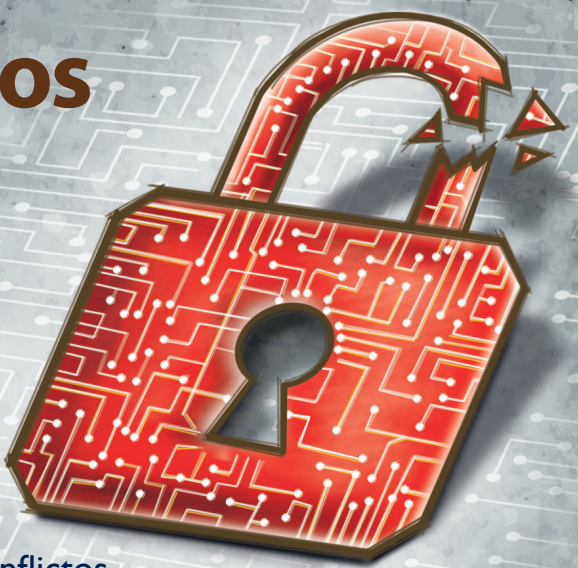
Revista Mexicana de Ciencias Penales

Año 3 • Número 10 • enero-abril de 2020 • $100.00

Ciberdelitos



- Tecnología, derecho y conflictos
  Bibiana Beatriz Luz Clara
- Convertir una debilidad en fortaleza. Primeras experiencias acumuladas
  Damián Paret Francia
- Los Estados, las criptomonedas y la ciberseguridad
  Humberto Martín Ruani
- Las operaciones con recursos de procedencia ilícita y las *fintech*: responsabilidad penal de las personas morales
  Alberto Enrique Nava Garcés

INACIPE
INSTITUTO NACIONAL DE CIENCIAS PENALES

REVISTA MEXICANA DE CIENCIAS PENALES

REVISTA MEXICANA DE CIENCIAS PENALES

REVISTA MEXICANA DE CIENCIAS PENALES es una publicación del INACIPE, cuyo objetivo es dar a conocer investigaciones, análisis, reflexiones y opiniones acerca de las ciencias penales en México y en el mundo. En esta revista se dan cita los autores más reconocidos en estas disciplinas.

Año 3 • Número 10 • enero-abril de 2020
ISSN 0187-0416

·INACIPE·
INSTITUTO NACIONAL DE CIENCIAS PENALES

DIRECTORIO

Diseño editorial
Lizeth Violeta Méndez Guadarrama
Daniel Leyte Muñiz

Cuidado editorial
Irene Bárcenas Jara
Víctor Fernando Gálvez García

Diseño de portada
Israel Eliseo Martínez Sánchez

REVISTA MEXICANA DE CIENCIAS PENALES, año 3, No. 10, enero-abril 2020. Es una publicación trimestral editada por el Instituto Nacional de Ciencias Penales, a través de la Dirección de Publicaciones y Biblioteca. Calle Magisterio Nacional núm. 113, Col. Tlalpan, Alcaldía Tlalpan, C. P. 14000, Ciudad de México, México. Tel. 5487 1571; www.inacipe.gob.mx; e-mail: publicaciones@inacipe.gob.mx. Reservas de Derechos al Uso Exclusivo No. 04-2017-080214584200-102, ISSN: 0187-0416, ambos otorgados por el Instituto Nacional del Derecho de Autor, Licitud de Título y contenido: 17106. Expediente: CCPRI/3/TC/18/21019 otorgado por la Comisión Calificadora de Publicaciones y Revistas Ilustradas de la Secretaría de Gobernación.

Impresa por Ediciones Corunda, S.A. de C.V., Tlaxcala 19, Col. San Francisco, Alcaldía Magadalena Contreras, C.P. 10810, Ciudad de México. Este número se terminó de imprimir en abril de 2020 con un tiraje de 500 ejemplares.

Instituto Nacional de Ciencias Penales

@ INACIPE

www.inacipe.gob.mx

CONTENIDO

VISIONES PARA EL FUTURO

CARTA EDITORIAL

Con la llegada de la *era* de la información se modificó determinantemente la relación del ser humano con su entorno social. La aparición de las tecnologías informáticas, la televisión, la computación y el internet, así como el desarrollo de las redes sociales, establecieron nuevos paradigmas culturales que no están exentos de verse afectos por una naciente dinámica delictiva. A decir verdad, la llegada de la cultura informática se encuentra aparejada con la estructuración de una nueva actividad criminal: los ciberdelitos.

Es precisamente por ello que el actual número de la *Revista Mexicana de Ciencias Penales* (*RMCP*) incide en el fenómeno informático y su relación con la delincuencia.

Así, el artículo "Las operaciones con recursos de procedencia ilícita y las *fintech*", de Alberto Nava Garcés y Juliette Núñez Ruiz, incide en el fenómeno de la responsabilidad penal de las personas jurídicas, el lavado de dinero y la creación de las denominadas *fintech*, es decir, la fundación de aquellas empresas que brindan servicios financieros (algunos de estos innovadores) a través del uso de tecnologías de la información.

Por su parte, Alicia Rubí Guerra Valdivia presenta un artículo denominado "La identidad en la era digital", el cual incide en la importancia de generar una adecuada legislación y tratamiento de la tecnología de la información. En términos similares, Bibiana Beatriz Luz Clara refiere que el uso de la tecnología ha modificado nuestra sociedad y creado nuevos procesos disruptivos, los cuales requieren de un análisis y regulación desde el espacio jurídico.

Mario Anselmo Gómez Sánchez analiza un fenómeno que ha cobrado gran importancia en los últimos años y del que se sabe poco: los derechos de acceso, rectificación, cancelación u oposición de datos personales (ARCO), su reconocimiento constitucional y la forma en que estos han funcionado en México en los 10 años que llevan siendo protegidos.

Carlos Ramírez Castañeda, por su parte, advierte la existencia de una ciberguerra que no se está ganando porque no existe una

conciencia social de los peligros en la red: la utilización de *malware*, los ataques a infraestructuras y los vacíos legales.

Pero este número no solo alude al internet, a las empresas o a los derechos de información, también advierte la incidencia de los videojuegos en la codificación de una estructura social más violenta. ¿Acaso jugar un videojuego puede influir en la conducta de una persona? Daniel Córdova Herrera investiga la posible respuesta a esta pregunta en su artículo "Videojuegos y delitos: ¿correlación o supersticiones?".

Así, la *RMCP*, a través de los autores, busca ofrecer respuestas innovadoras a los fenómenos sociales que inciden en la actividad delictiva actual.

Alejandra Silva
Directora de Publicaciones y Biblioteca

TENDENCIAS Y PERSPECTIVAS ACTUALES

LAS OPERACIONES CON RECURSOS DE PROCEDENCIA ILÍCITA Y LAS *FINTECH*: RESPONSABILIDAD PENAL DE LAS PERSONAS MORALES

Alberto Enrique Nava Garcés*
Juliette Núñez Ruiz**

* Investigador y miembro del Comité de Investigación del Instituto Nacional de Ciencias Penales.
** Investigadora asistente del Instituto Nacional de Ciencias Penales.

PALABRAS CLAVE *KEYWORDS*

Delitos informáticos	*Cybercrime*
Responsabilidad de las personas morales	*Business responsability*
Fintech	*Fintech*
Fortalecimiento financiero	*Crowdfunding*

Resumen. El concepto de empresa ha ido evolucionando a lo largo del tiempo, dicha capacidad de mutación ha influenciado en el mundo impactando no solo de forma económica, sino también social y culturalmente, lo anterior ya que no se ha limitado a los tipos de empresas o sociedades que conocíamos, sino que se ha dado un nuevo concepto derivado de la búsqueda de innovación y un modelo de negocios rentable.

Por lo anterior es que se crea el sector *fintech*, mismo que ha ido ganando terreno en la economía, en negocios e incluso en las legislaciones, por lo tanto, se identificará la evolución de este sector y el grado de reglamentación que ocupa en México, para ello hemos de verificar la evolución que han tenido las empresas y los inicios de la *startup*, que ha servido de base para crear las *fintech*.

Abstract. The fourth industrial revolution, together with the discredit of traditional banking, as a result of the last great crises and other phenomena that will unfold in this work, has been affecting the financial sector and led to the rise of new ventures and web platforms linked to finance. In this way, the world of crowlending, peer to peer lending and fintech are entered.

The technologies they use and the way in which some of these new business models operate make them liable to bec ome instruments for money laundering and terrorist financing. In this sense, the circumstances that have facilitated the emergence of these new online business models, linked to the financial sector, are analyzed.

SUMARIO:

I. INTRODUCCIÓN

El derecho penal y las nuevas tecnologías tienen puntos de convergencia más a menudo, ya que han incidido tanto en la creación de nuevos tipos penales como en el cambio de óptica respecto de figuras que parecían inamovibles, como la responsabilidad penal de las empresas, que hoy en día ha abierto un debate por demás interesante y enriquecedor.

Antonio Mazzitelli , representante en México de la Oficina de las Naciones Unidas contra la Droga y el Delito, (UNODC, por sus siglas en inglés) lo ha señalado con gran claridad en diversos foros:

> La lucha contra el crimen organizado, y la corrupción es un tema de ir detrás del dinero, si queremos de verdad golpear al crimen organizado, la actividad más importante es tratar de extraer su fortaleza, esto es, su capacidad de infiltrarse, de controlar y de legitimar una cultura criminal.
>
> No nos adentraremos en los temas específicos y técnicos de la lucha contra el lavado de activos, el objetivo de esta ponencia es mostrar cómo el crimen organizado se está estructurando, evolucionando y mostrando nuevas caras, así como su infiltración en la sociedad. […]
>
> En diciembre de 2011, se trató de elaborar un primer informe, estimando los flujos financieros relacionados con las actividades criminales, trabajo de compilación, sustentado en el análisis de cuánto dinero pueden generar los mercados criminales, es decir, se trata de ver al crimen organizado desde una perspectiva diferente y no solamente a sus bienes, las drogas, la trata de personas, el robo, sino a los mercados criminales, partiendo del presupuesto del concepto de los mercados y operadores que tratan de maniobrar dichos mercados.[1]

El flujo de activos, ahora en esta época virtual, así como la creación de nuevos modelos de empresa, obligan a conocer el funcionamiento de esta, así como la preparación de una regulación que permita conocer el origen de los recursos que administra o transfiere.

[1] Cfr. http://www.cinu.mx/noticias/la/antonio-mazzitelli-el-experto-/ consultado el 8 de junio de 2019, 14:44 hs.

II. LA RESPONSABILIDAD PENAL DE LAS PERSONAS MORALES

Cuando nos referimos al sujeto activo estamos acostumbrados a pensar en la persona física que, por sí misma o a través de otra, actualiza el verbo núcleo del tipo, pero en los últimos años se ha hecho énfasis en que la persona jurídica o moral tenga una concepción similar para hacerla responsable penalmente. Y al respecto adelanto mi posición: la persona moral delinque a través de las personas que actúan en su nombre y, además, la persona moral puede ser el constructo jurídico para dar apariencia de empresa a lo que en realidad es una organización orientada a la comisión de un delito.

Hace algunos años, el doctor Fernando Flores García (1989) escribió unas líneas extraordinarias, cuando el tema no cobraba la vigencia que tiene hoy. En la conclusión de su análisis el maestro escribió:

> Se han logrado considerables avances y establecido puntos de coincidencia. Es de desearse que en futuros congresos jurídicos, en libros, ensayos, proyectos legislativos, etc., se renueven los esfuerzos para dar una solución que resuelva los problemas que en la vida real representan las actividades ilícitas de las personas jurídicas colectivas. (Flores, 1989; 1998)

Y es que al hablar de responsabilidad debe quedar claro si el concepto parte de la sustitución del juicio de reproche o bien, es la consecuencia procesal de un acto en particular. En todo caso, la voluntariedad y el conocimiento que exige la culpabilidad siempre serán un gran reto para quien diserte sobre este tema.

Recientemente, se han desarrollado distintas iniciativas de ley, derivadas de los instrumentos internacionales que ha firmado México, entre los cuales destacan: la Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional y la Convención de las Naciones Unidas Contra la Corrupción. Ambas contienen la posibilidad de que los Estados legislen sobre la responsabilidad penal de las personas jurídicas.

La Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional en su artículo 10 señala:

- la obligación de los Estados a adoptar medidas necesarias y establecer la responsabilidad de las personas jurídicas;
- las materias competentes para conocer de la responsabilidad se limitarán a penal, civil o administrativa;

- las responsabilidades serán excluyentes a la que se relaciona con la materia penal,
- los Estados velarán por la imposición de sanciones penales.

Por su parte, la Convención de las Naciones Unidas Contra la Corrupción establece lo siguiente:

- los Estados deberán adoptar medidas para establecer la responsabilidad de las personas jurídicas cuando se participe en las conductas tipificadas por la convención;
- las materias competentes para conocer de la responsabilidad se limitarán a penal, civil o administrativa;
- las responsabilidades serán excluyentes a la que se relaciona con la materia penal,
- los Estados velarán por la imposición de sanciones penales.

Asimismo, en el ámbito nacional, se ha abordado en varias iniciativas de ley lo relativo a la responsabilidad de las personas morales, con distintas perspectivas doctrinales y distintas soluciones. Además, se ha abonado lo relativo a los derechos humanos que le son propios a las personas jurídicas;[2] sin embargo, de la lectura de los pocos artículos que le dedica al tema el Código Nacional de Procedimientos Penales (artículos 421 al 425), podemos vislumbrar que el procedimiento penal a las personas jurídicas apenas está en sus comienzos y deberá ser en la legislación sustantiva donde deba ser regulado.[3]

[2] "Las personas morales gozan de aquellos derechos fundamentales que conforme a su naturaleza le resulten necesarios para la realización de sus fines con el fin de proteger su existencia, su identidad y asegurar el libre desarrollo de su actividad". Así lo estableció el Pleno de la Suprema Corte de Justicia de la Nación el 21 de abril de 2014, al resolver la Contradicción de Tesis 360/2013.

[3] Ramón Eduardo Ribas escribe sobre el procedimiento penal a las personas jurídicas: "La construcción de un sistema de responsabilidad penal de las personas morales puede encauzarse jurídicamente a través de dos vías fundamentales:

a) En primer lugar, acudiendo a las categorías y criterios de imputación penales ya conocidos.
b) Creando, en segundo término, un nuevo Derecho Penal, exclusivo de las entidades colectivas.

La primera de estas soluciones consiste en *adoptar* el Derecho Penal clásico, de base individualista, y aplicarlo a los comportamientos criminales protagonizados por entidades colectivas. Obviamente, dicha adopción y la subsiguiente aplicación no pueden realizarse de forma mecánica o automática; sería preciso ajustar, antes, mediante una reinterpretación funcionalista, la teoría del delito individual. Sin esta nueva normativización de los conceptos penales, la inadecuación de éstos para enfrentarse a formas de criminalidad colectiva obligaría a una *resignación descriptiva* o a crear un sistema de responsabilidad penal específico para empresas o personas colectivas. Característico de estos planteamientos es, en fin, su intento de adecuar las categorías penales a las personas jurídicas antes que sustituirlas por otras.

Radicalmente contraria a la flexibilización de las categorías penales existentes se muestra Zúñiga Rodríguez. En su opinión, dicha flexibilización comportaría el riesgo de «contaminar» todo el sistema de responsabilidad individual de esas ansias de «adaptabilidad», pudiendo desembocar en la pérdida de la validez de las garantías ganadas y construidas durante dos siglos. También Tamarit Sumalia considera, ante los riesgos de «contaminación conceptual» que pudieran derivarse de la integración de la responsabilidad de las personas jurídicas en el sistema penal, que sería aconsejable un «dualismo no disgregador del sistema.

La segunda solución, a mi juicio más plausible, toma como punto de partida la siguiente idea: las personas jurídicas, por ser sujetos diferentes, necesitan de

Sin embargo, bajo este tenor, las empresas *fintech* podrían ser imputadas penalmente si incurriesen en algún delito, en especial el blanqueo de capitales o lavado de dinero, cuya denominación en la legislación mexicana es operaciones con recursos de procedencia ilícita (CPF, 2014: art. 400 bis).

III. EMPRESAS TECNOLÓGICAS

Jorge Barrera Graf (2010) define a la empresa como un "conjunto de personas y cosas organizadas por el titular con el fin de realizar una actividad onerosa, generalmente lucrativa de producción o de intercambio de bienes y servicios destinados al mercado".[4] O bien, como lo define la Real Academia Española, como una "unidad de organización dedicada a actividades industriales, mercantiles o de prestación de servicios con fines lucrativos". Pero también encontramos definiciones que son más extensas por integrar un número más amplio de conceptos a los cuales se dedica. Tal es el caso de Julio García y Cristóbal Casanueva (2001), que en su libro *Prácticas de la gestión empresarial* la definen como una "entidad que mediante la organización de elemento humanos, materiales, técnicos y financieros proporciona bienes o servicios a cambio de un precio que le permite reposición de los recursos empleados y la consecución de unos objetivos determinados".

La capacidad de mutación que la empresa ha demostrado durante el transcurso de los años ha permeado hasta nuestros tiempos de forma que, gracias a ello, gran parte de la economía que perciben los países se ha visto beneficiada por ellas, por lo que se han generado diversas oportunidades para la creación de las mismas, así que ya no se limitan a sociedades civiles, colectivas, anónimas, o bien por tamaños, siendo pequeña, mediana o grande empresa, sino que han surgido diversos tipos, como lo son las *fintech*.

