MISIÓN JURÍDICA

La importancia de la ciberseguridad y los derechos humanos en el entorno virtual

The importance of cyber security and human rights in the virtual environment

Autores: Erick Francisco Tapia Hernández, Raúl Ruiz Canizales y Antonio Vega Páez

DOI: https://doi.org/10.25058/1794600X.1912

LA IMPORTANCIA DE LA CIBERSEGURIDAD Y LOS DERECHOS HUMANOS EN EL ENTORNO VIRTUAL *

The importance of cyber security and human rights in the virtual environment

A importância da cibersegurança e dos direitos humanos no ambiente virtual

Erick Francisco Tapia Hernández [a]
erick.tapia@uaq.mx

Raúl Ruiz Canizales[b]
canizales@uaq.mx

Antonio Vega Páez[c]
vegapaez@uaq.mx

Fecha de recepción: 1 de octubre de 2020
Fecha de revisión: 12 de octubre de 2020
Fecha de aceptación: 27 de noviembre de 2020

DOI: https://doi.org/10.25058/1794600X.1912

Para citar este artículo:
Tapía Hernández, E.; Canizales Ruiz, R. y Vega Páez, A. (2021). La importancia de la ciberseguridad y los derechos humanos en el entorno virtual. *Revista Misión Jurídica, 14*, (20), 142-158.

RESUMEN

El presente artículo enfatiza la necesidad de una cultura de la ciberseguridad de los usuarios, ante las amenazas y los riesgos a los que se exponen en el entorno virtual, derivados del desconocimiento y las afectaciones que ello ocasiona, mismas que a simple vista parecen inofensivas, pero que repercuten de forma importante en los derechos humanos de las víctimas como la vida, integridad psicológica, intimidad, privacidad o el patrimonio.

Por lo anterior, se mencionan algunas de las amenazas más importantes, se destaca que existen delitos que utilizan como medio de comisión el entorno virtual y que hay delitos que surgen dentro de dicho

** Artículo de investigación científica que presenta resultados de un proyecto de Investigación de la Universidad Autónoma de Querétaro. (Realizado con financiamiento propio). No. de registro: FDE202004.*

a. Tapia Hernández, Erick Francisco. Licenciado, Especialista en Derecho Constitucional y Administrativo, Maestro y Doctor en derecho con Posdoctorado en Ciencias Sociales. Profesor e investigador de la Facultad de Derecho de la Universidad Autónoma de Querétaro.

b. Ruíz Canizalez, Raúl. Licenciado, Especialista, Maestro y Doctor en derecho. Profesor e investigador de la Facultad de Derecho de la Universidad Autónoma de Querétaro, en la que también funge como Jefe de Posgrado de la misma Facultad.

c. Vega Páez, Antonio. Maestro en Ciencias Computacionales. Profesor investigador de la Facultad de Derecho de la Universidad Autónoma de Querétaro, en la que también funge como Coordinador de informatización.

entorno. Así mismo, se señalan algunos derechos humanos originados desde el entorno virtual, y cuyo reconocimiento por parte de los Estados es necesario para así garantizarlos

PALABRAS CLAVES

Ciberseguridad; ciberdelitos; ciberamenazas; derechos humanos; derecho al olvido en el ciberespacio; seguridad y prevención.

ABSTRACT

This article highlights the need for a culture of cybersecurity for users, the threats and risks they face in the virtual environment derived from their lack of knowledge and the effects they have, which at first sight may seem harmless but have a significant impact on the human rights of the victims such as life, psychological integrity, intimacy, privacy or patrimony.

Therefore, some of the most important threats are mentioned, emphasizing that there are crimes that use the virtual environment as a means of commission and that there are crimes that arise within this environment. Similarly, some human rights that have arisen from the virtual environment are pointed out and whose recognition by the States is necessary in order to guarantee them.

KEY WORDS

Cybersecurity, cybercrime, cyber threats, human rights, right to be forgotten in cyberspace, security and prevention.

RESUMO

Este artigo enfatiza a necessidade de uma cultura de cibersegurança para os usuários, diante das ameaças e riscos a que estão expostos no ambiente virtual, derivados do desconhecimento e dos efeitos que isso causa, que à primeira vista parecem inofensivos, mas que têm um impacto importante sobre os direitos humanos das vítimas, como vida, integridade psicológica, privacidade, privacidade ou patrimônio.

Assim, são mencionadas algumas das ameaças mais importantes, realça-se que existem crimes que utilizam o ambiente virtual como meio de perpetramento e que existem crimes que surgem nesse ambiente. Da mesma forma, são apontados alguns direitos humanos oriundos do meio virtual, cujo reconhecimento por parte dos Estados é necessário para garanti-los.

PALAVRAS-CHAVES

Cibersegurança; cibercrime; ameaças cibernéticas; direitos humanos; direito de ser esquecido no ciberespaço; segurança e prevenção.

> "La única computadora segura es la que está desenchufada, a los amantes de la ingeniería social les gusta responder que siempre se puede convencer a alguien para que la enchufe. El factor humano es el eslabón más débil de la seguridad informática, y no hay un sólo equipo en el mundo que no dependa de un ser humano" (Jara, H. y Pacheco, F.G., 2012, pp.295-296).

INTRODUCCIÓN

Actualmente las comunicaciones y relaciones sociales se dan a través de los diversos dispositivos electrónicos dentro de un entorno virtual; lo cual, si bien acorta distancias y permite tener acceso a una cantidad infinita de contenido en solo segundos, al mismo tiempo representa un grave riesgo para la seguridad de los ciudadanos y una constante amenaza a sus derechos humanos.

Asimismo, existe una delgada línea entre la respuesta que brinda el Estado para la protección a la seguridad en el entorno virtual y la simultánea vulneración o indebida limitación a los derechos humanos, tales como la privacidad, la intimidad y la no intervención de comunicaciones privadas, entre otros, que lejos de incidir en la solución de las amenazas que se presentan en el *ciberespacio*, se convierten en una nueva amenaza para los usuarios.

En ese sentido, es necesario que las personas conozcan las amenazas a las que se exponen en el entorno virtual, así como la vulneración a los derechos en específico que ocasionan cada una de éstas, con la finalidad de que su uso sea responsable y tomen acciones preventivas, en aras de proteger y salvaguardar sus derechos humanos y en consecuencia la seguridad en entornos digitales.

Sin embargo, los supuestos jurídicos establecidos en ocasiones se ven superados por

las hipótesis de hecho, debido a que la tecnología y las situaciones que se suscitan en el entorno virtual rebasan lo establecido en las normas, situación que se agrava en materia penal en la que solo se puede condenar a las personas aludiendo a la exacta aplicación de la ley en esta materia.

Por lo anterior, el presente artículo destaca la necesidad de crear una cultura de la *ciberseguridad* apoyada en el respeto a los derechos humanos con miras a la protección y garantía de la seguridad, lo que permitirá comprender las amenazas en el entorno virtual a las que se enfrentan los usuarios, así como llegar a medidas y herramientas que permitan el uso responsable del *ciberespacio*, teniendo conocimiento no solo de los derechos fundamentales que se vinculan al uso de la internet, sino de aquellos derechos humanos cuyo reconocimiento se encuentra discutiéndose y que han surgido en el entorno virtual.

METODOLOGÍA

La metodología que se utilizará pretende destacar la importancia que reviste el enfoque humanista, así como la trascendencia del cambio de paradigma al hacer necesario que el estudioso del Derecho y las Ciencias Sociales cuente con herramientas enfocadas en la interpretación y argumentación jurídica, que incidan en su capacidad de análisis, sentido crítico y en la habilidad de enlazar el conocimiento de forma interdisciplinaria en asuntos que inciden en el entorno virtual.

