidad.aspx?i=2176&s=1

SUÁREZ, Eduardo. "Facebook compra WhatsApp por 19.000 millones de dólares". *El Mundo*. Edición España. Corresponsal en Nueva York, nota del 20 de febrero de 2014. Visto el 13 de febrero de 2018 a través del vínculo http://www.elmundo.es/economia/2014/02/19/53052f1e268e3eed5d8b456c.html

SWGDE. *Best practices for digital & multimedia evidence video acquisition from Cloud Storage*. Estados Unidos de América. Versión 1.0. Octubre 17 de 2017. Disponible en línea a través del vínculo https://www.swgde.org/documents/Released%20For%20Public%20Comment/SWGDE%20Best%20Practices%20for%20Digital%20and%20Multimedia%20Evidence%20Video%20Acquisition%20from%20Cloud%20Storage

SYMANTEC SECURITY RESPONSE. *What you need to know about the WannaCry Ransomware*. Publicado el 23 de octubre de 2017. Visto el 9 de diciembre a través del vínculo https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack

TARDIF CHALIFOUR, Eric. *El Derecho al Olvido Digital: Entre el Derecho a la Privacidad y el Derecho a la Libertad de Expresión*. Foro Jurídico. México, 2 de diciembre de 2016. Visto el 14 de diciembre de 2017 a través del vínculo https://www.forojuridico.org.mx/derecho-al-olvido-digital-derecho-la-privacidad-derecho-la-libertad-expresion/

TARTAKOFF, Joseph. *Forbes. Analyst: YouTube Will Lose Almost $500 Million This Year.* Publicación del 4 de marzo de 2009. Consultado el 20 de abril del año 2017 a través del vínculo https://www.forbes.com/2009/04/03/youtube-loses-money-technology-paidcontent.html

TCM/ EL UNIVERSAL. *Twitter tiene 35.3 millones de usuarios en México.* Notimex. 16 de marzo de 2016. Visto el 18 de noviembre de 2017 a través del vínculo http://www.eluniversal.com.mx/articulo/cartera/negocios/2016/03/16/twitter-tiene-353-millones-de-usuarios-en-mexico

TECHBIT. EL UNIVERSAL. *WhatsApp supera los mil millones de usuarios activos al día.* Periódico en línea del Universal. Redacción y Agencias. México, 28 de julio de 2017. Visible el 13 de febrero de 2018 a través del vínculo http://www.eluniversal.com.mx/articulo/techbit/2017/07/28/whatsapp-supera-los-mil-millones-de-usuarios-activos-al-dia

Techbit. *Enfrenta Youtube.mp3 acciones legales a nivel internacional.* El Universal. Septiembre de 2016, México. Pude consultar la nota completa a través de http://www.eluniversal.com.mx/articulo/techbit/2016/09/28/enfrenta-youtubemp3-acciones-legales-nivel-internacional

TECHNET, Microsoft. ¿Qué son los medios digitales? En el mismo artículo, se analiza los formatos digitales que se encuentran disponibles para los productos de la familia Microsoft, tales como WMA, WMV, MP3, JPEG y AVI. Puede consultar el texto íntegro a través de https://technet.microsoft.com/es-es/library/what-is-digital-media-2(v=ws.11).aspx

TEPP, Steven. *Big Data and Intellectual Property Go Hand in Hand.* U.S. Chamber of Commerce Foundation. Abril 25 de 2014. Recuperado el 14 de diciembre de 2017 a través del vínculo https://www.uschamberfoundation.org/blog/post/big-data-and-intellectual-property-go-hand-hand/34384

TURING, Alan. *Computing Machinery and Intelligence.* Mind 49. 1950; mismo que se puede consultar en línea a través de http://www.csee.umbc.edu/courses/471/papers/turing.pdf

TWITTER. *Política de derechos de autor*. https://support.twitter.com/articles/20170921#3. Visto el 18 de noviembre de 2017

U.S.SECRETE SERVICE *Best Practices for Seizing Electronic Evidence v.3. A Pocket Guide For First Responders.* US Dept of Homeland Security. 2007. http://www.listcrime.com/BestPracticesforSeizingElectronicEvidence.pdf