El tema que se expondrá en forma referencial, teórica y analítica requiere del entendimiento de diversos conceptos básicos de la materia para la comprensión mínima y correcta, por lo que a fin de entender el término *fintech* en su totalidad, y para pasar a una crítica de esta tecnología de financiamiento, nos vemos obligados a adentrarnos al tema, no sin antes definir lo

un derecho penal distinto del de las personas físicas, precisamente porque el problema es que éste no les resulte aplicable. Asumida la necesidad de un Derecho Penal distinto, será necesario determinar que deberá tener este nuevo Derecho *antiguo* para seguir conceptuándolo como Penal: si no tuviera nada, no nos hallaríamos ante un Derecho Penal distinto, sino, como indica García Arán, ante algo distinto del Derecho Penal". (Ribas, 2009: 281-282)

[4] Citado en Dávalos (2010:101).

que entendemos por *startup*, ya que como es sabido muchas empresas comienzan siéndolo y cambian al sector *fintech*.

IV. INICIOS DE UNA *STARTUP*

El término comienza a utilizarse en razón del surgimiento de diversas empresas pequeñas que ofrecen servicios innovadores; por ello podemos identificarlas como aquel proyecto original que se identifica por no tener un símil y, aunque el mundo empresarial la alcance, contará con un *business* plan y una ventaja competitiva que la ayudará a destacar de las otras empresas.

Steve Blank y Bob Dorf (2000) la definen como una "organización temporal en busca de un modelo de negocio rentable, que puede repetirse y que es escalable", pero también debemos tomar en consideración el concepto de *startup*. Según *Cambridge Dictionary* se entiende como "pequeño negocio que apenas ha empezado", o bien, como lo establece Montoya Pineda (2015), "es casi una hipótesis todavía en conducción y aún no demostrada en su totalidad, aunque también se asume en la región como una compañía consolidada demostrada en la práctica y vigente en los tiempos cambiantes".

El término de *startup* fue acuñado en los años 50 del siglo pasado en Silicon Valley, en donde —aproximadamente en 1957— se crea la primera empresa orientada a este concepto conocida como Fairchild Semiconductor.[5]

[5] Los párrafos anteriores nos permiten tener una serie de características que deben portar las *startups* que, en términos generales, envistamos no sin antes mencionar que es enunciativa, más no limitativa, por lo que podemos resumir en:

- Ideas innovadoras
- Rápido servicio
- Fácil de evolucionar
- Generalmente, apuestan por proyectos relacionados con la tecnología

La creación de las *startup* ha generado diversas empresas que en la actualidad son populares y muy utilizadas, como en el caso de Facebook, Amazon, Google, Privalia, Edreams, por mencionar algunas. Estas empresas se han valido de costos de inicio más bajos que para otros negocios de índole tradicional; esto limita las necesidades de financiamiento y ayuda a que a bajo costo se pueda crear la empresa. Lo anterior ha hecho creer a expertos en la economía que estas empresas se denominen como una "nueva economía"; esto, derivado de que exista la evolución de una economía basada en los progresos tecnológicos, principalmente, con ayuda las TIC.

Por lo mencionado anteriormente es que diversos organismos nacionales e internacionales se han interesado en dicho segmento, en especial los países miembros de la OCDE, pues según CEPDAL en 2013 se marcó una clara diferencia entre la economía de los países misma que tuvo influencia de estas *startup*.

Lo anterior se ve marcado en el estudio económico citado con antelación, ya que en dicho año la creación y desarrollo de esas empresas no se sentía propio en los países de América Latina. Sin embargo, en 2016 podemos apreciar que se sumaron esfuerzos para la creación de estas empresas y se cuenta con un "32% de *startups* en México dividido en 10% CDMX., 8% en Guadalajara y 8% en Monterrey. Pero otros países del continente también han dado paso a ellas, tal es el ejemplo de Chile con un 80%, también Brasil cuenta con 60% en São Paulo y 12% en Río de Janeiro" (OCDE , 2016).

V. EVOLUCIÓN DE *STARTUP* A *FINTECH*

Una empresa *startup* deja de serlo para convertirse en parte del sector *fintech*. Lo anterior ocurre como consecuencia de varios factores que comienzan a ocurrir: la cotización en bolsa, competencia en el mercado sobre el producto que se ofrece al público, deja de ser independiente y, en la mayoría de los casos, es adquirida por una empresa.

Pero la lista no termina ahí. Derivado de la gran cantidad de *startups* que se han convertido a *fintech*, se encuentra la empresa irlandesa Sedicii, que se ha encargado de generar un sistema para verificar la identidad de los usuarios; además, su sistema previene el robo de identidad. Pero también tenemos otras que, con base en una red global, ayudan a las empresas en tiempo real a fin de poder ofrecer financiamiento a los clientes.

VI. ¿QUÉ ES UNA *FINTECH*?

Una vez comprendidos los términos anteriores es de vital importancia definir lo que es una *fintech*, para lo cual nos apoyamos en el buró de entidades financieras: "Fintech deriva de las palabras 'financial technology' y se utiliza para denominar a las empresas que ofrecen productos financieros, haciendo uso de tecnologías de la información y comunicación, como páginas de internet, redes sociales y aplicaciones para celulares" (CONDUSEF).

Estas instituciones de tecnología financiera han aprovechado la innovación tecnológica y, la mayoría, su incorporación a grandes compañías a fin de desarrollar diversos productos y servicios que van desde la gestión de materia, ofrecimiento de seguridad financiera e incluso monederos digitales, los cuales muchas veces se acompañan de un asesoramiento online.

Las *fintech* se muestran en nuestra vida diaria en forma de páginas web, aplicaciones para teléfonos inteligentes o por medio de métodos que van de la mano con la tecnología. Lo anterior con ayuda de los bajos costos que manejan y aprovechando en todo momento la tecnología que tienen a su alcance;-situación que incluso implementaron como una ventaja, aunado a lo amigables que son sus servicios que, al contrario de los bancos, han sabido aprovechar para ganar más terreno en los negocios y la economía.

VII. CARACTERÍSTICAS

Las *fintech* poseen ciertas particularidades:

- bajo costo;
- financiamiento por diversos métodos de capital que incluso incluyen el de riesgos;
- información digitalizada;
- desafíos al sector bancario;
- productos únicos e innovadores;
- generalmente no se acude a ninguna sucursal,
- se componen por personas dispuestas a prestar su dinero a cambio de cierto rendimiento económico.

Estas entidades, mediante las características planteadas, resultan ser novedosas y en lo general atrapan a jóvenes que en su mayoría son el *target* de estas empresas; esto, debido a que son las personas que regularmente se encuentran más cerca de los proyectos tecnológicos que ofrecen innovación y trascendencia de servicio.

VIII. SERVICIOS OFRECIDOS

Si bien es cierto que las *fintech* se han caracterizado por realizar préstamos a cambio de cierto monto de rendimiento, también lo es que han sabido ampliar más allá el mercado meta a fin de ofrecer distintos tipos de servicios. De esta forma su crecimiento se ha visto favorecido.

Lo anterior ha tenido como consecuencia que las *fintech* se agrupen en distintos campos de especialización, lo cual ha beneficiado a que distintos segmentos que no han sido explotados o que han quedado atendidos de forma parcial se vean beneficiados; sin embargo, esto también representa un riesgo financiero, pues su situación no necesariamente será encontrada por las estadísticas que reflejen los sistemas financieros; esto de forma independiente sobre ciertas conductas delictivas que deriven de ellas como el lavado de dinero.

IX. EL ACIERTO DE REGULAR LAS *FINTECH*

Como consecuencia de los servicios que presta una *fintech*, está obligada a:

1. Establecer medidas y procedimientos para prevenir y detectar actos, omisiones u operaciones que pudieran ubicarse en los supuestos previstos en el Capítulo II del Título Vigésimo Tercero del Código Penal Federal.

2. Identificar a sus clientes y usuarios; de conformidad con lo establecido por los artículos 115 de la Ley de Instituciones de Crédito; 87-D, 95 y 95 Bis de la Ley General de Organizaciones y Actividades Auxiliares del Crédito.

3. Presentar ante la Secretaría los reportes sobre actos, operaciones y servicios que realicen con sus clientes y lleven a cabo funcionarios y empleados de la propia entidad.

4. Entregar a la Secretaría de Hacienda y Crédito Público, por conducto del

órgano desconcentrado competente, información y documentación relacionada con los actos, operaciones y servicios a que se refiere este artículo.

5. Conservar, por al menos 10 años, la información y documentación relativas a la identificación de sus clientes y usuarios o quienes lo hayan sido, así como la de aquellos actos, operaciones y servicios reportados.

6. Prohibición de uso de efectivo en las actividades vulnerables en caso de actualizar determinados montos, la cual dependerá de la actividad a realizar.

La supervisión, verificación y vigilancia del cumplimiento de las obligaciones a que se refiere esta sección, así como las disposiciones de las leyes que especialmente regulen a las entidades financieras se llevarán a cabo, según corresponda, por la Comisión Nacional Bancaria y de Valores, la Comisión Nacional de Seguros y Fianzas, la Comisión Nacional del Sistema de Ahorro para el Retiro o el Servicio de Administración Tributaria.

Como es sabido, la actividad realizada por estas empresas se ha dado de forma posterior a que las mismas se vieran implementadas y en operaciones. Esta deficiencia se ha visto en varios países no solo de América, sino de todo el mundo, y como consecuencia se han tenido que regular sus actividades para no afectar al sistema de pagos, al sector económico, la competencia entre empresas e incluso a los consumidores.[6]

El beneficio que ha existido al crear la regulación de las *fintech* consiste en poder seguir cuidando la solidez de las instituciones que se tienen en el país pues, como ya se había mencionado, existen múltiples beneficios que estas empresas han ofrecido al contrario de otras, como los sistemas bancarios, que se han quedado rezagados cuando el tema de la tecnología ha entrado en acción; a su vez, se ha dado la posibilidad de seguir dando crecimiento a estos temas de innovación sin dejarlos de lado, como ocurrió antes de su regulación cuando se crearon las normas después de que las acciones fueron visualizadas.

X. LA REGULACIÓN DE LAS *FINTECH* EN MÉXICO

Como un acierto se toma que México sea de los primeros dos países en América, junto con Brasil, en apoyar el desarrollo de las *fintech*, pues según *Fintech en América Latina 2018: crecimiento y consolidación*, en

[6] El país pionero en la regulación de las *fintech* es Reino Unido, quien en 2014 creó la Financial Conduct Authority y, misma que dedicó a las empresas que habían obtenido su capital de inversionistas y estos requerían sus ganancias. Así comenzó a otorgar permisos y planes para los casos de quiebra, hasta 2017 en donde aumentó los requisitos; sin embargo, también otorgó un periodo de prueba para las empresas a fin de que su terminación no acabara con sus activos. (Silva y Ramos, 2017)

2018, "Brasil aporta 380 emprendimientos de esta categoría mientras que México 273". En razón de lo anterior, México logró consolidar aquellas iniciativas en materia de regulación de las *fintech,* siendo así uno de los pocos países que contemplan una ley para la materia.

La legislación a la que hacemos referencia es la Ley para Regular las Instituciones de Tecnología Financiera, la cual contempla la innovación y estabilidad financiera, la sana competencia entre las empresas de esta índole, la protección a los consumidores y, además, la prevención del delito de operaciones con recursos de procedencia ilícita.

Dentro de esta legislación se contemplan diversos términos que ayudan a que una empresa no llegue a la quiebra de forma temprana por las implicaciones que esto conlleva. Por ello se tiene un *sandbox,* que no es otra cosa que los modelos novedosos, el cual permite que la empresa creada tenga un periodo de prueba a fin de no realizar ciertos trámites regulatorios, pues existe la posibilidad de que la empresa no tenga una vida duradera, por lo que existe un comité que evalúa su plan de negocios.

Estas instituciones de tecnología financiera, como lo denomina la ley sustantiva, las divide en dos tipos: una de ellas como colectivas y las otras de fondo de pago electrónico. Ambas deberán cumplir con las disposiciones de la Comisión Nacional Bancaria y de Valores (CNBV), quien tendrá un órgano especializado para asegurar que se cumplen las reglas impuestas en la norma. A su vez, cuenta con las facultades de investigación, inspección y revocación; sin embargo, no es la única autoridad que las rige en México, pues también deben estar acordes a las autoridades financieras, como el Banco de México (BANXICO), la Secretaría de Hacienda y Crédito Público (SHCP) y la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (CONDUSEF).

A. INSTITUCIONES DE FINANCIAMIENTO COLECTIVO

Son aquellas que realizan actividades con el fin de contactar a diversos sujetos con la finalidad de otorgarse financiamiento colectivo de deuda, capital y copropiedad o regalías, por medio de aplicaciones informáticas, interfaces, internet o cualquier medio de comunicación electrónico o digital. Estas instituciones actúan como mandatarias o comisionistas de sus clientes. Además, se regulan las obligaciones que tendrán que cumplir, entre las que se encuentran: dar a conocer los medios que utilicen para operar, analizar

e informar posibles inversionistas y entregar recursos a los inversionistas. Incluso, se muestran limitantes a su actividad, como resulta asegurar retornos o rendimientos sobre la inversión o garantizar el resultado o éxito de las inversiones.

B. INSTITUCIONES DE FONDOS DE PAGO ELECTRÓNICO

Son aquellas empresas que emiten, administran y transmiten fondos de pago automático de acuerdo con diversas aplicaciones informáticas, páginas de internet o medios de comunicación electrónica o digital.

La ley establece qué debemos considerar como fondos de pago electrónico y las facultades que tienen, pero a su vez las hipótesis en que podrán otorgar los créditos y préstamos. Por último, tenemos las prohibiciones, como no otorgar rendimiento o beneficio monetario a los clientes por el saldo que se acumule o mantenga en un momento dado.

Pero, para los efectos de esta ponencia, resulta de especial interés la ingente cantidad de delitos que la Ley para Regular las Instituciones Financieras (2018) ha establecido para las instituciones de tecnología financiera. A saber:

Delitos para la Protección del Patrimonio de los Clientes de las ITF y de las Sociedades Autorizadas para operar con Modelos Novedosos.

- A quien en forma indebida utilice, obtenga, transfiera o de cualquier otra forma, disponga de los recursos, fondos de pago electrónico o activos virtuales de los Clientes de las ITF, de las sociedades autorizadas para operar con Modelos Novedosos o de los recursos, fondos de pago electrónico o activos virtuales de éstas. (art. 119)
- Quien se encuentre facultado para disponer de los recursos a cargo de una ITF o una sociedad, Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos y no realice la devolución de éstos a sus clientes, estando obligado a hacerlo o se niegue sin causa justificada. (art. 120)
- Los accionistas, socios, consejeros, funcionarios, directivos, administradores, empleados o proveedores de una ITF o de una sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos, que desvíen los recursos, fondos de pago o activos virtuales de sus Clientes o de las propias ITF, para cualquier fin distinto al que se haya pactado. (art. 121)
- A quienes utilicen o divulguen la información financiera o confidencial de los Clientes para cualquier fin distinto al de la realización de las Operaciones, sin contar con autorización previa y expresa del Cliente. (art. 122)

Delitos contra la adecuada operación de las ITF, o de las Empresas Autorizadas para operar con Modelos Novedosos.

- Todo aquel que, habiendo sido removido o suspendido, por resolución firme de la CNBV, continúe desempeñando las funciones respecto de las cuales fue removido o suspendido o bien, ocupe un empleo, cargo o comisión, dentro del sistema financiero mexicano, a pesar de encontrarse suspendido para ello. (art. 123)
- Lleve a cabo operaciones o actividades de las reservadas para las ITF o para las sociedades o Entidades Financieras u otros sujetos supervisados por alguna Comisión Supervisora o por el Banco de México, autorizados para operar modelos novedosos, sin contar con la autorización prevista en esta Ley, y Habiendo sido autorizado para operar como ITF, realice actividades con activos virtuales o divisas, sin contar con la autorización a que se refiere el artículo 30 o bien, tratándose de instituciones de crédito, sin la autorización. (art. 124)
- Quien para obtener la autorización para operar como ITF o con Modelos Novedosos o con activos virtuales, proporcione información falsa a la autoridad financiera que corresponda. (art. 125)
- A quien proporcione a las Autoridades Financieras que correspondan, información falsa respecto de su situación contable, financiera, económica y jurídica, que le sea requerida en términos de esta Ley. (art. 126)
- A quien por sí o a través de un tercero, difunda, publique o proporcione al público de la ITF o sociedad autorizada para operar con Modelos Novedosos, información falsa o alterada o que induzca al error. (art. 127)
- A quien destruya, modifique total o parcialmente, los sistemas o registros contables o la documentación que dé origen a los asientos contables de una ITF o sociedad autorizada para operar con Modelos Novedosos, con anterioridad al vencimiento de los plazos legales de conservación. (art. 128)
- A quien se ostente frente al público en general como una ITF o sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con Modelos Novedosos. (art. 129)

Delitos para la Protección del Patrimonio de las ITF y de las Sociedades Autorizadas para operar con Modelos Novedosos.

- A quien valiéndose de cualquier medio físico, documental, electrónico, óptico, magnético, sonoro, audiovisual, informático o de cualquier otra clase de tecnología, suplante la identidad, representación o personalidad de cualquiera de las Autoridades Financieras o de alguna de sus unidades administrativas o áreas o de un servidor público, de las ITF o sociedades autorizadas para operar con Modelos Novedosos o de alguno de sus directivos, consejeros, empleados, funcionarios, dependientes o representantes legales. (art. 130)
- A quien utilice, realice u obtenga, por sí o a través de interpósita persona, cualquier servicio, Operación o producto proporcionado por alguna de las ITF o sociedad o Entidad Financiera u otro sujeto supervisado por alguna Comisión Supervisora o por el Banco de México, autorizado para operar con

Modelos Novedosos previstas en esta Ley bajo una identidad falsa o suplantada. (art. 131)

- Se sancionará con prisión de tres a nueve años y multa de 5,000 a 150,000 UMA, al que sin causa legítima o sin consentimiento de quien esté facultado para ello, acceda a los equipos o medios electrónicos, ópticos, informáticos o de cualquier otra tecnología de las ITF o sociedades autorizadas para operar con Modelos Novedosos. (art. 132)
- Al que sin autorización obtenga, extraiga o desvíe recursos, fondos de pago electrónicos o activos virtuales por medio de los sistemas o equipos de informática de las ITF o de las sociedades o Entidades Financieras u otros sujetos supervisados por alguna Comisión Supervisora o por el Banco de México, autorizados para operar con Modelos Novedosos. (art. 133)

Este nuevo catálogo de delitos especiales debe observarse de manera conjunta con la legislación establecida para combatir las operaciones con recursos de procedencia ilícita. Con lo que, lejos de considerar que se ha cubierto adecuadamente el problema, podemos considerar que se ha abierto un verdadero berenjenal para acreditar adecuadamente alguna de estas actividades.