En esa tesitura, en el presente trabajo se evidencia el método deductivo, al indicar preceptos contenidos en la normatividad mexicana y la forma en que se plantean en determinados casos en concreto, relacionados al entorno virtual.

Asimismo, se favorece el método inductivo a través del análisis de problemas o fenómenos jurídicos, que permiten indicar el contenido esencial de los derechos humanos y sus límites del tema en la norma.

El método exegético se utiliza en el análisis de la connotación derecho al olvido, lo que permite analizar la problemática actual referente a la omisión de regular el tema.

Por lo que hace al método comparativo, se realiza un análisis de las formas de entender y comprender el Derecho en el uso de las tecnologías relacionadas al entorno virtual hoy en día, contrastándola con las mismas conductas cuando no son en dicho entorno y en relación con otros países.

1. AMENAZAS EN EL ENTORNO VIRTUAL

No resulta extraño que actualmente exista una proliferación de amenazas en el *ciberespacio*, ya que como señala Leiva (2015) es un medio rentable en cuanto a términos económicos se refiere, además de ser una herramienta de fácil acceso, permite que la comisión de conductas, que ponen en riesgo o vulneran derechos humanos, sean realizadas de forma anónima, desde cualquier parte del mundo y en consecuencia, en muchas ocasiones, bajo el cobijo de la impunidad.

Una de las principales amenazas que encontramos en el entorno virtual es el denominado *malware*, que se define como "cualquier tipo de aplicación no autorizada que resida en nuestro sistema [de los dispositivos electrónicos]…con la intención de dañar al usuario" (Dominicci, s.f.), comúnmente se les conoce como códigos maliciosos, los cuales si bien no ocasionan por sí solos un daño directo al usuario, tienen la intención de "recopilar información confidencial del usuario [y] controlar el equipo de forma remota para realizar más ataques o dañar el equipo" (García, 2016, p.60).

Dicha amenaza se considera de las más importantes, ya que facilita que las personas vean vulnerada su seguridad en el entorno virtual, debido a la gran cantidad de datos personales e información a la cual se le da acceso a terceros que se infiltran en los sistemas de los dispositivos electrónicos, por lo que si el *malware* por sí solo no genera un daño, es la puerta de entrada para la comisión de diversas conductas delictivas o que no estando tipificadas dañan a las personas.

Si bien es necesaria la acción del usuario para que su dispositivo sea infectado con *malware*, los cibercriminales hacen uso de la denominada ingeniería social, la cual se define como el "conjunto de técnica y trucos empleados por los intrusos y *hackers* para extraer información sensible de los usuarios de un sistema informático" (Gómez, 2011), lo que permite obtener información personal, contraseñas, números de cuenta bancaria y cualquier otra información, sin que el usuario se percate de la falsedad de

ISSN 1794-600X Número 20 • Enero - Junio de 2021

la página a la que le está proporcionando su información o de que el tercero que le solicita la información tiene la finalidad de hacerle daño o que se está colocando en situación de potencial víctima de un delito.

Al respecto, Gómez (2011) señala algunas técnicas que se utilizan mediante la ingeniería social, tales como: la suplantación de identidad del personal de empresas para obtener información; el envío de correos electrónicos masivos que suplantan la identidad de empresas, organizaciones o personas con la finalidad de que los usuarios ingresen sus contraseñas o brinden información personal, también conocidos como correos *spam*; aparición de ventanas emergentes que llevan al usuario a sitios web fraudulentos o que descargan archivos o programas con *malware* en el dispositivo del usuario, o páginas o mensajes a través de los servicios de mensajería instantánea que ofrecen falsas ofertas, promociones o descuentos a cambio de contestar encuestas, cuya finalidad es recopilar información personal sin que el usuario obtenga lo prometido.

Cabe mencionar, que la manipulación que se realiza mediante la ingeniería social, se enfoca incluso en temas de la actualidad por ser atractivos para el usuario o que se pueda realizar el engaño con mayor facilidad, verbigracia, actualmente con el tema del coronavirus, la ingeniería social se enfoca en el envío de correos masivos con comunicados falsos realizados por la OMS, que invitan al usuario a descargar archivos adjuntos para mayor información o aplicaciones que supuestamente le indican al usuario cuantas personas a su alrededor tienen Covid-19 a cambio del depósito de cierta cantidad de dinero, para lo cual le piden al usuario información bancaria, y una vez que éste la introduce, se convierte en víctima del robo de sus datos, contraseñas bancarias y posteriormente del retiro de dinero de sus cuentas, sin que la aplicación cumpla con lo ofrecido (Aguiar, 2020).

Esas amenazas representan un riesgo para la seguridad, aunado a la cantidad de datos personales que se comparten de forma pública en las redes, ante el desconocimiento de las amenazas a las que se enfrentan los usuarios en el entorno virtual, lo que los convierte en vulnerables. Marañón (2012) menciona que los jóvenes son aquellos que usan más las redes sociales, y que si bien muestran una gran capacidad de habilidades tecnológicas, descuidan el tema de proteger su intimidad, lo que facilita la comisión de delitos.

En el entorno virtual existen delitos que utilizan como medio de comisión dicho entorno y, delitos que surgen dentro de ese entorno; en el caso de los primeros, las conductas delictivas ya existen tipificadas y simplemente el delincuente utiliza como herramienta el entorno virtual para llevar a cabo el delito.

1.1. Extorsiones o amenazas por *malware*

Una de las conductas delictivas que existen previamente y se sofistican con el entorno virtual son las extorsiones o amenazas a través del *malware* como el denominado *ransomware* el cual "bloquea o cifra el contenido de un ordenador o dispositivo, exigiendo el pago de una recompensa para volver a ser disponible" (Ballestero, 2020, p. 42), uno de los casos más famosos fue el *ransomware* llamado *WannaCry*, en mayo del 2017, el cual bloqueó información de archivos de audio, imágenes, videos y documentos en diversas partes del mundo, posteriormente se le exigió al usuario el pago de un rescate, para restaurar esos archivos, el cual oscilaba entre los 300 y 600 dólares en criptomonedas (Gónzalez, 2018), ese ataque afectó a más 200,000 mil equipos en todo el mundo, incluidos 40 hospitales en Reino Unido y compañías de telecomunicaciones en España, además se registraron 366 pagos de rescate, de acuerdo con Tovar, González y García (2017) y en algunos casos, a pesar de haber realizado el pago los usuarios no recuperaron sus archivos.

Cabe señalar, que el pago del rescate que se exige en este tipo de amenaza, no garantiza que los archivos sean devueltos, como sucedió con el Hospital de Cardiología de Kansas en 2016, el cual pagó el rescate que les exigieron para descifrar sus archivos; sin embargo, solo liberaron algunos y les exigieron otro pago con la finalidad de devolverles los archivos restantes (Martínez, 2017). Una de las cuestiones preocupantes, es que actualmente ya no solo se exige un pago en dinero sino en especie, como en el caso de denominado *nRansomware*, cuyo rescate consistía en que la víctima enviara material íntimo de índole sexual (Sala, 2017).

1.2. Secuestro virtual

Otro delito es el denominado secuestro virtual, que es una modalidad del delito de extorsión, y consiste en contactar a una persona, a quien

amenazan con atentar contra su integridad física o vida en caso de no seguir las instrucciones que le indican, las cuales generalmente consisten en permanecer incomunicado y aislado en determinado lugar, con la finalidad de poder comunicarse posteriormente con sus familiares para solicitar el pago de un rescate derivado del supuesto secuestro físico de la víctima. Amescua (2010) nos indica que este delito tiene la característica de basarse en el engaño para obtener la colaboración de la víctima.