UN/ ITU. *Digital Divide closing, but still significant, says United Nations Telecoms agency.* Centro de Noticias. 11 de octubre de 2012. Visto el 10 de diciembre de 2017 a través del vínculo http://www.un.org/apps/news/story.asp?NewsID=43265#.Wi4GsdKWbIU

UNESCO. *Carta sobre la preservación del patrimonio digital.* 15 de octubre de 2003. Versión en español que se puede consultar a través del portal http://portal.unesco.org/es/ev.php-URL_ID=17721&URL_DO=DO_TOPIC&URL_SECTION=201.html

UNESCO. *Memory of the World. Directrices para la preservación del patrimonio digital*. Preparado por la Biblioteca Nacional de Australia. División de la Sociedad de la Información. Puede consultar la versión en español de este documento a través del vínculo http://unesdoc.unesco.org/images/0013/001300/130071s.pdf

UNIVISION. *Hacker mexicano condenado a seis años de cárcel por "sextorsión"*. Medio Tiempo. Publicado el 01 de septiembre de 2011. Noticias. Visto el 7 de diciembre de 2017 a través del vínculo http://www.univision.com/noticias/hacker-mexicano-condenado-a-seis-anos-de-carcel-por-sextorsion

UNOCERO. *Ni se te ocurra transmitir una película en Facebook. Un joven es arrestado por haber transmitido Deadpool en vivo*. España. 18 de junio de 2017. Visto el 24 de noviembre de 2017, a través del vínculo https://www.unocero.com/noticias/cine/se-te-ocurra-transmitir-una-pelicula-facebook/

VALENCIA MONGE, Juan G. *Validez jurídica de los contratos por internet*. Temas de derecho civil en homenaje al doctor Jorge Mario Magallón Ibarra. Porrúa. México, 2011. Visto el 29 de noviembre de 2017 a través del vínculo https://archivos.juridicas.unam.mx/www/bjv/libros/8/3861/20.pdf

VIÑAS, Verónica. *Los nuevos mecenas de la cultura*. Diarios de León. Cultura. España, 7 de agosto de 2012. Recuperado el 13 de diciembre de 2017 a través del vínculo http://www.diariodeleon.es/noticias/cultura/los-nuevos-mecenas-de-cultura_714384.html

WARREN, Samuel & BRANDEIS, Louis. *The Right to Privacy*. Hard Law Review. Vol. 14. Número 5. Diciembre 15 de 1890. Recuperado el 14 de diciembre de 2017 a través del vínculo http://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf

WhatsApp Inc. *Privacidad y Términos. Cifrado de extremo a extremo*. Preguntas frecuentes. 2018. Visto el 28 de febrero de 2018 a través del vínculo https://faq.whatsapp.com/es/general/28030015

WIPO Internet Domain Name Process. *La gestión de nombres y direcciones de internet: cuestiones de Propiedad Intelectual* "Informe Final sobre el Proceso de la OMPI relativo a los Nombres de Dominio de Internet" de 30 de abril de 1999. Consultable en línea, a través de http://www.wipo.int/amc/es/processes/process1/report/finalreport.html Visible el día 21 de febrero de 2017.

Referencias Legislativas, Normas y Precedentes en Derecho Comparado

ACURIO DEL PINO, Santiago. *Manual de Manejo de Evidencias Digitales y Entornos Informáticos. Versión 2.0*. Dirección Nacional de Tecnología de la Información. *Organization of American States*. Washington, D.C. Visto el 04 de diciembre a través del vínculo https://www.oas.org/juridico/spanish/cyber/cyb47_manual_sp.pdf

APC. *Carta APC sobre derechos en internet.* Estados Unidos, Noviembre de 2006. Visto el 15 de diciembre de 2017 a través del vínculo https://www.apc.org/es/pubs/carta-de-apc-sobre-derechos-en-internet