XI. CONCLUSIONES

Las *fintech*, a la par de las nuevas tecnologías, vinieron a cambiar de manera toral el mercado al que sirven. Dieron una nueva faz a la empresa tal y como la conocimos apenas hace algunos años.

Pero, de manera proporcional a la novedad de estas empresas, la utilidad que potencialmente pudieran tener para el blanqueo de capitales, el flujo de activos y el financiamiento de actividades ilícitas reviste el mayor interés para conocer su funcionamiento y contar con mecanismos de supervisión.

Al respecto, se han creado leyes particulares para abarcar estos aspectos, prevenir el delito y sancionar el mismo acorde con una legislación que esté al día en la materia. Sin embargo, estamos ante el cambio emergente de las distintas actividades y procesos que abarcan, de modo tal que, en los años por venir, habrán de pasar por el tamiz de la eficacia del derecho o, de lo contrario, estaremos en presencia de un problema mayor: el flujo impune de activos virtuales.

Creemos que lejos de considerar que se ha cubierto adecuadamente el problema, podemos considerar que se ha abierto un verdadero berenjenal para acreditar adecuadamente alguna de estas actividades. La taxatividad será el tema ante los tribunales encargados de validar los tipos penales a la luz del principio constitucional de exacta aplicación de la ley.

Pronto sabremos si la misma está a la altura de los retos que representa este sector financiero y tecnológico.

XII. FUENTES DE CONSULTA

Banco Interamericano de Desarrollo (octubre de 2018). *Fintech en América Latina 2018: crecimiento y consolidación*. Disponible en https://publications.iadb.org/en/fintech-latin-america-2018-growth-and-consolidation

Blank, S. y Dorf, B. (2000). *El manual del emprendedor*. España: Ediciones Gestión.

Cambridge Academy (s.f.). *Diccionario de Cambridge*. Disponible en https://dictionary.cambridge.org/es/diccionario/ingles/start-up?q=startup, consultado el día 26 de mayo de 2019.

CONDUSEF (2017). *¿Qué son las Fintech?*. Disponible en https://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/educacion-financiera/763-que-son-las-fintech, consultado el 28 de mayo de 2019.

Dávalos Torres, M.S. (2010). *Manual de introducción al derecho mercantil*. México: Cultura jurídica.

Daza Gómez, C. (2001). *Teoría general del delito*. México: Cárdenas Editor.

Díaz Aranda, E. (2006). *Teoría del delito*. México: Straf.

Flores García, F. (1989). "La responsabilidad penal de la persona jurídica colectiva". En *Ensayos Jurídicos*, (120), pp. 99-143.

Flores García, F. (1998). "Principales corrientes acerca de la responsabilidad penal de la persona jurídica colectiva". En *Liber Ad Honorem Sergio García Ramírez*, Tomo II. México: IIJ-UNAM.

García Del Junco J. *Prácticas de la gestion empresarial*. Mc Graw Hill, Madrid, 2001.

Jiménez Huerta, M. (2000). *Derecho penal mexicano*, Tomo I. México: Porrúa.

Malo Camacho, G. (2000). *Derecho penal mexicano*. México: Porrúa.

Montoya, D. (2015). "Startups: tendencias en América Latina y su potencialidad para el crecimiento empresarial". En *Revista Contexto*, (4), pp. 7-20.

OCDE Dev Centro de Desarrollo (2016). *Estudios del Centro de Desarrollo Startup América Latina 2016 Construyendo un futuro innovador. Síntesis y recomendaciones de política*.

Pavón Vasconcelos, F. (2005). *Delitos contra el patrimonio*. México: Porrúa.

Real Academia Española (s.f.). Disponible en https://dle.rae.es/?id=EsuT8Fg, consultado el 25 de mayo de 2019.

Ribas, R. E. (2009). *La persona jurídica en el derecho penal. Responsabilidad civil y criminal de la empresa*. Granada: Editorial Comares.

Silva Nava, A. y Ramos Medina, M.C. (2017). *La evolución del Sector Fintech, Modelos de Negocio, Regulación y Retos*. México: FUNDEF.

Zamora Pierce, J. (2007). *Delitos Patrimoniales*. México: Porrúa.

LEGISLACIÓN Y TRATADOS

Código Penal Federal. *Diario Oficial de la Federación*. Última reforma publicada el 14 de marzo de 2014.

Código Nacional de Procedimientos Penales. *Diario Oficial de la Federación*. Última reforma publicada 22 de enero de 2020.

UNODC (2004). Convención de las Naciones Unidas Contra la Corrupción. Disponible en https://www.unodc.org/documents/mexico andcentralamerica/publications/Corrupcion/Convencion_de_las_NU_contra_la_Corrupcion.pdf

UNODC (2004). Convención de las Naciones Unidas Contra la Delincuencia Organizada Transnacional y sus Protocolos. Disponible en https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

SHCP (2018). Ley para Regular las Instituciones de Tecnología Financiera. *Diario Oficial de la Federación*. Disponible en http://www.diputados.gob.mx/LeyesBiblio/ref/lritf/LRITF_orig_09mar18.pdf

LA IDENTIDAD EN LA ERA DIGITAL

Alicia Rubí Guerra Valdivia*

*Actualmente labora en el Consejo de la Judicatura Federal. Cuenta con la certificación Ethical Hacking and Countermeasures (CEHv7).

PALABRAS CLAVE *KEYWORDS*

Biometría	*Biometrics*
Datos	*Data*
Derecho	*Law*
Identidad	*Identity*

Resumen. Las tecnologías de la información y comunicación representan un gran avance en la sociedad, así como un reto en cuanto a una adecuada legislación y tratamiento. En el presente artículo se destacan algunos retos que enfrentamos al respecto, evidenciando el papel tan trascendente que también nos corresponde a los que hacemos uso de la tecnología.

Abstract. The information and communication technologies represent a great development in society, but also implies a huge challenge in terms of its adequate legislation. This article highlights some challenges we face as a society in this regard and prove the important role that also come into those who make use of technology in daily basis.

SUMARIO:

I. IDENTIDAD E IDENTIDAD DIGITAL

La identidad es un término multívoco, su significado variará dependiendo del área de aplicación; por lo que, en un sentido general, podemos precisar dos características principales: la primera señala las particularidades de un objeto que lo distinguen de los demás; y la segunda determina las peculiaridades que permiten asegurar que es el mismo objeto en distintos momentos del tiempo. Estas dos características nos permiten forjar una correlación, ya que podemos distinguir un objeto de otros si este dura en el tiempo, y, solamente tiene sentido decir que un objeto permanece si podemos singularizarlo frente a los demás (Villoro, 2016: 190).

Bajo este aspecto, dentro del ámbito jurídico, nuestro máximo tribunal se ha pronunciado acerca de lo que entendemos por derecho a la identidad, el cual postula que toda persona desde su nacimiento debe acceder a una identidad, la cual se entiende como el conjunto de rasgos propios de un individuo que lo caracterizan frente a los demás y que le dan consciencia de sí mismo; razón por la cual se relaciona con otros derechos fundamentales como el nombre, nacionalidad, la filiación o personalidad jurídica.

Hoy en día, con el uso de las tecnologías de la información y comunicación, queda clara la necesidad —creada y aceptada— de forjar una identidad digital,[1] pues en la mayoría de los casos no es suficiente contar con una identidad, sino que es menester crearla digitalmente. Nativos y migrantes digitales disponemos de una comunicación más ubicua, portátil e inmediata y podemos notar algo que no puede pasar desapercibido: la creación de nuestra identidad digital.

Podemos entender como identidad digital al conjunto de datos relacionados a una entidad. Dicha información representa a esa entidad frente a terceros, situación que

[1] Cabe destacar que en 2018 se llevó a cabo en México el denominado *Primer Seminario de Identidad Digital en México.* En mayo de 2019, *El Economista* presentó una nota de la cual se advierte —entre otras cosas— la idea de una asociación de identidad digital a partir del seminario en comento, además del fomento y la ayuda a la consolidación "de ecosistemas de identidad digital en México", así como la colaboración "con las autoridades en la formación y maduración de una normativa legal para el uso de la identidad digital en México". La nota completa se encuentra disponible en la siguiente liga: https://www.eleconomista.com.mx/tecnologia/Presentan-la-Asociacion-de-Identidad-Digital-de-Mexico-20190521-0094.html

nos permite identificarnos y diferenciarnos unos de otros con ayuda de la tecnología. Compuesta de un conjunto de características diversas que cumplen con estas propiedades, resulta entonces exponencialmente trascendente la información que decidimos aportar a través de las TIC; misma que se va almacenando a medida que la proporcionamos.

Søren Aabye Kierkegaard afirmó en su momento que *la vida se vive hacia delante, pero se entiende hacia atrás*, y así sucede con nuestra identidad digital, pues los vestigios que decidimos que se queden en la red y de los que vamos haciendo partícipes a terceros serán los que nos forjen dicha identidad. Puede decirse entonces que la identidad digital, tanto de personas físicas como morales, va siendo alimentada continuamente según las necesidades que se presenten; y si para una persona física es elemental un criterio adecuado sobre la creación de esta, cabe precisar que para personas morales resulta de suma importancia la elaboración de la misma, pues debe estar basada en la seguridad, sencillez y confianza que se genere al interactuar con ellas.

II. BIOMETRÍA

Teniendo como premisa lo referido en párrafos precedentes, podemos inferir que dentro de la identidad se encuentran los datos biométricos.

La biometría[2] consiste en el reconocimiento automático de las personas en función de sus características físicas únicas y de comportamiento, por lo que debe elegirse una característica lo suficientemente variable de un individuo a otro (la cara, la huella, la geometría de la mano, el iris, la voz, las venas, el pulso cardiaco, la radiografía dental, el ADN, la forma de escribir a mano,[3] etcétera). El funcionamiento de esta tecnología consta de una parte física que en la mayoría de las ocasiones son sensores que llevan a cabo las mediciones, y una parte lógica que ejecuta las comparaciones de los datos que han sido registrados previamente (Cortés, Medina y Muriel, 2010), valiéndose del reconocimiento de formas, inteligencia

[2] No pasa desapercibido que el término de *biometría*, dependiendo del autor, puede ser tomado como una ciencia o como las técnicas de uso. Al respecto, tenemos lo siguiente:

A) Richard Hopkins (1999) en su libro, *An Introduction to Biometrics and Large Scale Civilian Identification*, señala: "La definición estricta de la biometría es la ciencia que implica el análisis estadístico de las características biológicas".

B) Por otro lado, la acepción que se le da a la misma también puede referirse como la técnica a través de la cual la estadística auxilia a diferentes ciencias para resolver problemas (King y Stansfield, 2006).

[3] También conocido como "reconocimiento de escritor", mismo que consiste en identificar al autor de determinado texto manuscrito auxiliándose de un software de reconocimiento óptico de caracteres; lo anterior, bajo la premisa de que cada persona tiene una manera única de escribir, teniendo en consideración rasgos propios e inconfundibles para las letras. Situación que, indiscutiblemente, nos remite a los peritos en grafoscopía.

artificial, algoritmos matemáticos y aprendizaje de computadoras, entre otras cosas.

A. DATOS BIOMÉTRICOS

En razón de lo anterior, podemos identificar como dato biométrico a aquel que surge a través de un proceso de registro o codificación de las características de la persona física a la que corresponde el registro y la hace identificable entre los demás.

Los motivos para hacer uso de la biometría son variables y con frecuencia coinciden (Pato y Millett, 2010). Esto es, se piensa en un mejoramiento en la eficiencia de transacciones y acceso,[4] en reducir el fraude y la usurpación de identidad y, por supuesto, en una mejora en cuanto seguridad pública y privada, entre otras cosas. No obstante ello, habrá que cuestionarse la efectividad, el uso correcto y la manipulación de los mismos;[5] contextos variables que se ven reflejados en un impacto social y en consecuencias de privacidad por sus secuelas legales y políticas.

Como se ha planteado a lo largo de este artículo, la identidad se forja a partir de ciertas características y datos que son propios de cada persona física o moral, por lo que se estima necesario destacar que el buen uso de los datos biométricos parte de la trascendencia que estos tienen al ser considerados bajo ciertas circunstancias y para efectos legales, como datos personales. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales se ha pronunciado al respecto (INAI, 2018), haciendo hincapié en que un dato biométrico aislado que no esté registrado en un sistema biométrico y no pueda ligarse con una persona física particularmente o sea comparado con otras muestras no tiene el carácter de dato personal, ya que no puede identificar a su titular.

Caso similar sucede al darles el carácter de dato personal sensible, pues deberá cumplir con alguno de los supuestos contemplados por las leyes en materia de protección de datos, estos es: primero, la afectación de la esfera más íntima del titular;

[4] A manera de ejemplo, tenemos el caso del banco británico Barclays, que desde 2014 anunció el ofrecimiento para que, a partir de 2015, sus clientes contaran con la posibilidad de tener acceso a sus cuentas bancarias a través de un lector biométrico que detectaba las venas del dedo índice de cada cliente con el fin de dificultar el fraude por usurpación de datos personales.

[5] Uno de los casos más recientes es el de la aplicación FaceApp, que volvió a ser tendencia (después de 2017). Esta "novedad", alentaba a usuarios para que a través de dicha aplicación y por medio de su filtro "edad", compartieran fotografías en sus redes sociales (en su mayoría, aunque no limitativamente) con su rostro cambiado para simular un envejecimiento. Los términos y condiciones de la aplicación en comento no varían tanto respecto de otras, poniendo nuevamente de manifiesto cómo renunciamos a nuestra privacidad sin ser conscientes del alcance de ello; dejándonos, entre otras cosas, vulnerables a ser capturados digitalmente en usos de reconocimiento facial futuros.

segundo, que el uso indebido pueda dar origen a discriminación; y, tercero, que conlleve al titular a un riesgo grave.

Lo anteriormente abordado puede brindar un panorama general respecto a los casos en los que los datos biométricos son considerados como datos personales y datos personales sensibles; y, consecuentemente, proporcionar indiscriminadamente a terceros nuestros datos biométricos puede tener consecuencias desfavorables.

Actualmente, nos enfrentamos a la poca claridad referente a los datos biométricos y su adecuada protección en la legislación mexicana. Situación que se encuentra ligada a la falta de información por la cual se dan a conocer los mecanismos usados en la recolección, almacenamiento y análisis de los datos biométricos, así como del alcance de las políticas de los que tendrán la información en comento, o bien, si serán compartidos o transferidos entre distintos organismos públicos y privados y bajo qué circunstancias; por lo que la insuficiencia de una regulación apropiada al respecto no permite garantizar en su totalidad el tratamiento correcto de los datos biométricos, aun cuando los sujetos obligados tengan una serie de obligaciones. Esto, en razón de que los sistemas de identificación biométricos incrementan los riesgos de falsos positivos y de irrupciones a bases de datos que los contengan, en comparación a los riesgos de seguridad asociados a sistemas de identificación tradicionales.

Como hemos observado, dos de las características con las que cuentan estos datos es que son únicos e irremplazables, lo cual significa que se debe de tener especial cuidado para protegerlos de *robo*[6] o pérdida para que la identidad del titular no se vea comprometida, así como regular específicamente lo que pasaría bajo estos supuestos.

III. USURPACIÓN DE IDENTIDAD

La usurpación de identidad es una conducta ilícita que ha sido y sigue siendo una actuación que se encuentra presente prácticamente en cualquier ámbito de la sociedad.

Arreola González señala:

> El delito de usurpación de identidad, se tipifica como una conducta antijurídica, dolosa que emana de un individuo

[6] El director ejecutivo de la Red en Defensa de los Derechos Digitales, Luis Fernando García, hizo un señalamiento interesante en cuanto a datos biométricos: "El riesgo es mayor en comparación con otros datos, porque no se pueden cambiar. Por ejemplo, si te roban la contraseña, la puedes cambiar. Pero si se trata de las huellas digitales, no se puede. Y esos datos en manos equivocadas es muy peligroso". La nota completa está disponible en https://www.proceso.com.mx/464952/sistemas-biometricos-identificacion-los-ciber-riesgos. Consultado en línea el 04 de agosto de 2019.

> que dispone de la información personal de otro, sin su autorización con el ánimo de cometer una diversidad de delitos, manipulando diferentes fuentes para obtener la información íntima de una persona a través de un engaño hacia la víctima, y al mismo tiempo, maniobrando diversos medios convencionales y Tecnologías de la Información y Comunicación para realizar el delito, originándole un daño patrimonial o moral. (Arreola, 2017: 9)

En un ámbito penal, y por lo que hace a la legislación mexicana, el delito de usurpación de identidad se contempla únicamente en algunas leyes estatales,[7] encontrando la conducta en comento como usurpación de identidad o suplantación de identidad; lo que inevitablemente nos dirige a un tema de suma trascendencia, el cual se ha comentado: un Código Penal Nacional en México.