Este tipo de extorsión se ha sofisticado en el entorno virtual, ya que en muchas ocasiones los delincuentes cuentan con información y datos personales tanto de la víctima como de sus familiares, que obtienen a través de *malware* que infectó sus dispositivos electrónicos. Aunado a lo anterior, no es necesario que el delincuente se encuentre en el mismo espacio físico que la víctima, pues todo se realiza a través de un entorno virtual.

Uno de los últimos casos de secuestro virtual, tuvo lugar en la Ciudad de México, en mayo del 2020, en contra de 14 médicos adscritos al IMSS de Monterrey, quienes arribaron a la ciudad para solventar el déficit de personal médico ante la pandemia del Covid-19; sin embargo, recibieron amenazas vía telefónica y a través de videollamadas, en las que se les ordenó permanecer en determinado hotel bajo la amenaza de que estaban siendo vigilados, y que en caso de no seguir las instrucciones que les daban, atentarían contra sus vidas, posteriormente se pidió un rescate por 300,000 pesos para liberar al grupo de médicos (García, J., 2020).

1.3. Instigación virtual al suicidio

Este delito lo encontramos en el entorno virtual ejemplificadas con el denominado reto de la *Ballena Azul* que surgió en Rusia y tuvo repercusión a nivel mundial, el cual consistía en que adolescentes y niños seguían a diario un desafío, siendo un total de 50 desafíos, en el que último consistía en quitarse la vida (Ceballos-Espinoza, F., 2017). Si bien se considera que por sí sola la publicación de este tipo de retos en internet no es la única causa de que la persona cometa suicidio, éste incide en la comisión de este ante la influencia que genera en las víctimas para seguir este tipo de retos, ya sea que la conducta se consuma o no, aunado al hecho de que se registraron 130 muertes relacionados con este reto en países como México, Colombia, Chile, Brasil, Uruguay, España y Rusia (Agencia DPA, 2017).

Un reto similar, fue el de *Momo* que surgió en Japón y cuya repercusión de igual forma trascendió a nivel mundial, se difundió en redes sociales e incluso se filtró en videos de la plataforma Youtube Kids dirigidos para niños, esta forma de instigación por medio del entorno virtual reportó varios casos de niños a los que se les dio indicaciones para causarse daños a sí mismos o terminar con su vida (Estirado, 2019). En ese mismo país, en mayo de este año la luchadora profesional de 22 años Hana Kimura se suicidó después de recibir acoso cibernético luego de un incidente con un compañero en un reality show, sugiriéndole repetidamente que debería suicidarse (DW, 2020).

1.4. Divulgación de contenido íntimo de índole sexual en el entorno virtual

Aunado a los mencionados delitos, existen conductas que no se encontraban tipificadas previamente, en virtud de que nacen dentro de dicho entorno virtual. Existen muchos casos documentados respecto al contenido sexual en redes sociales en el entorno virtual y la falta de una regulación óptima como el caso de Daisy Coleman y Audrie Pott que lamentablemente terminaron en suicidio (Netflix, 2016).

En México, varios Estados han tipificado esta conducta, a raíz de la iniciativa impulsada por Olimpia Coral Melo Cruz, originaria de Puebla, quien fue víctima de divulgación de un video sexual que hizo con su novio, lo que provocó que recibiera insultos y acoso en redes sociales, ya que usuarios se burlaron de ella apodándola incluso como la *Gordibuena de Huachinango*, lo que repercutió en su integridad psicológica al ver expuesta su intimidad sexual, motivo por el cual intentó suicidarse en tres ocasiones (Rojas, 2019); sin embargo, se convirtió en activista con el objetivo de impulsar que dicha conducta no quedara impune en casos futuros, promoviendo la iniciativa denominada Ley Olimpia. Esta ley implicó un conjunto de reformas/adiciones en los ordenamientos de diversos estados y en la legislación federal, en la que merece resaltar las que se realizaron al Código Penal para el Distrito Federal, a la Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México, así como a la Ley General de Acceso a las Mujeres a una Vida Libre de Violencia. La conducta

ISSN 1794-600X Número 20 • Enero - Junio de 2021

antijurídica que se sanciona en cada una de ellas (divulgación de contenido íntimo de índole sexual en el entorno virtual), se engloba en la expresión 'violencia digital'. El caso de la "Ley Olimpia" es uno de los más frescos de cara a las agendas legislativas locales y la propia normativa nacional en las que se incorporan puntos de interés común como el de la violencia digital (Ruíz, 2020, pp. 17-38).

Atendiendo a la naturaleza y la forma como opera la violencia digital, se trata sin duda de un tipo de *violencia real*, de acuerdo con la propia taxonomía de G. Imbert (1992). Ahora bien, cuando se habla de violencia digital se hace en términos generales y, en su significación, la víctima puede ser cualquier persona independientemente de su edad, sexo, etc. Por ello suele caracterizarse, *grosso modo*, como un tipo de violencia que se produce cuando una persona provoca o realiza daños físicos o psicológicos a otras personas, utilizando las nuevas Tecnologías de la Información y Comunicación (TIC) o cualquier espacio digital en las que se vulnera principalmente a la víctima en su dignidad, su propia imagen, honor y, sobre todo, su vida privada. Dentro de las múltiples definiciones que existen en la literatura asociada al concepto de TIC, nos adherimos a la que ofrece Tello Leal (2007), para quien:

> Las tecnologías de la información y comunicaciones (TIC) es un término que contempla toda forma de tecnología usada para crear, almacenar, intercambiar y procesar información en sus varias formas, tales como datos, conversaciones de voz, imágenes fijas o en movimiento, presentaciones multimedia y otras formas (p. 3).

En otras palabras, la violencia digital se verifica a través de cualquier otro medio que desplace a los cauces tradicionales de comunicación (Gómez, 2011). La propia descripción y la explicación de la forma como opera refiere efectos tanto físicos como simbólicos, lo que autoriza a ubicarla en la tipología de violencia real, pero a un mismo tiempo nos proporciona los elementos para colegir por qué estamos ante un nuevo escenario de violencia: se trata de la manifestación de pautas de conducta derivadas de una auténtica revolución en los modos y medios de comunicación, tales como la internet y el uso intensificado de telefonía celular. Lo cual se incrementa derivado de que "… la gratuidad absoluta es poco frecuente en la vida social" (Imbert, 1992, p. 23).

Los nuevos escenarios de violencia digital son la factura que las sociedades *hiper* comunicadas de finales del siglo XX en adelante han de pagar. Es una especie de colateralidad. El costo de esa factura ha sido alto. La velocidad y la inmediatez son los rasgos distintivos de la actual aldea global, circunstancia que merece analizarse con un poco de detenimiento e intentar descifrar cuáles son los verdaderos factores de riesgo.

La cuestión es que en las iniciativas en comento predomina la idea de "pérdida de control" como el factor determinante. Y es que, precisamente, con la llegada de internet, la pérdida del control del contenido resulta imposible de recuperarse en virtud de la rapidez y la inmediatez con la que el contenido se distribuye. Estos conceptos de aceleración del tiempo real, de inmediatez y rapidez son los que Paul Virilio —el primer crítico del cibermundo, teórico de la velocidad y del accidente— se ha encargado de advertir desde sus primeros escritos: la idea de una virtualización de la acción, de una virtualización del tiempo real en un contexto de mundialización que se constituye, entre otras cosas, en una bomba informática. En efecto, escribía a finales del milenio pasado que:

> Después de la primera bomba, *la bomba atómica* susceptible de desintegrar la materia por la energía de la radioactividad, surge en este fin de milenio el espectro de la segunda bomba, *la bomba informática* capaz de desintegrar la paz de las naciones por la interactividad de la información (1999, p. 74).