ARCHIVO GENERAL DE LA NACIÓN. *Uso de tecnologías avanzadas en materia de archivo. Decreto Legislativo 681.* 11 de octubre de 1991, Perú. Visto a través del vínculo http://webapp.regionsanmartin.gob.pe/sisarch/LEGISLACION/6.%20TECNOLOGIA%20AVANZADA%20EN%20ARCHIVOS/DL_No_681.pdf

ASAMBLEA LEGISLATIVA PLURINACIONAL DE BOLIVIA. *Ley General de los Derechos de las Usuarias y los Usuarios y de las Consumidoras y los Consumidores.* Ley número 453 de 4 de diciembre de 2013, publicada por el Presidente Constitucional Evo Morales. Puede consultar el texto íntegro a través del vínculo http://www.wipo.int/edocs/lexdocs/laws/es/bo/bo044es.pdf]

BANCO CENTRAL DO BRASIL. *Law 12,865 de octubre 9 de 2013.* SPB (Sistema de pagamentos Brasileiro). Regulación de esquemas de pago e instituciones de pago que de ahora en adelante formarán parte del Sistema de Pagos Brasileño. Traducción del portugués al inglés por *DEBAN (Department of Banking Operations and Payments System).* Puede consultar el texto íntegro a través vínculo https://www.bcb.gov.br/Pom/Spb/Ing/InstitucionalAspects/Law12865.pdf visto el 01 de diciembre de 2017.

BANCO DE MÉXICO. *Circular 12/2018.* México, 10 de septiembre de 2018. Firma el Director General de Operaciones y Sistemas de pagos, así como el Director General Jurídico. Diario Oficial de la Federación. Visto el 21 de octubre de 2018 a través del vínculo https://www.dof.gob.mx/nota_detalle.php?codigo=5537421&fecha=10/09/2018

BOLIVIA. *Código Penal aprobado por DL 10426 de 23/08/1972, elevado al rango de Ley por Ley 1768 de 10/03/1997.* Vigente a partir del año 1973. Visto el 7 de diciembre de 2017 a través del vínculo https://bolivia.infoleyes.com/norma/1401/codigo-penal-cp

CÁMARA DE DIPUTADOS DE LA NACIÓN DE ARGENTINA. *Firma Digital. Ley 25.506.* Promulgada el 11 de diciembre de 2001. Argentina. Visible el 04 de diciembre de 2017 a través del vínculo http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/norma.htm

CÁMARA DE DIPUTADOS DEL CONGRESO DE LA UNIÓN. *Código Federal de Procedimientos Civiles.* Publicado el 09 de abril de 2012 en el Diario Oficial de la Federación. Visible el 13 de febrero de 2018 a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/6.pdf

CÁMARA DE DIPUTADOS DEL CONGRESO DE LA UNIÓN. *Código Nacional de Procedimientos Penales.* Publicado el 17 de junio de 2016 en el Diario Oficial de la Federación. Visible el 13 de febrero de 2018 a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/CNPP_170616.pdf

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. Ley de Propiedad Industrial. Consultada en línea el 21 de febrero de 2017 a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/ref/lpi.htm

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Expedida el 05 de julio de 2010. Se puede consultar el texto íntegro de la ley, a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. Ley Federal del Derecho de Autor vigente. Puede consultar la misma a través del vínculo http://www.dof.gob.mx/nota_detalle.php?codigo=4907028&fecha=24/12/1996

CANADÁ. *Criminal Code R.S.C. 1985.* Con enmienda del pasado 18 de octubre de 2017. Visto el 7 de diciembre de 2017 a través del vínculo http://laws-lois.justice.gc.ca/eng/acts/C-46/

CNUDMI. *Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996).* Visto el 21 de noviembre de 2017 a través del vínculo https://documents-dds-ny.un.org/doc/UNDOC/GEN/N97/763/60/PDF/N9776360.pdf?OpenElement

CNUDMI. *Situación actual Ley Modelo de la CNUDMI sobre Comercio Electrónico (1996).* Visto el 27 de noviembre a través del vínculo http://www.uncitral.org/uncitral/es/uncitral_texts/electronic_commerce/1996Model_status.html