Al respecto, cabe precisar que el experto penalista, el doctor Alberto Enrique Nava Garcés, ha manifestado acertadamente en ocasiones previas la importancia de la realización de este proyecto, pues, tal como lo refirió, nos enfrentamos a la necesidad de:

> … contar con un sistema de justicia penal homologado, que tenga aplicación en todo el territorio y no permita que se formen nichos de impunidad derivados de los tantos códigos penales que regulan las conductas reprochables tanto en el ámbito federal como en las distintas entidades.[8]

Unificar criterios disímiles que prevalecen en las legislaciones locales implicaría emitir un criterio jurídico genuino a partir de casos concretos y subsanar el vacío jurídico que actualmente enfrentamos al respecto.

A. USURPACIÓN DE IDENTIDAD A TRAVÉS DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Dentro de la cadena de seguridad informática, el eslabón más débil es el factor humano; por ello, dentro de las técnicas que pueden ser útiles con el fin de cometer actos ilícitos, en este caso en particular la usurpación de identidad, podemos citar la ingeniería social.

[7] En el ámbito estatal, el delito de usurpación de identidad se encuentra contemplado en los códigos penales de: Durango, Colima, *Distrito Federal*, Hidalgo, Zacatecas, Nayarit, Baja California Sur, Tlaxcala, Guanajuato, Estado de México, Michoacán de Ocampo, Tamaulipas y Quintana Roo.

Por otro lado, una conducta delictiva similar tipificada como suplantación de identidad se contempla en los códigos penales de Campeche, Sinaloa, Chiapas, Nuevo León y Baja California.

[8] La entrevista realizada en mayo de 2018 al Dr. Enrique Alberto Nava Garcés puede ser consultada en su totalidad en la siguiente liga: https://elmundodelabogado.com/revista/posiciones/item/las-nuevas-tecnologias-y-el-codigo-penal-nacional. Consultado en línea al 30 de julio de 2019.

B. INGENIERÍA SOCIAL

La ingeniería social es la acción o conducta social destinada a conseguir información de las personas cercanas a un sistema con la finalidad de obtener datos de interés valiéndose de habilidades sociales. Dichas prácticas se encuentran relacionadas con la comunicación entre seres humanos (Borghello, 2019: 2).

Asimismo, podemos dividir la ingeniería social en dos factores principales: 1) técnicas que se valen de la interacción con máquinas; y 2) las basadas en la interacción humana (Xiangyu, Qiuyang y Chandel, 2017: 25-34); por consiguiente, la mayoría de los ataques aumentan sus posibilidades de éxito a partir de la combinación de ambos elementos.

Es importante puntualizar que la conducta delictiva podrá llevarse a cabo de forma directa o indirecta (Salahdine y Kaabouch, 2019). Para el caso de los ataques clasificados de forma directa, se usa el contacto directo entre el atacante y la víctima para realizarlo. En esta categoría podemos mencionar los que son realizados por contacto físico, visual o interacciones de voz. Cabe precisar que también pueden requerir la presencia del atacante en el área de trabajo de la víctima. A manera de ejemplificación, encontramos: acceso físico, *shoulder surfing*,[9] *dumpster diving*,[10] ingeniería social telefónica, suplantación en llamadas y robo de documentos importantes, entre otras.

Ahora bien, por lo que hace a los ataques llevados a cabo de forma indirecta, bastará precisar que estos no requieren la presencia del atacante para llevarse a cabo, es decir, el ataque se puede lanzar de forma remota a través de un *software* malicioso por archivos adjuntos de correo electrónico o mensajes. Ejemplos de estos ataques son: *phishing*,[11] *software* falso, ventanas emergentes, *ransomware*,[12] *smishing*[13] e ingeniería social inversa.[14]

[9] *Shoulder surfing*: es la técnica de observación directa al usuario para obtener datos.

[10] *Dumpster diving*: es la revisión de los papeles y documentos que se tiran a la basura y no son destruidos de manera segura.

[11] *Phishing*: técnica para intentar adquirir datos confidenciales, como números de cuenta bancaria, a través de una solicitud fraudulenta por correo electrónico o de un sitio web, en el que el atacante se hace pasar por una persona legítima.

[12] *Ransomware*: tipo de malware que intenta denegar a un usuario el acceso a sus datos, generalmente cifrándolos con una clave conocida por el atacante, hasta que se pague un *rescate*.

[13] *Smishing*: variante del *phishing,* es cuando alguien intenta engañar a un usuario para que proporcione información privada a través de un texto o un mensaje SMS.

[14] Ingeniería social inversa: podemos resumirla en tres pasos: sabotaje, publicidad y asistencia. En el primer paso, un atacante encuentra una manera de sabotear una red, desde lanzar un ataque contra el sitio web del objetivo o simplemente enviando un correo desde una dirección fraudulenta, haciendo creer a las víctimas la existencia de un problema. Posteriormente, el atacante da a conocer una "solución" a la problemática suscitada. Finalmente, la víctima (habiendo sido engañada) contacta al atacante y le brinda accesos, por lo que, habiendo

Sin duda, quien lleve a cabo la suplantación se vale de técnicas y habilidades en cuanto al lenguaje, pues se presupone una interacción con la víctima, por lo que el atacante depende en gran medida de su capacidad para desarrollar una relación de confianza con el objetivo y hacer una primera impresión positiva para ganarse la confianza de la víctima.[15]

Una vez abordado el panorama que precede, se estima conveniente hacer notar la diferencia que existe entre identidad digital y reputación digital, ya que, si bien la primera es la que cada persona física o moral se forja en línea respecto de sí misma, la variante radica en que la segunda dependerá de los juicios que terceros emitan al respecto,[16] de modo que la reputación es una consecuencia de la identidad.

Un atributo característico de la identidad que vamos formando en la red es la libertad que tenemos para compartir datos personales de manera voluntaria, expresar opiniones y el acceso a una gran cantidad de información. Según Lichtenberg *no hay que juzgar a los hombres por sus ideas, sino por aquello en lo que sus ideas los convierten*; e invariablemente nos damos a esa tarea ayudados de la tecnología, ya sea creando opiniones respecto de nuestra persona o la de terceros, dando pie a una ilusión de convivencia perfectamente trabajada, aunque no siempre en el mejor sentido. Nuestro derecho a una libre expresión lleva consigo la obligación de un buen criterio y respeto.

IV. LIBERTAD DE EXPRESIÓN

Es de gran trascendencia e impacto el buen criterio que debe de imperar al forjar y seguir alimentando nuestra identidad digital, lo que inevitablemente nos remite a otro derecho: la libertad de expresión.

La Suprema Corte de Justicia de la Nación se ha pronunciado respecto a la libertad de expresión y

obtenido el acceso, se podrán implementar *loggers*, robar datos confidenciales, etcétera.

[15] Aun cuando las diversas instituciones bancarias han advertido a sus clientes que no se revelen datos sensibles respecto de sus cuentas por teléfono —o cualquier otro medio—, los atacantes siguen valiéndose de llamadas telefónicas para obtener dicha información y llevar a cabo diversas conductas delictivas.

La Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros hace referencia a que México ocupa el octavo lugar a nivel mundial en el delito de robo de identidad; asimismo, indica que el 67% es por pérdida de documentos, 63% por robo de cartera y portafolio y el 53% por información tomada de una tarjeta bancaria. La nota completa se encuentra disponible en https://www.condusef.gob.mx/Revista/index.php/usuario-inteligente/consejos-de-seguridad/563-robo-de-identidad, y las estadísticas en https://www.condusef.gob.mx/gbmx/?p=estadisticas. Sitios consultados el 01 de agosto de 2019.

[16] En concordancia con lo referido por Carlos Pinzón al hacer hincapié en que la identidad digital es pilar de la reputación *on-line*, se estima que una no puede subsistir sin la otra. http://www.inveniopro.es/diferencia-entre-identidad-digital-y-reputacion-on-line/. Consultado en línea al 30 de julio de 2019.

sus diversas vertientes. Caso concreto podemos remitirnos a la resolución de 20 de junio de 2013 relativa a la acción de inconstitucionalidad 29/2011,[17] en la cual nuestro máximo tribunal esclarece lo siguiente:

> … la libertad de expresión constituye un derecho preferente, ya que sirve de garantía para la realización de otros derechos y libertades.[18] En efecto, tener plena libertad para expresar, recolectar, difundir y publicar informaciones e ideas es imprescindible, no solamente como instancia esencial de auto-expresión y auto-creación, sino también como premisa para poder ejercer plenamente otros derechos humanos –el de asociarse y reunirse pacíficamente con cualquier objeto lícito, el derecho de petición o el derecho a votar y ser votado– y como elemento funcional que determina la calidad de la vida democrática de un país.

En México tenemos derecho a gozar de un ámbito de proyección de existencia que quede reservado de la invasión y la mirada de los demás y que a su vez provea de las condiciones necesarias para el despliegue de nuestra identidad, compartiendo de manera consciente la información que estimemos adecuada y/o necesaria para un fin en particular. Por lo que, en un sentido más amplio, la protección de nuestra información también dependerá en gran medida del buen criterio que cada persona tenga al brindar de alguna manera ciertos datos.

Hoy en día, las TIC representan un medio esencial para la creación de nuestra identidad digital. Compartir lo que pudieran ser elaboradas peroratas no siempre resulta lo más conveniente, ya que, ocasionalmente, un error se disfruta como virtud. En el mundo digital actual podemos excusarnos en interpretaciones y sentidos dirigidos a ideas concretas, creamos continuamente la ilusión de un idioma privado compartido en forma íntima únicamente con aquellos que no difieren con nuestro pensar.

La libertad de expresión da pauta a que de manera simultánea nos equivoquemos u ofendamos al manifestar nuestro derecho de pensar y expresarnos; sin embargo, el respeto es un valor moral que las leyes no pueden imponer —independientemente de los indicios que haya al respecto—, situación que nos ha llevado a conformarnos con un instrumento más modesto: la tolerancia.

En varios casos, nuestro derecho a la libertad de expresión ha sido usado, no solamente para una confrontación de opiniones, sino también para proliferar inexactitudes

[17] Disponible en: http://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=132774. Consultado el 30 de julio de 2019.

[18] Por ejemplo, la Primera Sala ha desarrollado su doctrina sobre este tema, principalmente, en el amparo directo en revisión 2044/2008, sentencia de 17 de junio de 2009, en el amparo directo 28/2010, sentencia de 23 de noviembre de 2011 y en el amparo directo 8/2012, sentencia del 4 de julio de 2012.

y calumnias, creando noticias falsas para ser propagadas. Es evidente que la falsedad en las noticias tiene mejor desenlace, pero no siempre se puede ser capaz de sostener un repertorio de engaños. La desventaja radica en las consecuencias generadas a partir de la desinformación y, por supuesto, el engaño del que se hace partícipes a los usuarios.

A. NOTICIAS FALSAS

Las noticias falsas son también conocidas como *fake news,* término usado para conceptualizar la divulgación de noticias falsas que generan un círculo de desinformación. Las redes sociales permiten y facilitan que los usuarios sean productores y consumidores de diversos contenidos a la vez, y favorecen la difusión de información engañosa, falsa o fabricada (FIP, 2018).

Bajo ciertas circunstancias pareciera que el inventar noticias falsas cumple con una necesidad social y no necesariamente dotada de sentido común, pues la desinformación en internet es de los principales peligros a los que se puede enfrentar una sociedad democrática. A través de varios heterónimos, y a veces sin valerse de estos, se crean noticias falsas cuyo objetivo puede ser directamente una afectación económica, o bien, un objetivo ideológico de cualquier índole.

Valerse de la tecnología para acceder a la información ha dado lugar a que la autenticidad de las notas esté aún más cuestionada, o por lo menos así debería de ser bajo determinadas circunstancias. Otorgar inmediatamente el carácter de auténtico a la información que se comparte por medios sociales ha dejado de resultar la mejor forma de estar adecuadamente informado, pues la popularidad de una noticia, el grado en que esta genere indignación, los sesgos de confirmación y el nivel de implicación de las personas con los contenidos son elementos esenciales para impulsar su propagación, y, conjugados estos, los contenidos se vuelven virales a gran velocidad y escala, con independencia de la veracidad que los inviste (Bradshaw y Howard, 2018).

La gran mayoría hemos sido espectadores —por lo menos— de la enorme influencia que ejercen las redes sociales en la propagación de información, de ahí que derive la trascendencia política al valerse de estas plataformas; movimientos sociales siguen apoyándose de estas para asegurar y generar un gran impacto en distintos ámbitos.

En México, nuestro Código Penal Federal contempla sanciones para la propalación dolosa de noticias falsas por lo que hace a la economía

pública y las jornadas electorales (CPF, arts. 254, fr. III; 405, fr. XI y 406, fr. V). En esta misma línea, en algunos estados existen normativas estatales que contemplan conductas como el *ciberacoso,* abordando vagamente la idea del uso de las TIC como instrumento de hostigamiento o amenaza; sin embargo, uno de los grandes retos es encontrado en el desafío de diseñar e implementar soluciones que regulen a las redes sociales de forma tal que se evite una interferencia política autoritaria sin reprimir la libertad de expresión, pues existe una delgada línea entre nuestro derecho fundamental y la supresión de contenido perjudicial para la sociedad, sobre todo dentro de un ámbito político. En ese sentido, las mejores estrategias serán las decisiones tomadas a partir del buen criterio de los usuarios, razón por la cual es tan importante fomentar una cultura que valore y promueva la verdad, así como que reconozca la diferencia entre especulación y verdad.

V. CONCLUSIONES

Sin duda, nuestras condiciones de vida se ven mejoradas con las TIC y aun con ellas seguimos dando un valor a nuestra necesidad de existencia, lo que se traslada al ámbito digital. La interacción con personas nos permite experimentar el sentimiento de ocupar un lugar en el vínculo social, dando pie al disfrute de una autonomía y suficiencia personal para formar nuestra identidad.

Los datos biométricos forman parte de nuestra identidad. Aun cuando los sistemas de reconocimiento humano son falibles,[19] la posibilidad de error es mínima, por lo que se resalta la importancia en el robustecimiento de los sistemas biométricos, particularmente a medida en que estos vayan cobrando importancia, considerando que lo óptimo es que el diseño y la evaluación de estos sea bajo contextos específicos y no genéricos, pues su efectividad dependerá en gran medida del entorno social y del fortalecimiento de la tecnología y

[19] Las características biológicas de cada persona están sujetas a cambios, por lo que se estima que la biometría no es, en consecuencia, una ciencia exacta, debiendo de tener en consideración la gran variante de mecanismos que existen para la interpretación de datos, así como también las diferentes condiciones ambientales que imperaron al momento de que los datos en comento fueron capturados. A manera de ejemplo podemos citar las huellas digitales, que pueden ser marcadas o mutiladas deliberadamente de manera temporal, dañadas por factores externos o distorsionadas al momento de colocar el dedo; situaciones que hacen que la biométrica de una huella digital se torne variable, lo que puede generar que la confiabilidad del proceso de identificación se complique.

Lo mencionado en el párrafo precedente compete a una calidad biométrica que se enfoca a una calidad de muestra, sin embargo, se destaca la importancia que tienen los metadatos en los sistemas operativos, pues "las bases de datos necesitan estar al tanto de las relaciones erróneas entre los elementos de los datos, los cuales generalmente se generan por causas administrativas más que por causas biométricamente específicas". (Moses, s.f.)

seguridad que impliquen. El uso de la tecnología conjuntado con la biometría da resultados altamente eficientes para acelerar el proceso de identificación, haciéndolo práctico, rentable y preciso; empero, representa todavía un gran desafío tanto en un ámbito de funcionamiento eficiente y fiable como en la legislación al respecto.

En la usurpación de identidad, los ataques serán tan variados como la capacidad de quien los diseñe lo permita. Nos enfrentamos a una conducta delictiva que repercute en diversos ámbitos, ya sea con entidades bancarias o en las propias redes sociales al ser víctimas de la creación de perfiles falsos, por mencionar algo. Es por ello que es de gran trascendencia la mesura y el buen criterio que los usuarios debemos tener al compartir nuestros datos, pues en una era donde las diversas plataformas son parte de nuestro entorno, valorar nuestros datos personales ayudaría a mitigar la problemática que representa la usurpación, ya que un atávico sentido de prudencia podría evitar consecuencias adversas. Cabe precisar que no se pretende llegar a extremos de posturas como solución, sino que el buen uso de nuestra información dependerá de la colaboración de quien la brinde, quien la obtenga y su adecuada regulación.

Finalmente, se debe de considerar al hacer frente a los vacíos legales que, aun cuando la interpretación de diversas disposiciones en cuanto a la seguridad que se brinda a la identidad de una persona destaca que las personas pueden expresar libremente su identidad (en relaciones con la sociedad o en lo individual), vale la pena enfatizar su vinculación con otros derechos, por lo que las afirmaciones contenidas en las regulaciones deben ser útiles en la medida en que no sean tomadas de forma descontextualizada y surja su correcta interpretación a partir de un análisis minucioso entre los diferentes escenarios jurídicos en los que se encuentren en riesgo los derechos de las personas.

VI. FUENTES DE CONSULTA

Arreola González, J. (2017). *Delito de usurpación de identidad. La homogeneización del sistema jurídico*. México: Flores.

Borghello, C. (abril de 2009). "El arma infalible: la Ingeniería Social", en *Technical & Educational Manager de eset para Latinoamérica*, p. 2. Disponible en http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf. Consultado el 31 de agosto de 2019.

Cooke, K. (31 de octubre de 2017). "'Fake news' reinforces trust in mainstream new brands". En Kantar UK. Disponible en https://uk.kantar.com/business/brands/2017/trust-in-news/

Cortés Osorio, J., Medina Aguirre, F. y Muriel Escobar, J. (diciembre de 2010). "Sistemas de seguridad basados en biometría". En *Scientia et Technica*, XVII, (46), Colombia: Universidad Tecnológica de Pereira. Disponible en https://www.redalyc.org/pdf/849/84920977016.pdf. Consultado el 02 de agosto de 2019.