Para el teórico y pensador de la velocidad (de la inmediatez, la rapidez, la aceleración del tiempo real) la virtualización del tiempo real es el componente de una nueva condición que caracteriza a las sociedades de hoy, en las que ha surgido una especie de "mercado de la mirada" (p. 71) y en la que algunos ofrecen su intimidad a la atención de todos. Ese nuevo matiz que adquiere el tradicional concepto de velocidad convierte a las nuevas tecnologías en portadoras de ciertos tipos de accidentes el cual ya no es local: una imagen, de acuerdo con esta tesis, y su difusión por medio de las TIC, pierden su naturaleza local, sería un accidente ya no local ni mucho menos situado, como sí sucede con el descarrilamiento

de un tren, por ejemplo. A raíz de lo anterior Virilio (1997) advierte que:

> Cuando se nos dice que la red Internet es de ámbito mundial, es claramente evidente. Pero el accidente de Internet, o el accidente de otras tecnologías de la misma naturaleza, es también la aparición de un accidente total, por no decir integral. Sin embargo, esta situación no admite comparación.
>
> La puesta en práctica del tiempo real paras las nuevas tecnologías es, se quiera o no, la puesta en práctica de un tiempo sin relación con el tiempo histórico, es decir, un tiempo mundial. El tiempo real es un tiempo mundial (p. 14).

A su vez, "La inmediatez de la información amenaza con el desencadenamiento inmediato de la crisis, y pronto surge la necesidad de la disuasión" (1998 a, p. 48). La inmediatez de las TIC, por tanto, se configura en una amenaza al desencadenar un nuevo escenario de violencia, como la violencia digital, en el que, siguiendo esta última cita de Virilio, la necesidad de disuasión se traduce en la creación de un precepto punitivo que intente, en ese sentido, desalentar un efecto violento.

Por ello ha insistido en la propuesta de incorporar, de forma independiente de la economía de la riqueza, un estudio político de la economía de la velocidad, es decir, una *dromología*. Es esta nueva ciencia la que nos permite explicar que:

> Con el reciente advenimiento de la revolución informática de las transmisiones y la velocidad absoluta, el trayecto se ha emancipado finalmente de la Tierra originaria, y con él las nociones de <<posición>>, <<localización>< y <<dirección>> de los móviles. A partir de ahora, la velocidad sirve para ver, o para no ver. Esa es la cuestión (Rial, 2003, p. 65).

El factor rapidez, inmediatez, aceleración y virtualización del tiempo real son el caldo de cultivo para nuevas perspectivas de estudio del fenómeno de la *hiper* comunicación global, son ingredientes para los nuevos miedos en los que la inmediatez triunfa, es decir, velocidad y contacto se presentan en una relación directa, sin mediaciones, ni la del tiempo ni la del espacio (Augé, 2015, pp. 42 y 43).

Se busca que los Estados sancionen la obtención sin el consentimiento de imágenes o videos de las partes íntimas o genitales de una persona, así como la reproducción o el que se compartan las mismas con un tercero o de forma pública (*Código Penal del Estado de Querétaro*, art.167 quáter), delito que como hemos mencionado, ha surgido con el entorno virtual, mismo que puede tener como causa el que un tercero que participa en el video o grabó el mismo comparta dicho contenido de forma intencional; sin embargo, también puede darse el caso en que la persona que tenga el video en su dispositivo sea víctima de algún tipo de *malware* y por tanto del robo de esas imágenes o videos, lo que dificulta la tarea de las autoridades para ubicar al responsable dentro de un entorno virtual, ya que puede que éste no se encuentre en el mismo país de la víctima, ni siquiera en el mismo continente, aunado al hecho de que la obtención de este material sensible puede dar lugar a la denominada *sextorsión*.

1.5. Pornovenganza y sextorsión

En el caso de la pornovenganza, consiste en una "situación en la que una persona, generalmente una expareja, viraliza imágenes íntimas del otro miembro una vez terminada la relación en forma con el propósito de dañarlo" (Narvaja, 2019) y la sextorsión se considera la "realización de un chantaje bajo la amenaza de publicar o enviar imágenes en las que la víctima se muestra en actitud erótica, pornográfica o manteniendo relaciones sexuales" (Velázquez, 2011, p.3).

Ambas conductas fueron tipificadas derivado de la Ley Olimpia, mencionada en el apartado anterior, en el caso da la pornovenganza, como agravante en dado caso de que el sujeto activo del delito sea una persona con la cual se mantuvo una relación de concubinato o matrimonio y sin consentimiento obtenga, comparta, divulgue o reproduzca el contenido sexual íntimo, aumentando la pena hasta en una tercera parte (*Código Penal del Estado de Querétaro*, arts. 167 quáter y quinquies).

En el caso de la sextorsión, se tipificó a través de la sanción que se le impone a la amenaza de difundir videos o imágenes de una persona, de carácter eróticas sexuales, ya sea que hayan sido

ISSN 1794-600X Número 20 • Enero - Junio de 2021

obtenidas con el consentimiento de la persona o sin éste (*Código Penal del Estado de Querétaro*, arts. 167 quinquies). No obstante lo anterior, ambos delitos como se ha reiterado surgen en el entorno virtual, por lo que en el caso de Olimpia Coral en materia penal no se siguió ningún proceso en virtud a que no existía el delito.

Lo mismo sucede con todos aquellos delitos que surgen dentro del entorno virtual, ante los cuales la víctima en muchas ocasiones no recibe justicia ni reparación del daño, ya que recordemos que en materia penal existe el principio de la exacta aplicación de la ley, por lo que no existe delito sin que esté previamente en la ley. Aunado a lo anterior, ambas conductas pueden desencadenar afectaciones graves a la vida de las personas, incluso orillándolas a cometer suicidio (Da Silva, Barros y Barbosa, 2018), derivado de la vulneración que se realiza tanto a su integridad psicológica como a su intimidad sexual, que finalmente repercuten de forma importante en su dignidad.

Algunos casos que podemos mencionar en los cuales la pornovenganza orilló a personas a cometer suicidio, fue el de Tiziana de 31 años, originaria de Italia, quien en 2015 fue víctima de la difusión de videos sexuales por parte de su pareja, lo que ocasionó que en el entorno virtual la insultaran y se burlaran de ella, por lo que decidió poner fin a su vida (Seco, 2019); tenemos también en Italia el caso de Verónica Rubio en 2014, conocido como el caso Iveco, en virtud de que trabajaba en dicha empresa, quien difundió un video con contenido sexual con un grupo de amigos; sin embargo, uno de ellos tomó la decisión de compartirlo públicamente sin el consentimiento de Verónica, lo que provocó que incluso se hicieran videos en la plataforma YouTube con el fin de ridiculizarla, por lo que dos años después se suicidó (Vinaixa, 2019).

El último caso a gran escala de sextorsión y pornografía infantil es el denominado NTH *Room*, que ocurrió en Corea del Sur, en el que no solo se pedía dinero a las víctimas a cambio de no publicar sus fotos o videos, sino que se les obligaba a autolesionarse, enviar fotos o videos con contenido sexual íntimo y realizar actos sexuales con terceros, lo anterior a través de una aplicación llamada *Telegram*, en el cual se detectaron al menos 74 víctimas y 260,000 mil usuarios que pagaron para acceder a ese contenido (Milenio Digital, 2020).

Es necesario que las personas conozcan las amenazas y delitos que surgen en el entorno virtual, no solo para no ser víctimas de estas conductas, sino para evitar cometer alguna de ellas de forma culposa por desconocimiento de que están tipificadas, teniendo presente el principio en materia penal que menciona que la ignorancia de la ley no exime de su cumplimiento, por lo que se enfrentarán a un proceso penal, dado que incurren en un delito, tal es el caso del futbolista brasileño Neymar, quien fue denunciado por violación en 2019, por lo que en su defensa subió un video a redes sociales mostrando las conversaciones en el servicio de mensajería instantánea de *WhatsApp*, ante un intento de demostrar a sus seguidores el tipo de relación que tenía con la denunciante, y mencionando ser él la víctima de extorsión (Reyes, 2019).No obstante lo anterior, en las conversaciones que mostró se observan fotos de contenido íntimo de la denunciante por lo que ahora se enfrenta a un proceso por el delito de pornovenganza (Newell, 2020).