CÓDIGO CIVIL FRANCÉS en materia de prueba de las obligaciones, así como la reforma 2004/575 de 21 de julio de 2000, por la que se prescribe el poder vinculatorio de la firma digital. Puede consultar el texto íntegro a través del vínculo https://www.legifrance.gouv.fr/content/download/1966/13751/.../Code_41.pdf

COMMONWEALTH SECRETARIAT. *Model La won Computer and Computer Related Crime.* Vista el 9 de diciembre de 2017 a través del vínculo http://www.thecommonwealth-ilibrary.org/commonwealth/governance/2002-meeting-of-commonwealth-law-ministers-and-senior-officials/model-law-on-computer-and-computer-related-crime_9781848598188-16-en

CONGRESO DE COLOMBIA. *Ley 527 de 1999.* República de Colombia. Publicada el 18 de agosto de 1999. Puede consultar el texto íntegro a través del vínculo http://www.cancilleria.gov.co/sites/default/files/tramites_servicios/apostilla_legalizacion/archivos/ley_527_1999.pdf

CONGRESO DE LA REPÚBLICA DE COLOMBIA. *Proyecto de Ley 134 de 2015.* Visto el 13 de diciembre de 2017 a través del vínculo http://www.imprenta.gov.co/gacetap/gaceta.mostrar_documento?p_tipo=05&p_numero=134&p_consec=42958

CONGRESO DE LA UNIÓN. *Constitución Política de los Estados Unidos Mexicanos.* Visible a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf

CONGRESO DE LA UNIÓN. *Ley Federal de Procedimiento Contencioso Administrativo.* México. Última reforma publicada en el *Diario Oficial de la Federación*

el 27 de enero de 2017. Puede consultar el texto íntegro a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPCA_270117.pdf

CONGRESO DE LA UNIÓN. *Ley Federal para la prevención e identificación de operaciones con recursos de procedencia ilícita.* Publicado el 17 de octubre de 2012 en el *Diario Oficial de la Federación*. México. http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPIORPI.pdf

CONGRESO DE LA UNIÓN. *Lineamientos Técnicos y formales para la sustanciación del juicio en línea*. Publicado en el *Diario Oficial de la Federación* el 04 de mayo de 2011. Puede consultar el texto íntegro a través del vínculo http://dof.gob.mx/nota_detalle.php?codigo=5188284&fecha=04/05/2011

CONGRESO DE LA UNIÓN MÉXICO. *Código de Comercio*. Texto publicado el 13 de diciembre de 1889, cuya última reforma ocurrió el 02 de mayo de 2017. Visto el 27 de noviembre de 2017 a través del vínculo http://www.diputados.gob.mx/LeyesBiblio/pdf/3_020517.pdf

CONGRESO DE LOS ESTADOS UNIDOS DE AMÉRICA. *Public Law 107-204-Julio 30, 2002 Sarbanes-Oxley Act of 2002. Corporate responsibility.* Congreso 107°mo. Visto el 11 de diciembre de 2017 a través del portal https://www.sec.gov/about/laws/soa2002.pdf

CONGRESO NACIONAL DE CHILE. *Ley 19223.* Biblioteca del Congreso Nacional. Promulgada el 28 de mayo de 1993 y publicada el 7 de junio del mismo año por el Ministerio de Justicia. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_chi_ley_19223.pdf

CONGRESO NACIONAL DE ECUADOR. *Ley de comercio electrónico, firmas electrónicas y mensajes de datos (Ley 2002-67).* Registro oficial 557-S, 17-IV-2002. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_ecu_ley_comelectronico.pdf

CONSEJO EUROPEO. *Convenio Sobre la Ciberdelincuencia.* Budapest, 23 de noviembre de 2001. Texto en español a través del vínculo https://rm.coe.int/16802fa41c Puede consultar el texto oficial en inglés, a través del vínculo https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561.