Department of Homeland Security (24 de Agosto de 2017). *The future of ransomware and social engineering*. Disponible en https://www.dni.gov/files/PE/Documents/6---2017-AEP_The-Future-of-Ransomware-and-Social-Engineering.pdf

Díaz Limón, J. (2019). *Abogado digital, estudios sobre derecho cibernético, informático y digital*. México: Vlex.

Doctor, K. (26 de septiembre de 2017). "Newsonomics: Our Peggy Lee moment: Is that all there is to reader revenue?". En *NiemanLab*. Disponible en https://www.niemanlab.org/2017/09/newsonomics-our-peggy-lee-moment-is-that-all-there-is-to-reader-revenue/

FIP (2018). *¿Qué son las fake news? Guía para combatir la desinformación en la era de la posverdad*. Documento disponible en https://www.ifj.org/fileadmin/user_upload/Fake_News_-_FIP_AmLat.pdf. Consultado en línea el 06 de agosto de 2019.

Grevtsova, I. (9 de mayo de 2015). "¿Qué es el patrimonio digital?". En Digital Heritage & Culture. Disponible en https://irinagrevtsova.com/que-es-patrimonio-digital/

Google (febrero de 2019). *How Google Fights Disinformation*. Disponible en https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/How_Google_Fights_Disinformation.pdf

Herrán Aguirre, A. (2019). *Libertad de expresión y el internet*. México: Tirant lo Blanch.

Hopkins, R. (1999). "An introduction to biometrics and large scale civilian identification". En *International Review of Law, Computers & Technology*, 13(3), Yarm, UK, pp. 337-363.

IFAI (2018). *Guía para el tratamiento de datos biométricos*. Documento disponible en http://inicio.ifai.org.mx/DocumentosdeInteres/GuiaDatosBiometricos_Web_Links.pdf. Consultado en línea el 04 de agosto de 2019.

King, R. y Stansfield, W. (2006). *A Dictionary of Genetics*. Nueva York: Oxford University Press.

Lira Arteaga, O. (2018). *Cibercriminalidad. Fundamentos de investigación en México*. México: Ubijus.

Nava Garcés, A. (Coord). (2019). *Ciberdelitos*. México: Tirant lo Blanch.

Moses, K. (s.f.). *Sistema Automatizado de Identificación de Huellas Dactilares (afis)*, Documento disponible en https://www.ncjrs.gov/pdffiles1/nij/250979.pdf. Consultado el 04 de agosto de 2019.

OEA. Declaraciones conjuntas. Disponible en http://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp

Salahdine, F. y Kaabouch, N. (2 de abril de 2019). "Social Engineering Attacks: A Survey". En *Future Internet*, 11(89), USA: School of Electrical Engineering and Computer Science, University of North Dakota.

Pato, J., y Millet, L. (2010). *Biometric Recognition: Challenges and Opportunities*. Washington: National Academy of Sciences. Disponible en https://dataprivacylab.org/TIP/2011sept/Biometric.pdf. Consultado en línea al 03 de agosto de 2019.

Redacción (26 de diciembre de 2018). "Code of Practice on Disinformation". En Digital Single Market. Disponible en https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

Redacción (13 de septiembre de 2019). "Tackling online disinformation". En Digital Single Market. Disponible en https://ec.europa.eu/digital-single-market/en/tackling-online-disinformation

Toler, A. (19 de febrero de 2019). "Using the New Russian Facial Recognition Site SearchFace". En Bellingcat. Disponible en https://www.bellingcat.com/resources/how-tos/2019/02/19/using-the-new-russian-facial-recognition-site-searchface-ru/

UNESCO (2018). *Journalism, fake news & disinformation*. París, France: United Nations Educational, Scientific and Cultural Organization. Disponible en https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf

UNESCO (s.f.). "El patrimonio digital". Disponible en https://es.unesco.org/themes/information-preservation/digital-heritage

Villoro, L. (2016). *La significación del silencio y otros ensayos*. México: Fondo de Cultura Económica.

Xiangyu, L., Qiuyang, L. y Chandel, S. (12-14 de octubre de 2017). "Social Engineering and Insider Threats". En *Proceedings*

of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. Nanjing, China, pp. 25-34.

TECNOLOGÍA,
DERECHO Y CONFLICTOS

Bibiana Beatriz Luz Clara*

* Profesora e investigadora de la Universidad FASTA; Presidenta del Instituto de Derecho Informático del Colegio de Abogados de Mar del Plata.

PALABRAS CLAVE *KEYWORDS*

Tecnología	*Technology*
Derechos	*Rights*
Riesgos	*Risks*

Resumen. La tecnología ha impactado fuertemente en nuestra sociedad, modificándola y creando nuevos procesos disruptivos que traen aparejados cambios profundos también en la forma de relacionarse en lo social y comercial, entre otros ámbitos, que requiere del derecho un análisis para su adecuación y tutela efectiva frente a las nuevas situaciones conflictivas y delictivas que, facilitadas por las nuevas tecnologías, pueden producirse. En este articulo analizaremos algunos posibles riesgos y la necesidad de tomar conciencia y acciones para la protección y solución.

Abstract. Technology has strongly impacted our society modifying it and creating new disruptive processes that bring about profound changes also in the way of relating socially and commercially, among others subjects, which requires an analysis from the Law for its adequacy and effective protection against new conflictive and criminal situations that, faciliatated by new technologies, can occur. In this article we will analyze some possible risks, and the need to take awareness and actions for protection and solution.

SUMARIO:

I. INTRODUCCIÓN

Los procesos de cambio en nuestra sociedad permiten comparar la evolución de las personas en el espacio y tiempo y su actitud frente a los nuevos desafíos. En el caso de la sociedad actual, frente a las tecnologías de la información y las comunicaciones, que se encuentran transformando vertiginosamente el mundo, en comparación a como era conocido hace algunos años.

Según indicaba el filósofo Javier Echeverría,[2] se reconocen tres entornos: el primero es el de la naturaleza, en el que transcurre la sociedad rural agraria basada en el trabajo del campo (*physis*), donde los tiempos son los de las estaciones y, por ende, se trata de tiempos largos; el segundo es el entorno de la ciudad (*polis*), de la industria y del mercado, donde los tiempos ya se aceleran y se fabrica en masa; y el tercer entorno es el electrónico, el espacio de la sociedad de la información, que se superpone a los dos anteriores y coexiste con ellos, aquí el poder económico lo tienen quienes manejan la conectividad y las redes.

Los elementos de este tercer entorno son muy diferentes a todo lo anteriormente conocido, ya que la distancia entre las personas se vuelve irrelevante, se confluye en las redes y requiere adaptación a este nuevo espacio para quienes no son nativos digitales.[3] Esto debido a que estos últimos están rodeados desde la más temprana edad por las tecnologías[4] de información y las telecomunicaciones, lo que los mantiene familiarizados con habilidades tecnológicas desconocidas a esa edad por las generaciones anteriores. El lenguaje digital se vuelve su segundo lenguaje.

[1] Acrónimo proveniente del inglés: *Internet of Things*.

[2] En su conferencia del 17/01/2001 en Málaga, "Sociedad y nuevas tecnologías en el siglo XXI".

[3] Término acuñado y divulgado por Marck Prensky en su libro *Inmigrantes digitales* (2001) para indicar a los niños nacidos desde 1990 en adelante, para quienes utilizar los elementos tecnológicos es muy sencillo, a diferencia del resto de las personas que tienen que aprender y esforzarse.

[4] Videocámaras, celulares, computadoras, tabletas, videojuegos, etcétera.

II. INICIO DE UNA NUEVA ETAPA: EL ENTORNO ELECTRÓNICO

Este nuevo escenario fue propiciado por la aparición de internet,[5] que permite nuevos tipos de comunicación mediante el acceso a redes, y por el cual se pueden desarrollar actividades comerciales, educacionales, médicas, laborales, de gobierno, entre otras.

El entorno electrónico es un espacio internacional y eminentemente visual. Es más complejo que la propia internet, donde se hacen nuevas relaciones, basadas en intereses comunes, y que impacta en la estructura económica y social.[6] Su inmediatez y velocidad permiten que las personas estén conectadas a amplias redes de contactos en tiempo real, de acuerdo con afinidades.

Estas comunidades crecen virtualmente y en forma constante. Es un ambiente multicultural y electrónico, en el que se generan, como en cualquier otro, situaciones conflictivas, que muchas veces no se sabe cómo atender o no se encuentran las personas idóneas para gestionarlas eficientemente, pero lo importante, que debemos tener en la mira, es tratar de lograr un ambiente de paz para las relaciones virtuales.

También la dinámica comercial ha cambiado desde que es posible hacer compras y otras operaciones en línea. Aquí uno de los mayores inconvenientes es el problema de la deslocalización y el acceso a la justicia, marcado por la falta de información y conocimiento de los usuarios, los altos costos a enfrentar ante una demanda que debe hacerse en ajena jurisdicción, sobre todo cuando el monto de la reclamación es pequeño. Ante estas dificultades es posible que dichas personas decidan no hacer nada, quedando de este modo sus derechos vulnerados sin la correspondiente reparación.

[5] Los orígenes de internet se remontan a finales de los años sesenta (1969). En plena Guerra Fría, un proyecto de investigación en redes de conmutación de paquetes, dentro del ámbito militar (ARPA) desarrolló una tecnología de conmutación de paquetes, cuya principal característica reside en fragmentar la información, dividirla en porciones de una determinada longitud, llamados paquetes. Cada uno de ellos lleva asociada una cabecera con datos referentes al destino, origen, códigos de comprobación, etcétera. El paquete contiene información suficiente como para dirigirse a su destino. El camino a seguir no se encuentra preestablecido, así, si una parte de la red cae o es destruida, el flujo de paquetes será automáticamente desviado a otros nodos alternativos.

[6] La Organización para la Cooperación y el Desarrollo Económico (OCDE) ha trabajado —desde comienzos de este siglo— con el Grupo de Trabajo de Indicadores de la Sociedad de la Información (WPIIS, por sus siglas en inglés) para controlar las estadísticas de dichos indicadores, mediante cuestionarios modelo en hogares, empresas y gobiernos sobre el uso y aplicaciones de las TIC.

III. CONFLICTOS EN EL ENTORNO ELECTRÓNICO Y MEDIOS PARA RESOLVERLOS

Los métodos de resolución de disputas en línea (ODR)[7] aparecen aquí como una opción que puede aportar grandes beneficios, sobre todo cuando de relaciones de consumo se trata. Estas modalidades comerciales van en avance, y por ello es necesario dar respuesta rápida a sus necesidades por medio de mecanismos de resolución extrajudicial que complementen al sistema tradicional de administración de justicia, por su flexibilidad y pertenencia al medio electrónico, y permitan a los usuarios resolver sus conflictos en el mismo medio en el que se produjo el conflicto y con las herramientas electrónicas necesarias, reduciendo con ello los costos de la tramitación.

Los métodos ODR aprovechan la experiencia de los ADR[8] y le suman todas las posibilidades que brinda la tecnología para solucionar los conflictos que en el entorno electrónico se produzcan de modo ágil, y aun en otras situaciones que, habiéndose suscitado en el trato presencial, deciden optar por ellos para su resolución por las ventajas que implican, siendo los métodos principales:

- La negociación: aquí las partes actúan personalmente en la búsqueda de una solución al conflicto mediante sistemas que están automatizados y donde la comunicación puede ser sincrónica o asincrónica.[9] Se utilizan programas que facilitan la comunicación, identifican las posibles alternativas de solución y arman los acuerdos, emulando las funciones de un tercero neutral. Se utiliza mayormente para determinar los valores económicos en discusión. El éxito de estos sistemas depende de la naturaleza del conflicto, la precisión de la información que se suministra y la capacidad del *software* utilizado. La negociación puede ser totalmente automatizada[10] o negociación asistida,[11] según se tenga o no intervención humana en la negociación.

[7] *Online Dispute Resolution*: el término ODR es producto de las ciencias de la computación, donde se utiliza *on line*, que proviene del siglo pasado y es usado para hacer referencia al algoritmo que procesa sus entradas (*input*) de forma secuencial a medida que las recibe. Hace alusión a un servicio que se brinda a medida que se está produciendo una actividad. En su inicio los ODR eran métodos ADR conducidos *on line*, pero con el tiempo y el avance tecnológico fueron demostrando capacidades propias superadoras.

[8] ADR es el acrónimo inglés de *Alternative Dispute Resolution*. Se trata de los sistemas alternativos de resolución de conflictos, tales como el arbitraje, la mediación y la conciliación.

[9] Según sea que las partes estén en línea en el mismo momento, o no.

[10] *Fully automated negotiation.*

[11] *On line assited negotiation.*

- La mediación: es un método donde un tercero neutral, el mediador, mediante sus técnicas, ayuda a las partes a recuperar el diálogo perdido o a mejorar su comunicación, a fin de que encuentren por ellas mismas alternativas de acuerdo al conflicto. Se desarrolla mediante las herramientas electrónicas en línea. Las partes se comunican con la ayuda del mediador, ya sea en forma sincrónica o asincrónica. En la mediación concurrente, cuando varias personas interactúan en línea, la comunicación debe ser sincrónica. En cambio, cuando no se requiere la presencia, la comunicación puede ser asincrónica.

- El arbitraje en línea: es un método extrajudicial de resolver conflictos por el cual las partes, mediante su libre voluntad expresada en un acuerdo en tal sentido,[12] confían a un tercero la solución de sus controversias, atribuyéndole autoridad para emitir una resolución.[13] El tercero neutral es generalmente un experto en la materia requerida, que inspira la confianza de las partes por sus conocimientos y experiencia.

  El arbitraje es vinculante y podrá solicitarse el auxilio de la fuerza pública para lograr la ejecución del laudo, en el caso de que el obligado no cumpla, ya que los árbitros carecen de *imperium*.

Asimismo, en este entorno existen otros mecanismos de estímulo al cumplimiento de lo acordado entre las partes de modo voluntario. Estos son:

- Los sistemas de puntuación y reputación: estos son los que están basados en las opiniones que indican los clientes una vez que han utilizado el servicio y que les permite calificarlos según su satisfacción, opiniones a las que el público puede acceder y le permiten una mejor toma de decisiones.

- Sellos de confianza: donde se exhiben etiquetas de calidad que acreditan el cumplimiento de ciertos estándares.

- Los reembolsos, o chargeback: que permiten recuperar la suma pagada cuando las expectativas que tuvieron durante la transacción se han visto frustradas, especialmente cuando el pago ha sido realizado con tarjeta de o pasarelas de pago, a quienes se les solicitará la retención de lo pagado.

[12] La cláusula arbitral o cláusula compromisoria que las partes deciden insertar en los contratos para acudir al arbitraje en caso de conflicto.

[13] El laudo arbitral.

- Las cuentas de garantía: el dinero es entregado al comerciante cuando el cliente ha recibido el producto de conformidad, mientras tanto permanece depositado en una cuenta de un tercero al efecto.

- La suspensión del acceso: en este caso, se le suspende por su inconducta el acceso al sitio como usuario en el que se encontraba registrado o era miembro.

- Las *black lists*: son listas de comerciantes de riesgo para los usuarios, que se forman con los incumplidores y sirven para prevenir al público.

Todos estos sistemas son complementarios y ayudan a la desjudicialización, pero no impiden que el usuario haga uso de las acciones ante los tribunales si lo considera necesario.

Debemos agregar, además, a los *smart contracts*[14] o contratos inteligentes, que son negocios jurídicos programados gracias a las posibilidades que brinda el internet de las cosas (loT).[15] Se trata de programas en la nube que siempre actúan del mismo modo y permiten guardar información que no puede ser modificada. El *software* autorizará y corroborará que el contrato sea válido y registrará la operación de modo transparente en un registro contable digital que no podrá luego ser modificado, lo cual ayuda a la transparencia de las transacciones y ahorra costos. Utilizan *blockchain*[16] para garantizar que nadie podrá modificar las condiciones contractuales. En este caso, es el mismo protocolo de confianza del código el que hace cumplir las pautas programadas a ambas partes. Al encontrarse escritos en lenguajes de programación, no están sujetos a interpretación, con lo cual se evitan discusiones y diferencias.

El programa siempre actuará de la misma forma sin depender de la voluntad de un tercero. Asimismo, permite incorporar métodos ODR que integran a un sistema de verificación autónoma de las obligaciones que asumieron las partes, así como mecanismos de ejecución de las consecuencias indicadas en

[14] Se trata de un programa de *scripts* modulares que reproduce los acuerdos y las reglas pactadas y también las consecuencias de los incumplimientos.

[15] Interconexión de objetos de uso cotidiano. Se interconectan objetos heterogéneos a través de diferentes redes y métodos de comunicación, posicionando dispositivos que proveen información y realizan acciones en forma autónoma. Este ecosistema tiene tres partes: aplicaciones, *software* y sensores. Siempre por los sensores recibiremos la información, por eso deben ser especialmente cuidados, y cada día aumentan las aplicaciones para las distintas áreas.

[16] Cadena de bloques: es una estructura de datos en la que la información contenida se agrupa en conjuntos (bloques) a los que se añade metainformaciones relativas a otro bloque de la cadena anterior en una línea temporal, de manera que, gracias a técnicas criptográficas, la información contenida en un bloque solo puede ser repudiada o editada modificando todos los bloques posteriores, y en esto se basa su seguridad.

el contrato. Mediante este tipo de contrato se pueden cerrar de modo automatizado transacciones electrónicas y reclamaciones.