2. DERECHOS HUMANOS DE LOS USUARIOS AFECTADOS EN EL ENTORNO VIRTUAL

Se ha demostrado que las amenazas a las que se enfrentan los usuarios en el *ciberespacio* no solo repercuten en el ámbito económico (Hernández, 2017), sino que vulnera la esfera de su seguridad, provocando en consecuencia afectaciones a sus derechos humanos. Si bien se han realizado diversas estrategias en aras de implementar y dar seguimiento al tema de la *ciberseguridad*, en algunas ocasiones ante la falta de experiencia y conocimientos especializados sobre el tema, las estrategias restringen o vulneran los derechos de los usuarios bajo el argumento de brindarles seguridad en el *ciberespacio* (Hernández, 2018), por lo que debe tomarse en consideración ante qué circunstancias y el límite que tiene el Estado para intervenir en espacios de libertad de los cuales gozan los usuarios en el *ciberespacio*, como bien lo menciona Koch (2015).

Asimismo, se ha enfatizado en los riesgos a los que se enfrentan los usuarios en el entorno virtual, y la respuesta que brinda el Estado a través de reformas que se han hecho a los códigos penales con la finalidad de imponer penas a conductas como la *pornovenganza y sextorsión*, entre otras,

que afectan de forma importante la integridad psicológica de los usuarios llegando incluso hasta la física (Giant, 2016) o incluso agravar penas de delitos que ya se realizaban fuera del entorno virtual, pero que se sofistican en este.

Una de las reformas más importantes que tiene nuestro sistema jurídico, es la reforma constitucional de 2011 en materia de derechos humanos, la cual impone la obligación a todas las autoridades de promover, respetar, proteger y garantizar los derechos humanos (*Constitución Política de los Estados Unidos Mexicanos*, art.1), la cual no se limita a un espacio físico, sino que abarca también el entorno virtual, cuya tarea no es nada fácil, derivado de la dificultad de identificar a los sujetos activos de los delitos, ante el anonimato que permite dicho entorno, así como las técnicas que existen para evitar ser rastreados.

Sumado a lo anterior, tenemos que las amenazas en el entorno virtual afectan derechos tan importantes como la vida, la libertad, la salud –en particular lo relacionado a la integridad psicológica— intimidad y patrimonio, afectaciones que inciden en el menoscabo a la dignidad humana, eje central de los derechos humanos. De ahí que, son necesarias las respuestas que brinda el Estado para salvaguardar y proteger a los usuarios mediante la prevención, investigación, sanción y reparación en caso de que dichos derechos humanos sean vulnerados (CPEUM, art.1).

En ese sentido, en la protección al usuario en un entorno virtual, constantemente nos encontramos con la delgada línea que existe entre los derechos humanos y su limitación o intervención, en virtud de que algunas medidas tomadas por los Estados afectan en menor o mayor grado nuestros derechos, como en el caso de la Geolocalización en México, misma que causó controversia cuando se encontraba regulada por el artículo 40 bis de la Ley Federal de Telecomunicaciones –actualmente se encuentra en el artículo 303 del Código Nacional de Procedimientos Penales—, toda vez que se consideraba que vulneraba el derecho a la privacidad de las personas, incluidas aquellas que eran sospechosas en una investigación, lo cual dio como resultado la acción de inconstitucionalidad 32/2012 promovida por la Comisión Nacional de los Derechos Humanos, misma que resolvió la Suprema Corte de Justicia de la Nación en el 2014, mencionando que era una restricción constitucionalmente válida a la vida privada en aras de garantizar el orden público y, derechos de las víctimas en la investigación de los delitos.

En ese sentido, ante cada decisión que tome el Estado en aras de garantizar la protección de los usuarios, es necesario un análisis de los derechos fundamentales en los que se interviene con las medidas que se implementarán, con la finalidad de que su restricción o limitación supere el denominado test de proporcionalidad y, por tanto, se consideren constitucionales, para lo cual debe: 1) Perseguir un fin constitucionalmente válido, 2) Sea una medida que satisfaga un propósito constitucional, 3) la no existencia de medidas alternativas menos lesivas y 4) que el grado de realización del fin perseguido sea mayor al de afectación de los derechos (Tesis: 1a. CCLXIII/2016).

En relación a la perspectiva teórica surge la necesidad de que los operadores jurídicos conozcan la aplicación de teorías como el *neoconstitucionalismo* en la aplicación práctica y la interpretación de los derechos en el entorno virtual, toda vez que es fundamental para abordar temas en los que la ley no es suficiente para la resolución de conflictos, más aún cuando los temas relacionados con la tecnología, rebasan en muchas ocasiones los parámetros establecidos en la ley; sin embargo, los límites a los derechos humanos relacionados al uso de la tecnología deben definirse aplicando la argumentación y lógica jurídica al caso concreto, que precisamente esta teoría aborda.

3. RECONOCIMIENTO DE DERECHOS EN EL ENTORNO VIRTUAL

Con el entorno virtual, surgen nuevos derechos tales como el acceso a internet, el derecho al olvido en el *ciberespacio* y la seguridad cibernética, cuyo análisis reviste especial relevancia y complejidad frente a la obligación que adquieren los Estados al reconocerlos dentro de sus sistemas jurídicos, toda vez que se comprometen en tal sentido a garantizarlos; y en el caso del usuario, el beneficio es la ampliación del catálogo de derechos fundamentales cuyo cumplimiento puede exigirle al Estado.

3.1. El derecho al olvido

Respecto a la imperante necesidad del reconocimiento de derechos humanos vinculados con el entorno virtual, destaca lo expuesto por Álvarez (2015) en relación al derecho al olvido

ISSN 1794-600X Número 20 • Enero - Junio de 2021

en internet, mismo que se encuentra vinculado con la intimidad y privacidad de los usuarios, que representa un desafío relacionado a la cancelación o supresión de datos personales en el *ciberespacio*, aunado a lo anterior, visto en un sentido amplio como lo sugiere Zárate (2013) esto es el derecho a olvidar y a ser olvidado, traducido en rectificación, cancelación y oposición.

Cabe mencionar que en otros países, verbigracia España, el tema no solo ha sido discutido, sino que se ha llevado a la práctica a través de la emisión de sentencias que lo reconocen, tal y como lo expone Simón (2015), asimismo destaca la investigación realizada por Mate (2016) acerca del análisis de la normativa y resoluciones por parte de los tribunales españoles ante las crecientes exigencias de los usuarios en la búsqueda del reconocimiento de este derecho por parte del Estado y por ende su garantía.

En ese mismo tenor, Platero (2016) señala como evoluciona el tema del derecho al olvido de ser una solicitud de tutela de un derecho que realizaban los usuarios al Estado, pasando por un cuasi-derecho fundamental derivado del reconocimiento que le brindaba en las resoluciones emitidas por los tribunales españoles, hasta llegar a un derecho fundamental enmarcado dentro de la esfera del derecho a la protección de datos.

Aunado a lo anterior, De Terwangne (2012) nos indica los problemas que enfrentaría el Estado ante el reconocimiento de dicho derecho, toda vez que lo equipara a la atribución de la caducidad de los datos personales, lo cual representa un problema en el caso del uso de las redes sociales por lo que hace al ámbito de acción y regulación.