CONVENCIÓN AMERICANA SOBRE DERECHOS HUMANOS. Puede consultar el texto íntegro a través de https://www.colmex.mx/assets/pdfs/4-CADH_51.pdf?1493133911

CONVENIO DE BERNA, artículo 9.2, consultado en línea a través del portal http://www.wipo.org el 17 de abril de 2015

COPYRIGHT GOV. *Chapter 1.1: Subject Matter and Scope of Copyright. Section 119. Limitation on exclusive rights: Secondary transmissions of distant television programming by satellite.* Puede consultar el texto íntegro en el vínculo https://www.copyright.gov/title17/92chap1.html#109

CORTE AMERICANA DE APELACIÓN DEL NOVENO CIRCUITO. *Kevin Khoa Nguyen V. Barnes & Noble, INC.* Apelación número 12-56628 de 18 de agosto

de 2014. Puede consultar el texto íntegro a través del vínculo http://cdn.ca9.uscourts.gov/datastore/opinions/2014/08/18/12-56628.pdf

CORTE CONSTITUCIONAL. *Constitución Política de Colombia.* Consejo Superior de la Judicatura. Centro de Documentación Judicial-CENDOJ. Biblioteca Enrique Low Murtra. Actualizado 2016. Recuperado el 14 de diciembre de 2017 a través del vínculo http://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia.pdf

CORTE DE APELACIÓN DEL QUINTO DISTRITO DE ILLINOIS. *Dewayne Hubbert V Dell Corporation.* Apelación del Circuito de Madison. Número 5-03-0643. Notificado el 8 de diciembre de 2005.

COUNCIL OF THE EUROPEAN UNION. *General Data Protection Regulation.* Bruselas, 6 de abril de 2016. Visto el 13 de diciembre de 2017 a través del vínculo http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

ESTADOS UNIDOS DE AMÉRICA. *U.S. Code Part I- Crimes- Title 18.* Vista el 7 de diciembre de 2017 a través del vínculo https://www.law.cornell.edu/uscode/text/18/part-I

EUROPEAN COMISSION. *Factsheet on the Right to be Forgotten ruling (C-131/12).* Press release. Justice. Recuperado el 14 de diciembre de 2017 a través del vínculo http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf

GOB.MX/ México Digital. *Carta Internacional de Datos Abiertos.* Acciones y Programas. México, 30 de septiembre de 2015. Visible el 16 de diciembre de 2017 a través del vínculo https://www.gob.mx/mexicodigital/acciones-y-programas/carta-internacional-de-datos-abiertos

GOVERNMENT OF BARBADOS. *Computer Misuse Act 2005.* Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_bbs_computer_misuse_2005.pdf

GUYANA. *Interception of communication Act 2008.* Acta 21 de 2008. Autorizado por la Asamblea Nacional el 17 de octubre de 2008. Vista el 7 de diciembre a través del vínculo http://www.oas.org/juridico/mla/en/guy/en_guy_Inter_Commun_Act_2008.pdf

GWG/UN. *Bogota Declaration.* 4th Global Conference on Big Data for Official Statisitics. 8-10 November 2017. Colombia. https://unstats.un.org/unsd/bigdata/conferences/2017/Bogota%20declaration%20-%20Final%20version.pdf

INTERNET RIGHTS & PRINCIPLES COALITION. *Carta de Derechos Humanos y Principios en Internet.* Enero de 2015. Primera Edición. Organización de las Naciones Unidas. Visto el 15 de diciembre de 2017 a través del vínculo http://internetrightsandprinciples.org/site/wp-content/uploads/2017/03/IRPC_spanish_1stedition_final.pdf

JAMAICA. *Acta 2010 sobre Cibercrímenes.* Aprobada por la casa de representantes el 16 de febrero de 2010. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/PDFs/jam_act2010.pdf

JEFATURA DEL ESTADO, MINISTERIO DE LA PRESENCIA, RELACIONES CON LAS CORTES E IGUALDAD, GOBIERNO DE ESPAÑA. *Ley 1/2000*. 7 de enero, de Enjuiciamiento Civil. BOE número 7, de 8 de enero de 2000. Visto a través del Boletín Oficial del Estado en https://boe.es/buscar/act.php?id=BOE-A-2000-323