Como vemos, todas estas herramientas ágiles presentan una visión transformadora de la realidad social y comercial, por ello es preciso entender el paradigma de desarrollo actual y aplicar, por tanto, las nuevas tecnologías como mecanismo que facilite el acceso a la justicia, fomentando la dignidad e igualdad de las personas en un acceso más equitativo que el uso de tales herramientas puede propiciar.

Podremos cumplir, así, con el objetivo número 16 de los Objetivos de Desarrollo Sustentable (ODS) de las Naciones Unidas, que indica: "Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y crear instituciones eficaces, responsables e inclusivas a todos los niveles" (ONU, 2015), base de la sostenibilidad económica, social y ambiental de los 193 estados miembros firmantes.

Para que dichas políticas tengan éxito se requiere de alianzas entre los gobiernos, el sector privado y la sociedad civil, construidas sobre principios y valores comunes y metas compartidas de la agenda para el desarrollo.

IV. INTERNET DE LAS COSAS (IOT),[17] RIESGOS Y ACCIONES DE PROTECCIÓN

Otro de los fenómenos frente al cual nos encontramos es la interconexión de objetos heterogéneos de uso cotidiano a través de diferentes redes y métodos de comunicación, posicionando dispositivos que proveen información y realizan acciones en forma autónoma. La IoT lo conecta todo. Vivimos en un mundo hiperconectado que se potenciará aún más cada día.

Este ecosistema tiene tres partes: aplicaciones, *software* y sensores. Es por medio de los sensores que recibimos la información, por eso deben ser especialmente cuidados, ya que progresivamente aumentan las aplicaciones para las distintas áreas.

Las tendencias de mercado confluyen hacia la IoT desde la irrupción de IPV,[6] por lo cual se deben tener reglas claras para mantener la estabilidad de internet, pues cuantos más dispositivos conectados encontremos más riesgos a considerar:

- La interconexión entre dispositivos de alta y baja seguridad conforma un ambiente vulnerable, que puede facilitar los accesos indebidos, por lo cual se deberá contar con algoritmos

[17] Acrónimo proveniente del inglés: *Internet of Things*.

criptográficos y gestión de claves adecuadas.

- La privacidad de los datos obtenidos, sobre todo en los aspectos más sensibles, tanto los que genera el usuario como los que se brindan a terceros[18] o los que adquiere el sistema de modo automático. Será necesario concientizar a todos los actores del sistema para el resguardo adecuado de dicha información.

- Debida identificación de la identidad de cada objeto conectado y su función para circunscribir la acción de cada uno de ellos al contexto y usuario correspondiente y así poder definir los mecanismos de seguridad apropiados.

- Definir la confianza en la IoT en un entorno dinámico y colaborativo entre todos los componentes vinculados. Los usuarios deben confiar en el uso adecuado de los dispositivos conectados, con un marco legal respaldatorio.

- Todos los objetos deberían: i) ser seguros por sí mismos en cuanto al *hardware* y al *software*; ii) conocer el estado de la red y sus servicios; iii) poder defenderse contra ataques de intrusos y fallas.

La economía mundial se realiza en forma electrónica, por ello es fundamental considerar las distintas amenazas al sistema, dada la cantidad de dinero que fluye en este entorno y los nuevos negocios que generan.

Debemos prevenir el robo de la información y su acceso de forma ilegal, comprometida o atacada, poniendo en riesgo a la comunidad, y mantener indemnes sus derechos.

Por ello, es necesario realizar el análisis de los métodos preventivos, dado el impacto económico y social que pueden implicar, de acuerdo con los siguientes criterios:

- Tipo de acción: interceptación, sabotaje, robo de datos, denegación de servicios

- Tipo de perpetrador: quien está cometiendo las acciones: hackers, terroristas, gobiernos, delincuentes, revolucionarios.

- Tipo de objetivo: hacia donde o quien se quiere atacar, por ejemplo, sociedad civil, organizaciones, empresas, medios de comunicación, unidades militares, infraestructuras críticas, etcétera.

[18] Datos de geolocalización, claves de acceso, números de teléfonos, de tarjetas de crédito, entre otros.

Es necesario evitar que la cantidad de personas afectadas se multiplique, ya que las amenazas son múltiples: *malwere* (software malicioso); *ramsomwere* (para tomar control de los datos por un precio); *botnets* (redes o dispositivos secuestrados que realizan acciones sin conocimiento de sus usuarios); denegación de servicios (para demostrar que se puede tomar control de los sistemas o para obtener ganancias); *phishing* (mediante ingeniería social se obtiene información de las personas a quienes se engaña para que realicen algo).

Las categorías de ciberseguridad que deben considerarse para ver cómo se pueden proteger los usuarios son: i) *Link* o enlace; ii) Infraestructura de telecomunicación; iii) Seguridad de internet (ISP, rutas, nombres de dominio, comunicación misma, elementos de hardware); iv) Seguridad de los procesadores; v) Aplicaciones; vi) Seguridad de los datos; vii) Comprobación de identidad de usuarios; viii) Seguridad de los servicios esenciales.

Los posibles problemas de seguridad pueden provenir de:

- Usuario travieso: cuando accede al dispositivo, de manera desprevenida para el fabricante, e ingresa a utilidades limitadas del producto.
- Fabricante inmoral: el productor del dispositivo usa y explota las tecnologías para revelar información del usuario a extraños.
- Agresor externo: conocido también como "entidad ajena" porque no forma parte de la red de la IoT y no tiene autorización para acceder, aun así, intenta obtener información confidencial y puede causar el mal funcionamiento de las entidades con IoT.
- Programación deficiente: el desarrollador de software para la aplicación IoT o los dispositivos IoT, pueden escribir códigos no seguros que permitan reconocer los datos del usuario.

Las fuentes de amenazas pueden ser utilizadas como vía de acceso para vulnerar los sistemas de seguridad digital del usuario, estableciendo situaciones de extorsión, robo, secuestro u otros delitos informáticos. Las áreas que más pueden verse afectadas por la IoT son la privacidad y la seguridad de las personas.

Se debe tener cuenta la alta escalabilidad de los ataques. Debido a que los sistemas IoT utilizan la red de redes para la comunicación y desde un punto cualquiera de la red, el ataque se difunde rápidamente hacia nuevas conexiones de puntos no atacados inicialmente.

Todos los componentes conectados a internet están expuestos a la intrusión indebida.

Existen, por lo tanto, algunos desafíos en este ecosistema de responsabilidades donde cada uno tiene un importante papel: realizadores de aplicaciones, operadores de plataformas, desarrolladores que no se toman el tiempo para considerar las implicancias de sus creaciones. Todos debemos involucrarnos para esta regulación, incluidos los usuarios, que tenemos el poder de decidir qué queremos y qué no. En este sentido, deben regularse las exigencias mínimas para que el uso de IoT sea seguro,[19] sobre todo para quien lo utiliza.

V. CONCLUSIÓN

Advertimos que el entorno electrónico es el espacio que se encuentra atrayendo la mayor parte de actividades de nuestra sociedad digital. Que es un espacio nuevo, dinámico y visual en el que pueden ocurrir distintos tipos de conductas, algunas que generan conflictos que deben resolver rápidamente para evitar que escalen y mantener las relaciones pacíficas, y para ello existen mecanismos ODR y otros ágiles y alternativos lo favorecen. Pero por la irrupción de las tecnologías vinculadas al uso de IoT, se pueden generar también situaciones de riesgo y conductas delictivas que deben ser perseguidas y fijar reglas claras para minimizar los riesgos a los que se enfrenta toda una sociedad conectada y vulnerable. Esto requerirá el esfuerzo conjunto de los países, mediante la conformación de espacios de trabajo interdisciplinarios, para fijar pautas comunes en cuanto a las normas técnicas y legales, y perseguir determinadas acciones dañosas, pero sin perder de vista que, si se regula demasiado, Internet puede perder su naturaleza libre, ya que lo que necesitamos es que sea abierta, y segura para todos

[19] La Online Trust Alliance (OTA), desde 2004, desarrolla estándares de seguridad, analiza las buenas prácticas, el futuro programa de certificación de IoT: abordaje de amenazas y vulnerabilidades, y reporta los incidentes ocurridos.

VI. FUENTES DE CONSULTA

Alzate Sáez de Heredia, R. y Vásquez de Castro, E. (2013). *Resolución de disputas en línea*. España: Ed. Reus.

Betancourt, D., Gómez, G. y Rodríguez J. (2016). "Introducción a la internet de las cosas", En *Revista Tecnogestión. Una Mirada al Ambiente*, 3(1). Disponible en: https://revistas.udistrital.edu.co/index.php/tecges/article/view/12132. Consultado el 31 de agosto de 2019.

Osepa, S. (14 de junio de 2019). "Conferencia IoT y Políticas Públicas". Internet Society.

Ebner, N. y Zeleznikow, J. (2015). "Fairness, trust and Security in Online Dispute Resolution". En *Journal of Public Law and Policy*, 36(2). Disponible en http://digitalcommons.hamline.edu/jplp/vol36/iss2/6

Echeverria, J. (1999). *Los señores del aire*. Barcelona: Ediciones Destino.

Vilalta Nicuesa, A. (2013). *Mediación y arbitraje electrónicos*. España: Ed. Aranzadi.

LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO: CAMBIOS EVOLUTIVOS A 10 AÑOS DE SU INCLUSIÓN A NIVEL CONSTITUCIONAL

Mario Anselmo Gómez Sánchez*

* Fundador de DataProtección. Socio de GYE Abogados.

PALABRAS CLAVE *KEYWORDS*

Datos personales	*Personal information*
Derechos ARCO	*ARCO´s rigths*
Vida privada	*Private life*

Resumen. El presente artículo tiene como objetivo principal describir los cambios legislativos e institucionales que ha puesto en marcha el Estado mexicano a partir del reconocimiento a nivel constitucional de los derechos de acceso, rectificación, cancelación u oposición (ARCO) sobre el tratamiento de datos personales. Esto, con la finalidad de reflexionar acerca de los principales logros y tareas pendientes para la protección de los datos personales en México.

Abstract. The main objetive of this article is to describe the legislative and institutional changes that the Mexican State based on recognition at the constitutional level of the rights of access, rectification, cancellation or opposition (ARCO) on the processing of personal data. This, with the goal to reflect on the main achievements and pending tasks for the protection of personal data in Mexico.

Los datos personales se definen como cualquier información que refiera a una persona identificada o identificable. Hacen alusión a múltiples aspectos de la vida privada, como su nombre, número telefónico, correo electrónico, entre otros. A aquellos que estan relacionados con la esfera más íntima del titular se les conoce como datos personales sensibles, como los referentes al origen étnico, creencias religiosas, preferencia sexual, financieros y demás. Los datos personales no dependen del medio que se utilice para captarlos, almacenarlos, utilizarlos o comunicarlos.

En este sentido, el derecho a la protección de datos personales tiene como principal objetivo garantizar a cualquier persona el poder de decisión y control que tiene sobre la información que le involucra; es decir, sobre la forma en que se utilizan y el destino de sus datos personales. Así, quien es titular de sus datos personales cuenta con múltiples facultades que le posibilitan el control de los mismos. Entre estas se encuentran los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) (INAI, s.f.: 4).

El derecho a la protección de datos personales tiene su sustento en el derecho a la privacidad. Derivado de esto, ha estado presente en múltiples instrumentos legislativos a lo largo de la historia del derecho mexicano. Uno de sus antecedentes más remotos se encuentra en la Ley de Imprenta de 1917, cuyo artículo 1° regulaba los ataques a la vida privada. O en el artículo 16 de la Constitución de 1917, en el que se contempla la protección a la privacidad al establecer que nadie puede ser molestado en su persona, familia o domicilio. A nivel internacional, el derecho a la privacidad se consagró como derecho fundamental al establecerse en el artículo 12 de la Declaración Universal de los Derechos del Hombre. En este, se indica que las personas tienen derecho a no ser "objeto de injerencias en su vida privada y familiar, su domicilio o su correspondencia, ni de ataques a su honra o reputación". Disposiciones similares se encuentran en la Convención para la Protección de los Derechos y Libertades Fundamentales, el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana sobre Derechos Humanos.

Fue hasta 1970 que surgió en Alemania la primera ley de protección de datos personales como dimensión específica del derecho a la privacidad. Para 1980, la Organización de Cooperación y Desarrollo Económico estableció las Directrices Relativas a la Protección de la Intimidad y de la Circulación Transfronteriza de Datos Personales, con el objetivo de unificar las

legislaciones nacionales. Un año después, surgió el Convenio 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal. Como se observa, desde su surgimiento han aparecido múltiples instrumentos normativos con la finalidad de garantizar el derecho a la protección de datos personales.

En México, la protección de datos personales no fue un tema de discusión durante las últimas décadas del siglo XX. No obstante, a partir del año 2000, con la alternancia política del titular del Poder Ejecutivo federal, se manifestó la demanda social por legislar sobre acceso a la información y transparencia. Así, en julio de 2002, se publicó la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (LFTAIPG). Esta norma tuvo como como finalidad regular el acceso a la información pública y garantizar la protección de datos personales en posesión de los sujetos obligados (LFTAIPG, 2002: art. 4).

De forma específica, el tema de protección de datos se contemplaba en los artículos dedicados a establecer los límites del derecho de acceso. Entre estos, se encontraba la hipótesis normativa que indicaba que se consideraba información confidencial a aquellos datos personales que requirieran el consentimiento de los individuos para su difusión, distribución o comercialización (LFTAIPG, 2002: cap. III).Posteriormente, en 2005, el entonces Instituto Federal de Acceso a la Información (IFAI) publicó los Lineamientos de Protección de Datos Personales (2005). Estos tenían por objeto instaurar las políticas generales y procedimientos que tenían que cumplir las dependencias federales para garantizar a las personas la facultad de decisión acerca del uso y destino de sus datos personales. Derivado de ello, un año después, se publicaron las *Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales* (2006), con la finalidad de fortalecer el marco normativo ya establecido. En 2007, se incorporó por primera vez a la Constitución federal la referencia al derecho a la protección de datos personales, como regulador del ejercicio de acceso a la información. Así, el artículo 6° estableció los principios y bases que rigen el ejercicio del derecho de acceso a la información. Entre estos se menciona que "La información que se refiere a la vida privada y los datos personales será protegida en los términos y condiciones que fijen las leyes…" (CPEUM, 2007: art. 6). No obstante los avances revisados, la mayor reforma en materia de protección de datos personales aconteció el 1 de junio de 2009. En

dicha fecha, se publicó en el *Diario Oficial de la Federación* un decreto por medio del cual se adicionaba un segundo párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. El nuevo texto constitucional establecía que:

> 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 de orden público, seguridad y salud públicas o para proteger los derechos de terceros. (CPEUM, 2009: art. 16)

De acuerdo con la exposición de motivos de la reforma en comento, la inclusión de este párrafo implica el reconocimiento del Estado del derecho a la protección de datos personales y los correlativos derechos ARCO. Asimismo, supone la creación de obligaciones en torno al manejo de los mismos a toda entidad o persona pública o privada que cuente con acceso o disponga de los datos personales de los individuos. La inclusión de este derecho a nivel constitucional amplía su aplicación para todos los niveles y sectores gubernamentales.

Es importante mencionar que unos meses antes de la adición del segundo párrafo al artículo 16 constitucional, se publicó el decreto por el que se adicionó la fracción XXIX-O al artículo 73 de la Constitución federal (2009), el cual establece que el Congreso de la Unión tiene facultad "para legislar en materia de protección de datos personales en posesión de particulares".

Adicionalmente a las disposiciones revisadas, el texto constitucional contiene múltiples referencias a la protección de datos personales. Por ejemplo, el artículo 20, apartado C, fracción V, establece reglas dedicadas a normar el tratamiento de datos personales de víctimas y ofendidos en el procedimiento penal. Por su parte, los artículos 26, apartado B; 73, fracción VIII; o el 109, fracción IV, contienen obligaciones del Estado relacionadas con el derecho a la protección de datos personales, específicamente, derivadas de la creación del Sistema Nacional de Información Estadística y Geográfica, el registro público sobre deuda pública y la investigación y sanción de responsabilidades administrativas y hechos de corrupción, respectivamente (CPEUM, 2009).

No obstante lo anterior, la normatividad en materia de protección de datos personales que existía en 2009 para el sector público no garantizaba de forma plena los derechos ARCO y, además, existían grandes vacíos legales en lo que respecta al sector privado. Para solucionar la problemática anterior, los

legisladores federales aprobaron, en abril de 2010, el decreto mediante el cual se expidió la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP).

Esta norma fue publicada por el Ejecutivo federal en julio del mismo año, y tiene por objeto "la protección de los datos personales en posesión de los particulares, con la finalidad de regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas" (LFPDPPP, 2010: art. 1).

Esta norma va más allá de los derechos reconocidos por el segundo párrafo del artículo 16 constitucional, puesto que no se limita a los derechos ARCO, sino que los concibe en términos amplios: como un conjunto de prerrogativas que pertenecen al derecho a la autodeterminación informativa de las personas. Adicionalmente, su artículo 6 indica que los responsables del tratamiento de datos personales deberán cumplir con determinados principios para la protección de datos personales. Estos son: licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.

Asimismo, posterior a la reforma de la constitución federal, diversas entidades federativas modificaron su normatividad para incluir disposiciones que garantizaran el derecho a la protección de datos personales. Algunas hicieron cambios en sus leyes de transparencia y acceso a la información e incluyeron capítulos especiales sobre protección de datos, mientras que otras crearon leyes específicas sobre la materia, como sería el caso de Tlaxcala o Durango (SCJN, 2019).

Siguiendo con las adecuaciones institucionales, producto de la inclusión del segundo párrafo del artículo 16 constitucional, y en consideración de las posteriores reformas que se realizaron en materia de transparencia y acceso a la información, en 2014 surgieron diversas iniciativas para crear una nueva Ley General de Transparencia y Acceso a la Información Pública (LGTAIP). Posterior a los procesos de discusión y aprobación, dicha norma fue promulgada en 2015. Una de las incidencias más importantes que tuvo en materia de protección de datos personales fue la transformación del IFAI al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) (SCJN, 2019). Este cambio tuvo como consecuencia el fortalecimiento de los mecanismos del instituto dedicados a garantizar el derecho a la protección de datos.