En el caso de México, no se encuentra reconocido como tal el derecho al olvido en el entorno virtual; se tiene el derecho de cancelación de datos personales regulado por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares; sin embargo, serviría como antecedente para que a futuro se reconozca el derecho al olvido. No obstante lo anterior, algunas opiniones diversas señalan que este derecho no tiene relación directa con el derecho a la privacidad y protección de datos personales y, por el contrario, violenta la libertad de expresión y merma el ejercicio de los derechos humanos a través de las tecnologías (Artículo 19, 2020), por lo que se hace necesario indicar los límites del mismo agregando desde luego el derecho de acceso a la información, cuando se incorpore en nuestro sistema jurídico, con la finalidad de no generar una colisión entre derechos fundamentales por no cumplir con las características para ser considerado constitucionalmente válido, considerando también la ponderación de derechos que implica el tema, confrontándose directamente con el derecho a la intimidad, dignidad humana, reinserción social y revictimización que puede alegarse por la persona que se considera afectada.

Con relación a ello, el pasado 5 de diciembre del 2019, se presentó la iniciativa LXIV/2PPO-67/102681, con el fin de reformar la Ley Federal de Protección de Datos Personales en Posesión de Particulares en la que incluso refiere que se debe entender por derecho al olvido, y establece: "la eliminación y supresión de todos los contenidos que se encuentren en medios electrónicos, plataformas digitales, buscadores de internet y demás medios digitales, incluyendo textos, comentarios, interacciones, ubicaciones, contenido multimedia, antecedentes penales y demás información" (Millán, 2020). Sin embargo, el presidente de la República descalificó dicha propuesta ante medios, refiriéndose a la iniciativa con las frases: "Prohibido, prohibir" y "perdón sí, olvido no" (San Martín, 2020).

3.2. El derecho al internet

En la era digital surge el debate de sí los Estados tienen la obligación de realizar diversas acciones con la finalidad de garantizar que todos sus ciudadanos tengan internet, mediante el reconocimiento del derecho al internet, o sí simplemente se debe reconocer el derecho de acceso que implica la garantía de no interferencia por parte del Estado en la utilización que los usuarios realicen. Ambos, conllevan obligaciones distintas, ya que el primero exige un actuar por parte del Estado con la finalidad de que todos participen en un entorno virtual; y el segundo, implica un no hacer en relación con uso que se le dé, lo cual desde un punto de vista económico, conlleva grandes inversiones económicas estatales si se opta por el primero.

En 2016, la Asamblea General de la Organización de las Naciones Unidas, reconoció el derecho al acceso al internet como derecho humano, mediante su resolución A/HCR/32/L.20. Finlandia, desde el 2010, fue el primer país que reconoció el servicio de internet de banda

ancha como derecho humano, por lo que ordenó a todos los proveedores de servicios de internet a proporcionar la conexión con ciertas características en aras de garantizar una determinada velocidad de la misma a todos los ciudadanos sin importar su ubicación (BBC News, 2010), a diferencia de la mayoría de países, como México, en el cual se reconoció el derecho humano al acceso al internet y banda ancha, esto en 2013 con una reforma al artículo 6 constitucional.

Coincidimos con la propuesta de Haideer (2016) respecto a la necesidad de una tutela multinivel de los derechos fundamentales en el entorno virtual, esto es considerando que no solo el Estado es competente para proteger los derechos humanos, sino que es tarea incluso de diversos organismos internacionales dado la globalización en la cual estamos inmersos y derivado de los nuevos derechos que han surgido en el entorno virtual.

4. IMPORTANCIA DE LA CIBERSEGURIDAD

No es ajeno el impacto que tiene la globalización en la esfera de los usuarios de internet, cuya preocupación reciente se ha centrado en la denominada *ciberseguridad* o seguridad cibernética, derivado de los problemas de seguridad, protección de datos y privacidad como bien lo señala Anchundia (2017). No obstante lo anterior, existe preocupación de la comunidad internacional en relación a la imperiosa necesidad de brindar respuestas integrales con pleno respeto a los derechos humanos de los usuarios, evitando como señala Carlini (2016), repercusiones comparables a la confrontación militar tradicional, ya que si bien las amenazas ponen en peligro a los usuarios, es necesario que exista una cooperación entre los usuarios del ciberespacio, con la finalidad de evitar optar por posibles respuestas, que lejos de resolver el problema de la vulneración a los derechos humanos en el entorno virtual, lo agravan, vulnerando de la misma forma los derechos humanos de los usuarios.

Destaca el hecho de que la *ciberseguridad* en un principio se ocupara de proteger la información de forma reactiva y actualmente, se considere que tienen una posición proactiva, esto es a través de la identificación y gestión de riesgos que amenazan a los usuarios en el uso del *ciberespacio* (Fojón, 2010); misma que se considera un medio para garantizar la convivencia en un Estado de Derecho (Galán, 2016) a través de medidas que contrarresten el denominado efecto destructivo (Pons, 2017) que tiene en la sociedad al ser el origen de conductas tipificadas por códigos penales, cuyo medio de comisión ahora es el *ciberespacio* y de conductas que afectan los derechos humanos que nacieron con la internet.

En 2019, la Secretaría de Seguridad y Protección Ciudadana de México mencionó que "No existe amenaza al Estado mexicano que no pueda ser resuelta por las capacidades de inteligencia [...] 9 de cada 10 delitos que se comenten a través de tecnologías de la información pueden ser evitados con medidas de prevención". Asimismo, McKinsey & Company, indica que "una estrategia de prevención de ciberriesgos se puede fortalecer fomentando una cultura de ciberseguridad" (2018, p.7.).

A pesar de que la ciberseguridad es un tema que requiere ser abordado desde la participación y cooperación a nivel internacional, es importante el papel de cada usuario en aras de protegerse y prevenir ser víctima de las diferentes amenazas que se encuentran en el entorno virtual, de ahí que se considere la necesidad de una cultura de la ciberseguridad enfocada en la prevención, mediante el conocimiento de los riesgos y las amenazas a las que se enfrentan al navegar en un entorno virtual, así como las medidas que se deben tomar para garantizar la seguridad y uso responsable del internet, además de contar con las herramientas necesarias para actuar en caso de ser víctima de algún delito o alguna conducta que, a pesar de que aún no esté tipificada, nos cause un daño.

Para ello, los esfuerzos se deben enfocar en los pronósticos sobre las amenazas realizados por expertos, como lo es la empresa de ciberseguridad Kaspersky, la cual mencionó en 2019 una lista con las 10 amenazas a las que cuales se debe prestar atención en Latinoamérica, a saber: 1) Campañas de desinformación y manipulación de la opinión popular mediante redes sociales; 2) Infecciones vía ataques a compañías dedicadas a la producción de software masivo; 3) Ataques a usuarios aprovechando que en Windows 7 existen vulnerabilidades; 4) Robo de contraseñas y claves de servicios de *streaming* para venderlas en mercados ilegales; 5) Aumento de sextorsión y estafas para recaudar dinero, 6) Aumento de ataques a instituciones financieras y a sus

ISSN 1794-600X Número 20 • Enero - Junio de 2021

clientes; 7) Campañas de extorsión bajo la amenaza de filtrar información personal al dominio público; 8) Clonación de líneas para robo de identidad o acceso a sitios financieros; 9) Ataques relacionados con la migración y desplazamiento regional de personas; y 10) Aumento de ataques de extorsiones a empresas y grandes corporaciones, por el robo de datos.