JEFATURA DEL ESTADO, MINISTERIO DE LA PRESENCIA, RELACIONES CON LAS CORTES E IGUALDAD, GOBIERNO DE ESPAÑA. *Ley 59/2003*. 19 de diciembre, de firma electronica. BOE número 304, de 20 de diciembre de 2003, páginas 45329 a 45343. Visto a través del Boletín Oficial del Estado en https://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399

JUSTIA. *Silverthorne Lumber Co., Inc. v. United States, 251 U.S. 385 (1920)*. Visible el 02 de diciembre de 2017 a través del vínculo https://supreme.justia.com/cases/federal/us/251/385/case.html

KAYE, David. *Informe del Relator Especial sobre la Promoción y protección del derecho a la libertad de opinión y de expresión.* Consejo de Derechos Humanos. 29° período de sesiones. Asamblea General de las Naciones Uuidas. A/HRC/29/3. 22 de mayo de 2015. Visto el 16 de diciembre de 2017 a través del vínculo http://www.eldiario.es/cultura/G1509588_EDIFIL20151209_0001.pdf

LA RUE, Frank. *Report of the special rapporteur on the promotion and protection of the right to freedom of opinion and expression.* Human Rights Council. Seventeenth session. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development. General Assembly. Uuited Nations. 16 mayo de 2011. A/HRC/17/27. Puede consultar la versión original –en inglés- a través del vínculo http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf Visto el 25 de junio de 2017.

LAS BAHAMAS. *Computer Misuse Act 2003.* Aprobada el 11 de abril de 2003 y entrada en vigor el 16 de junio del mismo año. Vista el 7 de diciembre de 2017 a través del vínculo http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf

LEGISLATIVE HISTORY. *Digital Millennium Copyright Act.* Public Law 105-304. 20 de octubre de 1998. Visible el 14 de agosto de 2018 a través del vínculo http://www.wipo.int/wipolex/es/text.jsp?file_id=337359

Ley 10/2017, de 27 de junio, de las voluntades digitales y de modificación de los libros segundo y cuarto del Código civil de Cataluña. Comunidad Autónoma de Cataluña. 21 de julio de 2017. Puede consultar el texto íntegro, a través del vínculo https://www.boe.es/diario_boe/txt.php?id=BOE-A-2017-8525

Ley 34/2002 para regular los servicios de la sociedad de la información y comercio electrónico, por la jefatura del Estado. Puede consultar el texto íntegro de la ley a través del vínculo https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

Ley 428884-6 que modifica la Ley de Información, Tecnologías de la Información y Protección de la Información de la Federación Rusa

Ley 5/2015, de 27 de abril, de fomento de la financiación empresarial. *Ley 5/2015.* BOE-A-2015-4607. Documento consolidado BOE Número 101, de 28 de abril de 2015. España. Visto el 13 de diciembre de 2017 a través del vínculo https://www.boe.es/buscar/act.php?id=BOE-A-2015-4607

Ley 59/2003, de 19 de diciembre, de firma electrónica. Publicado en «BOE» núm. 304, de 20 de diciembre de 2003, páginas 45329 a 45343, España. Artículo 3°. Puede consultar el texto íntegro a través del vínculo https://www.boe.es/buscar/doc.php?id=BOE-A-2003-23399

Ley de Transacciones Electrónicas, aprobada por Decreto en todos los Estados, en julio de 1999.

LIBRARY OF CONGRESS. *Regulation of Bitcoin in selected jurisdictions.* Estados Unidos de América. Dirección de Búsqueda Global Legal. Enero de 2014. Puede consultar el listado en el vínculo https://www.loc.gov/law/help/bitcoin-survey/

MINISTERIO DE ECONOMÍA, *Norma Ley 20217. Modifica el código de Procedimiento Civil y la Ley número 197999 sobre documento electrónico, firma electrónica y los servicios de certificación de dichas firmas.* 12 de uoviembre de 2007, Chile. Visto a través de la Biblioteca del Congreso Nacional de Chile en https://www.leychile.cl/Navegar?idNorma=266348

NEW YORK STATE/ DEPARTMENT OF FINANCIAL SERVICES. *Chapter 1. Regulations of the superintendent of financial services. Part 200. Virtual Currencies.* Edición de 24 de junio de 2015. Visible a través del vínculo http://www.dfs.ny.gov/legal/regulations/adoptions/dfsp200t.pdf