Otro de los cambios legislativos más importantes se dio apenas

hace dos años. Con la colaboración del INAI, y en aras de atender las lagunas que existían en materia de protección de datos en posesión de entes públicos, en 2017 se publicó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO). Esta norma tiene como objeto "establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona a la protección de sus datos personales, en posesión de sujetos obligados" (LGPDPPSO, 2017: art. 1).

Se considera que esta norma terminó de armonizar la normativa de protección de datos. Su carácter de ley general implica que los sujetos obligados por las disposiciones podrán pertenecer al ámbito federal, estatal o municipal, y serán cualquier órgano, entidad, autoridad u organismos de los poderes ejecutivo, legislativo y judicial u órganos autónomos, partidos políticos, fideicomisos y fondos públicos (LGPDPPSO, 2017: art. 1).

Las normas mencionadas tienen relación directa con la protección de datos personales. Adicionalmente, desde el cambio constitucional de 2009, han sido reformadas o publicadas múltiples normas secundarias que contemplan entre sus disposiciones el derecho a la protección de datos personales. Entre las más destacadas se encuentran: la Ley para la Transparencia y Ordenamiento de los Servicios Financieros (2018: art. 23 Bis), que contiene disposiciones que prohíben a las instituciones financieras compartir datos de sus clientes sin su autorización; la Ley Federal de Protección al Consumidor (1992: art. 76 Bis 1), en la que se prevé la obligación a quien comercialice, ofrezca o venda bienes de contar con mecanismos técnicos de seguridad apropiados que garanticen la protección y confidencialidad de la información personal; o la Ley para Regular las Instituciones de Tecnología Financiera (2018; art. 76), que establece que los datos agregados que manejen dichas instituciones no podrán contener un nivel de desagregación tal que puedan identificarse los datos personales de una persona.

Adicionalmente, se han realizado avances en materia de normas oficiales mexicanas. Para 2010, se promulgó la Norma Oficial Mexicana NOM-024-SSA3-2010, que establece los objetivos y funcionalidades que deberán observar los productos de sistemas de expediente clínico electrónico. Entre otros aspectos, se regulan aspectos como la autentificación de datos, el control de acceso a ellos, el intercambio seguro, la confidencialidad del paciente, la interoperabilidad de los sistemas estatales nacionales, entre otros.

También se han realizado avances en materia jurisdiccional. En 2014 el pleno de la Suprema Corte de Justicia de la Nación resolvió la contradicción de tesis 56/2011 y emitió la tesis aislada P.II/2014 (10a.), en la cual afirmó que las personas morales tienen derecho a la protección de los datos que puedan equipararse a los personales, a pesar de que dicha información haya sido entregada a una autoridad. Esto, debido a que las personas colectivas cuentan con espacios de protección ante cualquier intromisión arbitraria por parte de terceros respecto de cualquier información que, de ser revelada, pudiera anular o dañar su libre y buen desarrollo.

A nivel internacional, los dos instrumentos de los que el Estado mexicano forma parte y que prevén de forma explícita el derecho a la protección de datos personales son el Convenio 108 del Consejo de Europa y el Tratado de Libre Comercio de México, Estados Unidos y Canadá (T-MEC). Con lo anterior, México cuenta con disposiciones para garantizar, entre otros aspectos, los flujos transfronterizos de datos entre algunos de los países más importantes del mundo.

A partir de las consideraciones anteriores es posible advertir que el derecho a la protección de datos personales está presente en múltiples ámbitos de la vida de las personas y de la actividad estatal. Derivado de ello, las responsabilidades del Estado son diversas, dependiendo de la materia de la que se trate. La legislación de áreas como las responsabilidades administrativas, la fiscalización de recursos públicos, el registro de deuda pública, las telecomunicaciones, entre otros, también se ve afectada. Por tanto, se hace necesaria su adaptación para que, en la medida de sus respectivos ámbitos y consecuencias, garanticen el derecho a la protección de datos personales.

Con lo anterior se pone en relieve las diversas acciones que el Estado mexicano ha realizado con la finalidad de garantizar el derecho a la protección de datos personales en el país. En sí, estas acciones son un logro en la materia e, incluso, han sido reconocidas a nivel internacional. Apenas en 2018, la invitación de México para adherirse al Convenio 108 del Consejo de Europa se hizo en reconocimiento de la importancia que el Gobierno le ha otorgado en los últimos años a la defensa del derecho a la protección de datos y al hecho de que el INAI es considerada la autoridad de protección de datos más activa de Latinoamérica (Bojalil, Egan y Vela-Treviño, 2019).

Las leyes en la materia contienen gran variedad de derechos, temas e instrumentos que permiten

hacer más efectiva la protección de datos. Por ejemplo, la LFPDPPP (2010) contempla aspectos como la transferencia de datos; las autoridades que deben promover, regular y garantizar la protección de datos; los procedimientos de protección de derechos, de verificaciones y de imposición de sanciones; entre otros. Por su parte, la LGPDPPSO (2017) contiene disposiciones dedicadas a normar el Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos; la portabilidad de los datos; la relación entre el responsable y encargado; la comunicación de datos personales; y demás.

Adicionalmente, el INAI ha realizado múltiples acciones con el mismo propósito. Por ejemplo, cuenta con instrumentos interactivos como generadores de avisos de privacidad; el registro de esquemas de autorregulación vinculante; el vulnerómetro; IFAI Prodatos; o el evaluador de vulneraciones. Asimismo, brinda información sobre procedimientos para ejercer los derechos ARCO y para la presentación de denuncias, en el sector público y en el privado. Incluso, para facilitar estos últimos aspectos, ha creado formatos, como el Formato de Solicitud de Derechos ARCO o el Formato de Declaración y Ratificación de Datos (INAI, 2019).

También, cuenta con múltiples documentos para facilitar el cumplimiento de las normas de protección de datos, entre los que se encuentran: la *Guía de esquemas de autorregulación en materia de protección de datos personales*, la *Guía para el tratamiento de datos biométricos*, el *Estudio sobre sistemas de datos personales*, las *Recomendaciones para el manejo de incidentes de seguridad de datos personales*, entre otros.

México ha tenido grandes avances en materia de protección de datos personales; sin embargo, este derecho es poco conocido en la sociedad en general, lo que ha generado que sea poco exigido.

En México, muchas empresas no saben cómo implementar las normas de protección de datos personales, cumpliendo en algunos casos únicamente con el aviso de privacidad, desconociendo que este último documento debe ser el reflejo del cumplimiento de los principios establecidos en la norma, más allá del aviso de privacidad se deben documentar las acciones tomadas en el interior de la empresa para proteger los datos personales.

Asimismo, es importante realizar modificaciones legislativas a aquellas normas que no han sido revisadas en muchos años. La relación cercana del derecho a la protección de datos con la tecnología implica que la legislación sobre la materia

se examine y analice de forma recurrente. Esto, con la finalidad de que no quede obsoleta ante los constantes avances y cambios de los medios digitales. El segundo párrafo del artículo 16 constitucional no ha sido reformado desde su inclusión; normas como la LFPDPPP o la LGPDPPSO no se han actualizado desde que fueron publicadas; otras leyes, que retoman el tema de forma tangencial, como la LGTAIP o la Ley de Firma Electrónica Avanzada, tampoco han sido reformadas en los últimos años.

En relación con este último punto, también es necesario que las normas se adapten a las legislaciones internacionales más avanzadas. Si bien México ratificó en 2018 el Convenio 108 del Consejo de Europa, aún no ha realizado lo mismo con el Convenio 108+, el cual es una revisión y actualización de las disposiciones del primero. También, se considera importante la implementación o fortalecimiento de nuevos y mejores modelos de mediación, tanto a nivel nacional como internacional, a través de los cuales se hagan más efectivos los sistemas de protección de datos personales.

En temas más específicos, es importante la determinación de forma clara de los delitos y penas aplicables en violaciones al derecho a la protección de datos. También, la regulación debería perfeccionarse en aspectos como la previsión del consentimiento tácito y las consecuencias que este puede tener en materia de protección de datos. Además, deben realizarse avances en aspectos como portabilidad de los datos personales y desarrollar estrategias más efectivas que permitan proteger los datos personales que se ubican en plataformas digitales.

Como se advierte, a diez años de la inclusión del derecho a la protección de datos personales en el texto constitucional, México ha creado una normativa muy completa en la materia, con la finalidad de garantizar que todo sujeto pueda tener control de sus datos personales. Asimismo, ha creado instituciones sólidas como el INAI y gran cantidad de mecanismos que permiten a las personas el ejercicio de sus derechos ARCO.

Si bien el derecho a la protección de datos personales ha sido objeto de discusión y regulación desde hace décadas, la llegada en los últimos años de los medios tecnológicos y su incidencia en diversos ámbitos de la vida privada, pública, económica y social han reavivado el debate y el interés de los Estados por contar con mecanismos que garanticen de la forma más efectiva dicho derecho. Esto deriva del aumento en los sistemas de procesamiento, almacenamiento y transmisión de

datos personales y, al mismo tiempo, del incremento y surgimiento de amenazas a la privacidad.

Es claro el interés del Estado mexicano de contar con mejores instrumentos que permitan proteger la privacidad e intimidad de las personas; sin embargo, aún quedan múltiples acciones por hacer. La protección de datos sigue siendo un tema novedoso, que se encuentra en construcción y cambio constante, que requiere la revisión recurrente de las leyes en la materia y una mayor difusión, de tal manera que cualquier individuo cuente con el conocimiento necesario para hacer exigible este derecho.

I. FUENTES DE CONSULTA

Constitución Política de los Estados Unidos Mexicanos (5 de febrero de 1917). *Diario Oficial de la Federación*. Texto original.

Secretaría de Gobernación (2009). Decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos. *Diario Oficial de la Federación*. 30 de abril de 2009. México.

Secretaría de Gobernación (2007). Decreto por el que se adiciona un segundo párrafo con siete fracciones al Artículo 6° de la Constitución Política de los Estados Unidos Mexicanos. *Diario Oficial de la Federación*. 20 de julio de 2007. México.

Secretaría de Gobernación (2009). Decreto por el que se adiciona un segundo párrafo, recorriéndose los subsecuentes en su orden, al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. *Diario Oficial de la Federación*. 1 de junio de 2009, México.

INAI (s.f.). *Guía práctica para la atención de las solicitudes de ejercicio de los Derechos ARCO*. México. Disponible en http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pdf

INAI (2019). *Protección de Datos Personales*, 2019. Disponible en http://inicio.ifai.org.mx/SitePages/ifai.aspx

Ley de Imprenta (1917). *Diario Oficial de la Federación*. 12 de abril de 1917. México. Ley Abrogada.

Ley de Transparencia y Ordenamiento de los Servicios Financieros (2018). *Diario Oficial de la Federación.* 9 de marzo de 2018. México. Texto vigente.

Ley Federal de Protección al Consumidor (1992). *Diario Oficial de la Federación.* 24 de diciembre de 1992. México. Texto vigente.

Ley Federal de Protección de Datos Personales en Posesión de los Particulares (2010). *Diario Oficial*

de la Federación. 5 de julio de 2010. México. Texto vigente.

Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (2002). *Diario Oficial de la Federación*. 11 de junio de 2002. México. Ley Abrogada.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017). *Diario Oficial de la Federación*. 26 de enero de 2017. Texto vigente. México.

Ley para Regular las Instituciones de Tecnología Financiera (2018). *Diario Oficial de la Federación*. 9 de marzo de 2018. México. Texto vigente.

Lineamientos de Protección de Datos Personales (2005). *Diario Oficial de la Federación*. 30 de septiembre de 2005. México.

NORMA Oficial Mexicana NOM-024-SSA3-2010 (2010). *Diario Oficial de la Federación*. 8 de septiembre de 2010. México.

Bojalil, P., Egan, M. y Vela-Treviño, C. (2019). "Despuntan las reformas en materia de protección de datos en América Latina". En *Open Knowledge*, 2019. Disponible en *https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/*

Recomendaciones sobre medidas de seguridad aplicables a los sistemas de datos personales (2006). Acuerdo ACT/23/08/ 2006.03.03 del pleno del IFAI. 23 de agosto de 2006. México.

Suprema Corte de Justicia de la Nación (2019). *Exposición de motivos de la Ley de Transparencia y Acceso a la Información Pública*. Sistema de Consulta de ordenamientos, México. Disponible en *http://legislacion.scjn.gob.mx/Buscador/Paginas/wfProcesoLegislativoCompleto.aspx?q=s6n2if7Uv7A+Z8I-0w3ky6Rz2YfI3eWRDqk8+RRS/H4sEKSiI1+n0/nX/ujRFy1kRYe5Xrw/Q9eCMue2wogwjfA==*

Suprema Corte de Justicia de la Nación (2019). *Sistema de Consulta de Ordenamientos Jurídicos. Normatividad Estatal*. Disponible en *http://legislacion.scjn.gob.mx/Buscador/Paginas/Buscar.aspx?q=+xTvGEY+kZRl6RpM/aixVA==*

Tesis P.II/2014 (10a.). *Gaceta del Seminario Judicial de la Federación*. Décima Época, Libro 3, t. I. Febrero de 2014, p. 274.

RETOS EN LA PROCURACIÓN Y ADMINISTRACIÓN DE JUSTICIA

CONVERTIR UNA DEBILIDAD EN FORTALEZA. PRIMERAS EXPERIENCIAS ACUMULADAS*

Damián Paret Francia**

* Autorizado por el gobierno cubano para su publicación sin modificaciones.

** Experto en nuevas tecnologías. Cuba.

PALABRAS CLAVE *KEYWORDS*

Riesgos tecnológicos	*Technology Risks*
Wifi en Cuba	*Wifi in Cuba*
Servicios cubanos	*Cuban Services*

Resumen. Este trabajo tiene como objetivo principal ilustrar a la población cubana, usuaria de los servicios públicos de redes wifi, de los peligros potenciales que comienzan a enfrentar en las condiciones del desarrollo tecnológico de nuestro país.

A partir de la experiencia acumulada nos atrevemos a sugerir propuestas relacionadas con los usuarios que comienzan a recibir el servicio de internet en sus casas, así como sus efectos para que estén preparados ante los nuevos riesgos que pueden enfrentar.

Es importante para la familia cubana, en especial para los jóvenes, conocer los potenciales peligros que el uso de internet puede ocasionar, más aún, cuando nuestra legislación no está lo suficientemente preparada para responder a tales situaciones y exigencias, como tampoco quienes deben aplicarla.

Abstract. The main objective of this work is to illustrate the Cuban people user of public services of Wi-Fi networks, of the potential dangers that begin to face in the conditions of technological development of our country.

From the accumulated experience we dare to suggest proposals related to the users starting to receive internet service in their homes, as well as its effects so that they are prepared for new risks they can face.

It is important for the Cuban family, especially for young people, to know the potential dangers that the use of the internet can cause, furthermore, when our legislation is not sufficiently prepared it gives to respond to such situations and demands, as well as who should apply it.

SUMARIO:

I. INTRODUCCIÓN

Hasta hace poco el acceso a internet en Cuba estaba concentrado fundamentalmente en el sector estatal, fuera de ese sector, el número de personas que podían acceder a esta poderosa herramienta era menor.

Al decir herramienta, me hace pensar en un martillo tan útil y necesario que en algunos momentos puede salvarte y mal utilizado puede golpearte. Creo que ese término me ayuda muy bien a definir el tema que pretendo tratar.

No es difícil imaginar que en sociedades donde se estimula al consumismo tecnológico, es posible acceder a equipos como computadoras, tablets, laptops, móviles, entre otros, que permitan, junto a servicios con precios muy competitivos, un acceso pleno a internet, donde el límite y los permisos solo los pone usted con su bolsillo y conocimiento.

¡Conocimiento!, algo de lo que se carece en este tipo de sociedad donde se aprenden duramente los riesgos que conlleva una internet rápida, abierta y desconocida. En muchos casos los padres trabajan duro para tener estos servicios y equipos antes mencionados, para que sus hijos aprendan y no carezcan de internet, ¡herramienta al fin!, muy útil para estudiar. No se nos ocurriría darle un martillo a un niño o niña de 8 años y dejarle solo, ¡pero el internet sí! ¿Qué mal puede implicar dejar a sus hijos conectados buscando un trabajo escolar?, ¿o al chat con un amigo de la escuela o familiar? ¡Pero sí!, existe el riesgo, es real.

Para cualquier ciudadano cubano pensar en los riesgos de una internet es algo irrelevante. Por un lado, las velocidades a las que estábamos acostumbrados eran de 28 a 48 kbps, con una conexión conmutada, si navegar por una página nos llevaba todo un día, nadie piensa que un *hacker* se interesaría en nosotros, sería una tortura para él. Por otro lado, no pagamos con tarjetas de crédito por esta vía; el riesgo mayor está con qué tipo de personas nos relacionamos, y que información hacemos pública, incluso poniéndola como privada.

En estos tiempos donde los ya conocedores de la internet plena piensan en la seguridad de su información, en defender su privacidad a toda costa de los *hackers* y gobiernos de turno. Donde ya se hace una moda tapar las cámaras frontales de cada dispositivo, por miedo a ser

vistos, aun con el equipo apagado. Todo eso me hace preguntarme, ¿por dónde estamos nosotros? Y me atrevería a responder, más atrás, en la parte de "¡yo quiero la internet!", te la cambio por toda mi información personal, ….¡después veremos!