Algunas medidas preventivas que señalan Tovar, González y García (2018) son:

1. Hacer respaldos de la información periódicamente.

2. Mantener actualizado el sistema operativo e instalar los parches de seguridad.

3. No abrir correos electrónicos de remitentes desconocidos ni abrir los archivos adjuntos.

4. No abrir enlaces de dudosa procedencia a menos de estar seguro de la confiabilidad de quien lo publica.

5. Mantener actualizado nuestro sistema *anti-malware*.

Finalmente, el cambio de paradigma en la seguridad cibernética pasando de una visión proteccionista a una preventiva (Orellana, 2018) no solo permite que los esfuerzos se centren en orientar y garantizar el ejercicio de los derechos humanos en el entorno virtual, sino en la creación de una cultura de la *ciberseguridad* que desemboque en el uso responsable como usuarios del *ciberespacio* encaminado a la salvaguarda y protección de la seguridad.

CONSIDERACIONES FINALES

Es necesario que los usuarios conozcan y comprendan las amenazas a las que se enfrentan en el entorno virtual, así como los riesgos que derivan de ellas, no solo para prevenir ser víctimas de los mismos, sino saber cómo actuar en caso de ser víctimas, estando conscientes además de que hay conductas que no se encuentran tipificadas y, la difícil tarea que es en ocasiones ubicar al responsable beneficiado por el anonimato proporcionado por el entorno digital, que deriva en actos de impunidad en ocasiones ajenos incluso al actuar de las autoridades, por lo que el papel preventivo es de suma importancia.

Al respecto, concientizar sobre el uso responsable del internet, sobre todo para evitar que se cometan conductas que causen daño a terceros o incurran en un delito, por el desconocimiento que existe en relación con las afectaciones que conllevan determinadas acciones en el entorno virtual, que si bien parecieran a simple vista inofensivas, tienen grandes repercusiones en las víctimas. El conocimiento previo de dichas conductas es fundamental para evitar que se produzcan y puedan resultar impunes.

Asimismo, el usuario debe conocer los derechos que surgen en el entorno virtual con la finalidad de exigir que el Estado los reconozca dentro de su sistema jurídico para que se dé la ampliación detallada del catálogo de sus derechos fundamentales y en consecuencia exista la obligación por parte de las autoridades de protegerlos, promoverlos, respetarlos y garantizarlos, así como medidas tendientes a repararlos en caso de que sean vulnerados. Sin hacer óbice lo anterior, en la regulación se deben considerar las diversas posturas acerca de la ponderación de derechos humanos en casos en concreto como el derecho al olvido.

Se considera importante crear una cultura responsable de la *ciberseguridad* para los usuarios centrada en la prevención, ante la corresponsabilidad de éstos y el Estado para evitar riesgos en el *ciberespacio*, mediante la instrumentación de medidas de concientización acerca de la importancia de conocer las amenazas en el ambiente digital que vulneran la seguridad y la importancia de las líneas de acción con respeto irrestricto a los derechos humanos.

BIBLIOGRAFÍA

- Agencia DPA (04/05/ 2017). Primera víctimas adolescentes del juego ballena azul en Argentina. *El Comercio.* Disponible en https://www.elcomercio.com/tendencias/victimas-adolescentes-juego-ballenaazul-argentina.html
- Aguiar, A. R., (10/06/2020). Así funciona Ginp, el troyano bancario que pone su diana en España y que está detrás del 'phising' con el que los ciberdelincuentes intentaron suplantar al Ministerio de Sanidad. *Business Insider*. Disponible en https://www.businessinsider.es/ginp-troyano-bancario-ha-puesto-diana-espana-656469
- Álvarez C., M. (2015). *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital*. Madrid: Editorial Reus.
- Amescua Ch., C. (2010). El secuestro virtual en el continuum de la violencia. Visibilizar lo que se oscurece. *Trace. Travaux et Recherches dans les Amériques du Centre*. No. 57, pp.: 111-127.
- Anchundia B., C. E., (2017) Ciberseguridad en los sistemas de información de las universidades. *Dominio de las Ciencias*, (3), pp. 200-217.
- Augé, M. (2015). *Los nuevos miedos.* México: Paidós.
- Artículo 19, (14 de enero de 2020). *Iniciativa para reconocer el "derecho al olvido" abre puerta a la censura y es contraria a los derechos humanos*. Disponible en: https://articulo19.org/iniciativa-para-reconocer-el-derecho-al-olvido-abre-puerta-a-la-censura-y-es-contraria-los-derechos-humanos/
- Ballestero, F. (2020) La ciberseguridad en tiempos difíciles ¿Nos ocupamos de ella o nos preocupamos por ella? *Boletín económico del ICE, No. 3122*, pp.39-48.
- BBC News. (01/07/2010). *Finland makes broadband a 'legal right'*, Disponible en https://www.bbc.com/news/10461048#:~:text=Finland%20has%20become%20the%20first,megabit%20per%20second)%20broadband%20connection.
- Carlini, A. (2016) Ciberseguridad un nuevo desafío para la comunidad internacional. *Boletín I.E.E.E.*, abril-junio, (2), pp.: 950-966.
- Ceballos-Espinoza, F. (2017). Suicidio adolescente y Otredad: La ballena azul dentro del aula. VI Congreso Internacional de Psicología y Educación. Psychology Investigation, Lima. Disponible en https://www.aacademica.org/fceballose/16.pdf
- *Código Penal del Estado de Querétaro.* (1987). Sombra de Arteaga.
- Da Silva e S., A.; Barros P., R., y Barbosa R., Edith M. (2018). Instigación al suicidio como implicación del crimen de pornografía de venganza a la salud de sus víctimas. *Actas de Congreso del Centro Nacional de Información de Ciencias Médicas*, Disponible en http://www.convencionsalud2017.sld.cu/index.php/connvencionsalud/2018/paper/viewFile/1238/1269
- De Terwangne, C. (2012). Privacidad en Internet y el derecho a ser olvidado/ derecho al olvido. *Revista de Internet, Derecho y Política*, (13), pp.53-66.
- Dominicci A., J. A. (s. f.). *Estudio de caso: Malware en Android.* Universidad Interamericana Recinto de Guyana, Puerto Rico, Disponible en https://www.academia.edu/10898835/Malware_en_Android
- DW, (2020) *Hana Kimura: suicidio por acoso cibernético en Japón*. Disponible en https://www.dw.com/es/hana-kimura-suicidio-por-acoso-cibern%C3%A9tico-en-jap%C3%B3n/a-53570716 Fecha de consulta: 10 de junio de 2020
- Estirado, L. (28/02/2019) El peligroso reto 'Momo' se cuela en vídeos de Peppa Pig y Fortnite. *El Periódico*. Disponible en https://www.elperiodico.com/es/