OFFICE OF THE UNITED STATES TRADE REPRESENTANTIVE. *United States-Mexico-Canada Agreement Agreement (USMCA).* Estados Unidos de América, Septiembre de 2018. Executive Office of the President. Resource Center. Visto el 21 de octubre de 2018 a través del vínculo https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/19%20Digital%20Trade.pdf

OMPI. *Tratado de la OMPI sobre Derecho de Autor.* Adoptado en Ginebra el 20 de diciembre de 1996. Visible el 14 de agosto de 2018 a través del vínculo http://www.wipo.int/wipolex/es/treaties/text.jsp?file_id=295158

OPEN DATA CHARTER. *Carta Internacional de Datos Abiertos. Principios.* Versión completa en español. Octubre 28 de 2015. Visto el 16 de diciembre de 2017 a través del vínculo https://opendatacharter.net/principles-es/

PARAGUAY. *Código Penal de Paraguay Ley 1.160/97.* Visto el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_par_cod_penal.pdf

PARLAMENTO EUROPEO. *Normas de Derecho civil sobre robótica P8_TA(2017)0051.* Estrasburgo, 16 de febrero de 2017. Visible el 28 de octubre de 2018 a través del vínculo http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//ES

PROCURADURÍA GENERAL DE LA REPÚBLICA. *Protocolos de cadena de custodia. Dos grandes etapas: preservación y procesamiento.* México. Instituto Nacional de Ciencias Penales. 2012. 2ª edición. Visible el 13 de febrero de 2018 a través del vínculo http://www.inacipe.gob.mx/stories/publicaciones/descargas_gratuitas/ProtocolosdeCadenadeCustodia.pdf

REPÚBLICA DE COLOMBIA/ GOBIERNO NACIONAL. *Ley 1273/2009.* Bogotá, 5 de enero de 2009. Ministerio del Interior y Justicia. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_col_ley1273.pdf

REPÚBLICA DEL ECUADOR. ASAMBLEA NACIONAL. *Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación.* Publicada el 01 de diciembre de 2016. Puede consultar el texto íntegro a través del vínculo http://www.wipo.int/wipolex/fr/text.jsp?file_id=439750

REPÚBLICA DOMINICANA. *Ley 53-07 Crímenes y delitos de alta tecnología.* Promulgada el 23 de abril de 2007 por el presidente Leonel Fernández. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/PDFs/repdom_ley5307.pdf

SAINT VINCENT AND THE GRENADINES. *Electronic Transactions Act 2007.* Aprobada por la asamblea de representantes en 2007. Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_svg_electronic_act_2007.pdf

SECRETARÍA DE ECONOMÍA. *Norma Oficial Mexicana NOM-151-SCFI-2016 Requisitos que deben observarse para la conservación de mensajes de datos y digitalización.* México, 30 de marzo de 2017. Diario Oficial de la Federación. Visible el 19 de agosto de 2018 a través del vínculo http://dof.gob.mx/nota_detalle.php?codigo=5478024&fecha=30/03/2017

SECRETARÍA DE HACIENDA Y CRÉDITO PÚBLICO. *Disposiciones de carácter general aplicables a las Instituciones de Tecnología Financiera.* México, 10 de septiembre de 2018. Diario Oficial de la Federación. Firma el Presidente de la Comisión Nacional Bancaria y de Valores el 07 de septiembre de 2018. Visto el 21 de octubre de 2018 a través del vínculo https://www.dof.gob.mx/nota_detalle.php?codigo=5537450&fecha=10/09/2018

SUPREMA CORTE DE JUSTICIA DE LA NACIÓN. Semanario Judicial de la Federación y su Gaceta. Visible a través del vínculo https://sjf.scjn.gob.mx/sjfsist/

VENEZUELA. *Ley Especial contra los delitos informáticos.* Vista el 7 de diciembre de 2017 a través del vínculo http://www.oas.org/juridico/spanish/cyb_ven_LEY%20ESP_CON_DELI_INFOR.pdf