extra/20190228/peligroso-reto-momo-videos-peppa-pig-fortnite-7329283
- Fojón, J. E. y Sanz V., Á. F. (2010). Ciberseguridad en España: una propuesta para su gestión. *Boletín Elcano* (126), pp. 1-8.
- Galán, C. M., y Galán Cordero, C. (2016). La ciberseguridad pública como garantía del ejercicio de derechos. *Derecho y Sociedad*, (47), pp. 293-306.
- García G., N. (2016). Actividades cotidianas de los jóvenes en Internet y victimización por malware. IDP: *Revista de internet, derecho y política*, Universitat Oberta de Catalunya, (22), pp.59-72.
- García, J. (20/05/2020). El secuestro virtual de 14 enfermeros en Ciudad de México agrava la violencia contra los sanitarios. *El País*. Disponible en https://elpais.com/sociedad/2020-05-20/el-secuestro-virtual-de-13-enfermeros-en-ciudad-de-mexico-agrava-la-violencia-contra-los-sanitarios-que-atienden-la-pandemia.html
- Giant, N. (2016). *Ciberseguridad para la i-generación: Usos y riesgos de las redes sociales y sus aplicaciones.* Madrid: Narcea Ediciones.
- Gómez C., E. (2011). Derecho a la propia imagen, nuevas tecnologías e internet. En: Cotino H., L. (ed.). *Libertades de expresión e información en internet y las redes sociales: ejercicio, amenazas y garantías.* Valencia: Servicio de Publicaciones de la Universidad de Valencia.
- Gómez V., A. (2011). *Enciclopedia de la Seguridad Informática.* Madrid: Grupo Editorial RA-MA.
- González P., R. A. (2018). La creación de criptomonedas y la minería no autorizada. *Seguridad Cultura de prevención para ti*, No. 31, México: UNAM-CERT.
- Hernández M., A. (2017). Ciberseguridad y confianza en el ámbito digital. ICE: *Revista de economía,* (897), pp. 55-66.
- Hernández J.C. (2018). Estrategias nacionales de ciberseguridad en América Latina. Universidad de Granada. *Análisis GESI,* (8), pp. 54-69.
- Imbert, G. (1992). *Los escenarios de la violencia.* Barcelona: Icaria.
- Jara, H., y Pacheco, F. G. (2012). *Ethical hacking 2.0*, Buenos Aires: RedUsers Usershop.
- Kaspersky. (21 de noviembre de 2019). Kaspersky ofrece pronóstico de ciberseguridad 2020 para América Latina. *Kaspersky Latinoamérica*, Disponible en https://latam.kaspersky.com/about/press-releases/2019_kaspersky-ofrece-pronostico-de-ciberseguridad-2020-para-america-latina
- Koch M., S. (2015). La libertad en el ciberespacio: ciberseguridad y el principio del daño. *Revista Ensayos Militares*, (2), pp. 85-98
- Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Revista Latinoamericana de Ingeniería de Software*, 3(4), pp. 161-176.
- Marañón, C. O. (2012). Redes Sociales y jóvenes: Una intimidad cuestionada en internet. *Aposta. Revista de Ciencias Sociales*, No.54, (julio-septiembre), pp.1-16.
- Martínez, A. I. (25/09/2017). Millones de datos de pacientes, en riesgo por los agujeros de seguridad informática. *ABC Redes,* Disponible en https://www.abc.es/tecnologia/redes/abci-millones-datos-pacientes-riesgo-agujeros-seguridad-informatica-201608070100_noticia.html?ref=https:%2F%2Fwww.google.com%2F
- Mate S., L. C. (2016). ¿Qué es el derecho al olvido? *Revista de Derecho Civil*, 3 (2), pp.187-222.
- McKinsey & Company (2018), Perspectiva de ciberseguridad en México, COMEXI. Disponible en https://consejomexicano.

org/multimedia/1528987628-817.pdf
- Milenio Digital (25/03/2020) Corea del Sur identifica a sospechoso de crear grupo de chat con abusos sexuales. Disponible en https://www.milenio.com/internacional/asia-y-oceania/corea-sur-ubica-presunto-lider-red-trafico-sexual-digital
- Millán C., X. (6 de Julio de 2020). ¿Qué tanto podemos olvidar? Una revisión al derecho al olvido. Disponible en http://derechoenaccion.cide.edu/que-tanto-podemos-olvidar-una-revision-al-derecho-al-olvido/ Fecha de consulta: 20 de agosto de 2020.
- Miranda B., H. (2016). El acceso a Internet como derecho fundamental. *Ius doctrina*, 9 (15), pp. 1-23.
- Narvaja, M. E. (2019). Sexting: percepciones de estudiantes tucumanos sobre motivaciones y riesgos. *Ciencia, Docencia y Tecnología*, 30(59), pp.: 127-147. Disponible en https://www.redalyc.org/articulo.oa?id=145/14561215005
- Newell, L. (19/02/2020) Avances en la denuncia contra Neymar por el delito de porno-venganza. *Mundo Deportivo*. Disponible en https://www.mundodeportivo.com/vaya-mundo/20190912/47306681836/avances-en-la-denuncia-contra-neymar-por-el-delito-de-porno-venganza.html
- Orellana R., C. (2018) De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales. *Foro Revista De Derecho*, 1(27), pp. 5-21.
- Platero A., A., (2016). El derecho al olvido en internet. El fenómeno de los motores de búsqueda. *Revista Opinión Jurídica*, 15 (29), pp. 243-260.
- Pons G, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad*, (20), pp. 80-93
- Reyes, D. (02/06/2019). Neymar exhibe conversaciones y fotos que intercambió con mujer que lo acusa de violación. *Radio Fórmula*, Disponible en https://www.radioformula.com.mx/entretenimiento/20190602/neymar-conversaciones-whatsapp-acusaciones-violacion-fotos/
- Rial U., S. (2003). *Paul Virilio y los límites de la velocidad.* Madrid: Campo de Ideas.
- Rojas, A. G. (26/09/2019) Ciberacoso: "Pasé de ser la 'gordibuena' del video sexual que criticaba todo el pueblo a que 11 estados de México aprobaran una ley con mi nombre". *BBC Mundo*. Disponible en https://www.bbc.com/mundo/noticias-america-latina-49763560
- Ruíz, R. (2020). Violencia Digital contra la mujer en México: Honor, imagen y daño moral. El espectro del derecho penal simbólico en la 'Ley Olimpia'. *Revista Derecho y Realidad* (35), (enero – junio), pp. 17-38.
- Sala, M. (25/09/2017). Un nuevo virus informático que pide como rescate fotos desnudos. *El Español*, Disponible en https://www.elespanol.com/social/20170925/249475881_0.html
- San Martín, N. (12 de febrero de 2020). El presidente rechaza propuesta de Monreal sobre 'derecho al olvido", *Revista Proceso*. Disponible en https://www.proceso.com.mx/nacional/2020/2/12/el-presidente-rechaza-propuesta-de-monreal-sobre-derecho-al-olvido-238431.html
- Seco, R. (15/06/2020). Así se lucha contra la 'pornovenganza'. *El país*, Disponible en https://elpais.com/elpais/2019/06/14/ideas/1560532497_362604.html
- Simón C., P. (2015). *El reconocimiento del derecho al olvido digital en España y en la UE, Efectos tras la sentencia del TJUE de mayo de 2014*. Madrid: Bosch.
- Tello L., E. (2007). Las tecnologías de la información y comunicaciones (TIC) y la brecha digital: su impacto en la sociedad de

México. *Revista de Universidad y Sociedad del Conocimiento*, 4, (2), pp. 1-8.

- Tesis 1a. CCLXIII/2016, Test de proporcionalidad. Metodología para analizar medidas legislativas que intervengan con un derecho fundamental. *Gaceta del Semanario Judicial de la Federación*, Primera Sala de la Suprema Corte de Justicia de la Nación, Décima época, t. II, l.36, p.915.
- Tovar B., S. A.; González P. R. A. y García, D. (2017). Wannacry: ataque mundial y consideraciones sobre ciberseguridad. *Seguridad Cultura de prevención para ti,* (29).
- Velázquez R., L. M. (2011) "Sexting, sexcasting, sextorsión, grooming y cyberbullyng. El lado oscuro de las TICS", ponencia presentada en el XI Congreso Nacional de Investigación Educativa, Disponible en http://www.comie.org.mx/congreso/memoriaelectronica/v11/docs/area_17/0121.pdf
- Virilio, P. (1999). *La bomba informática.* Madrid: Cátedra.
- Virilio, P. (1998). *Estética de la desaparición.* Barcelona: Anagrama.
- Virilio, P. (1997). *El cibermundo, la política de lo peor*. Madrid: Teorema.
- Vinaixa, L. (07/08/2019). La pornovenganza del vídeo casero: "Me grababa solo para gustarle, hasta que lo compartió. *El Español*, Disponible en https://www.elespanol.com/reportajes/20190707/pornovenganza-video-casero-grababa-solo-gustarle-compartio/411709265_0.html
- Zárate R., S. (2013). La problemática entre el derecho al olvido y la libertad de prensa. *Derecom, 13*, pp.1-10.