Para quien sí conoce los riesgos, se asustaría al escuchar algo así, como cuando ves a alguien firmar un documento sin leer. Téngase en cuenta que la palabra firmar en estos temas tecnológicos tiene el mismo significado que presionar un botón si estás de acuerdo con los términos que *debiste leer*.

II. DESARROLLO

A. HISTORIA

Para quienes no conocen mucho Cuba, tal vez en mi introducción les hice pensar que estamos en la edad de piedra con las computadoras, y ¡no es así!, ¡no seremos de los primeros, pero para nada de los últimos!

Lo que sucede es que lo que más abunda en mi país son las entidades estatales, instituciones docentes, de salud, y de manera especial los llamados "Joven Club de Computación y Electrónica", ya con 30 años de creados, que constituyen un proyecto social con el objetivo de acercar las computadoras a la familia sin costo alguno —al menos hasta el 2015— según la Oficina Nacional de Estadística e Información (ONEI, 2016).

Tanto a las escuelas, universidades o Joven Clubs, le fueron entregadas sus computadoras por parte del gobierno, pero solo muchos años después pudieron ofrecer las bondades de la internet. También vale mencionar que, aunque con menos años de creados, existen otros sitios como "Las Salas de Navegación" o también llamadas "Salas Nauta", este último nombre por el servicio de correo internacional y luego de internet, con carácter comercial que comenzó a ser la opción más individual o personalizada al alcance de los que pudieran pagar por él, pero ya desde las casas o desde el móvil.

B. ACTUALIDAD DE LOS SERVICIOS

¿Pero qué está pasando ahora mismo en Cuba?, pues como parte de las mejoras que se están realizando, se han creado puntos wifi, principalmente en zonas donde hay parques y donde las personas pueden conectarse con sus dispositivos portátiles. Para los visitantes a la isla —que solo están de pasada— esto luce como algo muy loco, pues todos se esparcen por doquier, sentados tanto en bancos, pisos o aceras; pero al igual que los cubanos terminan integrándose también al sistema de la

navegación en tales sitios, porque para ellos es menos costoso que el servicio que se brinda en algunos hoteles, donde la hora se llegó a cotizar a 5 CUC (equivalente a 5 dólares) cuando en los sitios públicos estuvo a 2 CUC y a una velocidad a veces superior. Cabe señalar que estos precios han seguido mejorando hasta no menos de la mitad.

Y toda esta ola de personas nada cómodas, pero bien concentradas ¿para qué?, pues para meterse en la gran locura que son las redes sociales: revisar correo, navegar por la internet o hacer video conferencias con familiares y amigos que se encuentran en la distancia y, así, buscar un mayor acercamiento.

C. PRIMEROS GOLPES RECIBIDOS

¡Sabemos que todo lo que comienza implica nuevos riesgos! Aunque inicialmente se hicieron experimentos en algunas zonas de pruebas y después de varios estudios, una vez que se tomó la decisión para habilitar estos servicios de Internet de forma más personal a los clientes, aparecen nuevos personajes en nuestra vida social, utilizando las brechas de seguridad de estos servicios. Y quiero llamar la atención en uno muy específico: el uso de *hotspot* clandestinos.

Para hacerlo más claro intentaré ejemplificarlo: una persona se conecta a un *access point* oficial perteneciente a la red wifi de Etecsa (nuestro proveedor nacional de internet), pagando por este servicio, una vez dentro de internet habilita la opción de compartirla con otros. Si lo hiciera gratis no creo que hiciera mal a nadie más que a él mismo, ya que su internet sería mucho más lento y solo paga él. Pero no es así, esas personas que, curiosamente muchos de ellos apenas sabían cómo encender una computadora hasta hace poco, ahora comienzan aprendiendo de forma casi automática cómo ganar dinero, utilizando herramientas y tomando las notas precisas para ello, distribuyendo el mismo servicio por menos dinero a varias personas. Este ejemplo que expongo tiene riesgos que el usuario decide tomar para abaratar costos, pero hay otros en que se es víctima de un ciberdelito sin saberlo.

¡Les explico!, usted busca la red wifi oficial, imaginemos un nombre "WiFi_Alfin", y le aparece tal vez con más fuerza en la señal una de nombre similar "WiFi-Alfin", creo que la diferencia les puede parecer ahora muy evidente a ustedes, pero no para las víctimas que han llegado al lugar público con mucha dificultad, logrando encontrar un espacio lo más privado que se lo permita el momento, y la primera información

que su mente recibe al buscar la conexión es "¡Vaya! qué fuerte esta la señal aquí". Rápidamente se les carga en su equipo una página idéntica a la oficial que les pide poner su usuario y contraseña. Este suertudo usuario ingresa los datos que le brinda la tarjeta que compró para este fin y, sin duda, logra su objetivo, finalmente se conecta a internet, qué… ¿pensaron que no? pues sí se conecta, digamos que consume de una hora que le brinda su tarjeta solo 5 minutos, únicamente quería checar si le llegó el correo esperado.

¿Dónde está el problema entonces?, que en su siguiente intento de conexión en una red oficial, al intentar entrar, le notifica la web que su usuario está en uso o que ya se consumió todo el crédito. Les estoy hablando solo del consumo de una tarjeta con una hora de conexión, y no de una cuenta nauta de conexión a internet que puede tener un crédito de 10 o 20 CUC, por poner una cifra relativamente baja solo para internet. ¿Se imaginan?

¿Cómo fue eso?, pues estos estafadores modernos, ya no tan novatos, montan una especie de puente entre la conexión falsificada y la conexión oficial, se quedan con sus datos de conexión y utilizan su tiempo restante tal vez para ofertárselos a otros de una manera más económica, también pueden suplantar su IP, lo cual es utilizado en el caso del uso de las cuentas con crédito (Nauta).

D. CÓMO ENFRENTAR EL DESCONOCIMIENTO

El término más utilizado cuando trabajamos en la internet es el de "navegar", como si de estar en un bote o barco se tratase, navegando por un mar de información. Es por ello que para evitar ser víctimas de piratas o no quedarnos a la deriva, ¡al menos no por el desconocimiento!, propondría que se otorgue una licencia al solicitar un servicio de internet en las casas, dicha licencia puede ser otorgada automáticamente a personas que tengan una carrera técnica o universitaria donde se les enseñe sobre el uso y los riesgos de la internet. !A los que no¡, se les puede brindar un curso de entrenamiento; los tópicos a tratar pudieran ser: la terminología o palabras utilizadas, las herramientas de navegación, los antivirus nacionales e internacionales, también los sitios web, entre ellos los buscadores, foros y blogs más importantes y, por supuesto, los riesgos a que nos enfrentamos según la experiencia internacional.

Vale mencionar que nosotros en Cuba tenemos dos canales de televisión conocidos como "canales educativos" donde se dan algunas de

las asignaturas que reciben los estudiantes que cursan el nivel preuniversitario, también cursos de inglés y otros idiomas. A estos programas, ¡que ya el hecho de tenerlos es un lujo!, no pueden faltar estas clases de preparación informática bien ilustradas y algo importante a destacar es el horario de transmisión, para asegurarnos que se cumpla el objetivo de informar a la familia. La utilización de los medios de comunicación —cuales sean— es fundamental.

E. CAUSAS QUE ESTIMULAN EL EXCESO DE TIEMPO EN LA INTERNET EN LOS JÓVENES

De las causas generales que quiero mencionar, les diré qué tanto pueden afectarnos hoy a nosotros los cubanos.

¡Qué mejor excusa para un estudiante de cualquier edad que los trabajos escolares!, estos pueden ser resueltos por esta vía. En nuestro caso ya sea el trabajo de los padres, tiempo de maquina en las universidades o un joven club de los ya mencionados son de las opciones más comunes.

O nuestro cuidado con los hijos advirtiéndoles tanto de la calle y sus peligros, que concluyen ¡mejor si se está en casa! Solo una minoría pudiera tener esta preocupación en la isla, ya sea por lo caro o difícil que resulta tener aún este servicio, como por los peligros que suele tener un joven normal, no somos un país peligroso.

Que decir de los juegos online; al comienzo pensamos que ese era un gran problema, después nos dimos cuenta que no, ¡era solo el comienzo! ¿Adictos a los juegos?, sin duda tenemos, ¿cómo lo hacen?, estoy seguro que contarles es tan interesante como para hablar de ello en un próximo trabajo, por lo pronto les puedo adelantar que jugar conectados directo a la internet solo una minoría y no creo que sea pagándola.

Y si se trata de acercarse a todos aquellos que están lejos sin importar fronteras, el tiempo se nos va ¡a riesgo de alejar a los que tenemos cerca! No luce nada agradable ver en una cena familiar a parte de la familia chateando. Sin duda, me atrevo a decir que chatear y estar conectado a redes sociales es el mayor tiempo a lo que le dedican nuestros ciberusuarios, no visto aún como en otros países porque no suelen haber lugares que brindan servicios de comida o de otro tipo donde ofrezcan un internet gratis, y ¿si! aún es caro para el cubano promedio y los lugares con internet no son muchos, así que ahora tenemos nuevas tendencias de salir con amigos a lugares bonitos cercanos, a donde

puedan conectarse a la wifi y divertirse al menos una hora *online* y bien acompañados.

No podemos dejar de mencionar el término ciberadictos, que bien podemos utilizar cuando ya caen en la trampa de algunas aplicaciones como Snapchat, por mencionar solo una, donde se estimulan con chispas las publicaciones y se pierden cuando se deja de usar, ¡todo un gancho! Estas personas no pueden hacer una acción aun dentro de casa sin dejar de publicarla. ¿Qué se come o se bebe?, ¿dónde se está? y ¿con quién? Con todo lo anterior expuesto de nuestra realidad creo que con ejemplos como este es cuando solo me atrevería, pensando como padre, a decir: ¡menos mal que no tengo internet en casa!

F. ALGUNAS EXPERIENCIAS CON JÓVENES

En una entrevista realizada a una joven *alemana* de 15 años, ella comentó de sus experiencias en la internet, al igual que sus compañeros de aula. Cuenta que las aplicaciones más utilizadas por ella y sus colegas, entre las que se encuentran: Instagram, Snapchat, Whats app, Tik Tok, HouseParty, WattPad, Matthew, YouTube, ASKfm y si de juego se trata los varones juegan Fortnite juntos. Después de tantos nombres, la mayoría desconocidos para mí, ¡debe ser porque ya me alejé de los 15!, me puse a investigar de qué se trataban:

Si la moda es lo que les preocupa aplicaciones como *21 Buttons*, *Stylemaker* e *Influencers* son su solución.

21 Buttons: permite estar al día de las últimas tendencias de moda, compartir estilos y comprar *online* las prendas etiquetadas por otros usuarios. Las ventas que genera cada usuario a través de las imágenes que comparte, dan lugar a una recompensa en forma de saldo que puede acumularse o reembolsarse en cualquier momento.

Wattpad*:* es una aplicación que permite compartir historias con otras personas. Se pueden publicar artículos, relatos, poemas, blogs, *fanfics*, ciencia ficción e historias sobre temas diversos, ya sea en línea o a través de la aplicación.

Matthew*:* esta aplicación puede escanear la tarea matemáticas del usuario y se le enviará la forma de cálculo y la respuesta. Resuelve problemas matemáticos instantáneamente desde la aritmética hasta el cálculo. Escanea problemas matemáticos impresos o escritos a mano para obtener soluciones al instante pero por pasos.

Houseparty: esta aplicación permite participar en una videollamada grupal, con un máximo de ocho participantes, muy usada por los

jóvenes. En el caso de la entrevistada me cuenta que cuando ve películas de interés entre sus amigos desde sus casas utilizan esta aplicación y es como estar todos en el mismo lugar comentando y haciendo bromas entre sí.

Snapchat: ¿Qué es y cómo funciona?, ¡seguro que lo saben mejor que yo!, considerado por muchos como una fiebre entre los jóvenes para estar comunicados.

Para mí, saber que esta joven en su perfil nuevo de Snapchat (¡no sé qué le pasó con el anterior!), mando 76 mil fotos en un año y tiene entre 50 y 100 mil chispas acumuladas, ¡me deja sin palabras! Que las chispas son por persona y la puntuación más alta con una persona es de 100. ¡Aun creo que no lo logro entender! Una de sus preocupaciones era que si en 24 horas no mandaba una foto, podía perder sus chispas. ¡Hasta yo comencé a preocuparme!, ¿seguro que en las escuelas los profesores les dan clases a estudiantes y no a dispositivos?, ¿les dará tiempo para bañarse sin el móvil?, ¡confío en que lo hagan!.

Después de conocer qué tanto hacían los jóvenes de países más distantes, llegó el momento esperado, entrevistar a los míos; ver si me estaría perdiendo de algo. En esta ocasión, entrevisté a un chico de 18 años, que junto a dos de sus amigos de la misma edad, me cuenta del uso que le dan a internet.

Su uso principal, la comunicación con amigos y familiares tanto dentro como fuera del país, buscar información relacionada con sus gustos y trabajos de escuela, bajar aplicaciones que sean útiles y funcionales sin internet, y estar al tanto de cual aplicación es la que sirve para burlar la seguridad y tener internet gratis, ¡demasiado sano todo, hasta que llegamos a ese punto!

De las aplicaciones más utilizadas y tal vez menos conocidas por ustedes, se encuentran:

Imo: Esta aplicación es todo un éxito en la isla por su fácil uso para realizar videollamadas y enviar mensajes. Funciona como otras tal vez más populares internacionalmente como Whatsapp, pero Imo es la que pego.

Zapya: programa que también hemos hecho como propio, se utiliza para bajar aplicaciones, pero como más la utilizamos es sin internet, para compartir archivos entre móviles, tablets y computadoras, utilizando una conexión wifi entre ellos, incluso entre dispositivos con sistema Android e IOS.

El resto, CubaMessenger, 9Apps, InstaSave, VidMate, un poco más de lo mismo, no quiero aburrirlos con nuestra tienda de aplicaciones más usadas.

III. CONCLUSIONES

Podemos concluir que no somos ni seremos infalibles a los riesgos que trae consigo el avance tecnológico, pero si podemos aprender de los errores ya cometidos, algunos vistos en la experiencia internacional; somos humanos, somos jóvenes y existen tendencias a repetir lo mismo.

En cuanto a la sanción penal posible ante hechos delictivos, el Código Penal cubano no prevé aún los delitos informáticos, dentro de los cuales están los delitos con el uso de medios informáticos y el ciberdelito, por lo cual habría que aplicar tipos delictivos relacionados con *la actividad económica ilícita*, *la estafa*, *la apropiación indebida* y, en su caso, hacer una interpretación del hecho para su adecuación.

Actividad económica ilícita:
"ARTICULO 228.1.- (Modificado). El que, con ánimo de lucro, realice cualquiera de las actividades de producción, transformación o venta de mercancías o prestación de servicios de las autorizadas legal o reglamentariamente sin poseer la licencia correspondiente; o realice alguna actividad de esa naturaleza no autorizada en forma expresa por disposición legal o reglamentaria, incurre en sanción de privación de libertad de tres meses a un año o multa de cien a trescientas cuotas o ambas.

Estafa:
"ARTICULO 334.1.- El que, con el propósito de obtener para sí o para otro, una ventaja o un beneficio patrimonial ilegítimo, y empleando cualquier ardid o engaño que induzca a error a la víctima, determine a éste a realizar o abstenerse de realizar un acto en detrimento de sus bienes o de los de un tercero, incurre en sanción de privación de libertad de tres meses a un año o multa de cien a trescientas cuotas o ambas."

Apropiación indebida:
"ARTICULO 335.1.- El que, con el propósito de obtener una ventaja o un beneficio patrimonial ilegítimo para sí o para otro, se apropie o consienta que otro se apropie de bienes que le hayan sido confiados, incurre en sanción de privación de libertad de tres meses a un año o multa de cien a trescientas cuotas o ambas".

Nuestra legislación no está aún lo suficientemente preparada para responder a tales situaciones y exigencias, como tampoco quienes deben aplicarla. Aun así, no quedan impunes estos hechos si son apresados infraganti, pero al momento tendría que usarse una figura delictiva diferente para la aplicación de una sanción penal conjunta que pudiese ser en un comisor primario, la multa y la confiscación de los instrumentos

usados para cometer el delito y ante la reincidencia, podría agravarse la pena.

Aún tenemos obstáculos que vencer para progresar ante el feroz avance tecnológico de estos tiempos, pero al menos contamos con especialistas de primera línea, tanto en escuelas de nivel técnico en informática, como en la Universidad de Ciencias Informáticas (UCI) entre otras destacadas, donde sus conocimientos les han permitido clasificar múltiples veces para participar en eventos internacionales como son: la Competición Internacional Universitaria de Programación (en inglés International Collegiate Programming Contest, abreviado ACM-ICPC o solo ICPC) uno de los torneos más importantes internacionalmente en esta área, cuyos resultados han estado por encima de universidades del primer mundo.

El recién electo presidente de los Consejos de Estado y de Ministros de Cuba, Miguel Manuel Diaz-Canel Bermúdez, ante un debate el pasado año sobre la Política Integral para el Perfeccionamiento de la Informatización de la Sociedad en Cuba, en su intervención mencionó:

> tenemos que defender que Internet, las redes sociales, nuestras plataformas informáticas de desarrollo de servicios y aplicaciones, estén orientadas a la gestión del conocimiento. Y que los cubanos puedan usar Internet para aumentar sus saberes, elevar su cultura general integral, enriquecer sus valores espirituales. (Díaz, 2017).

Estas palabras solo confirman la voluntad política de nuestro gobierno de procurar cada vez más el acceso a la internet. Por nuestra parte, si hacemos de las vulnerabilidades y debilidades identificadas una fortaleza, ¡la espera habrá valido la pena!

IV. FUENTES DE CONSULTA

Androidapk. "Mathew". Disponible en http://androidapk-s.com/app/1337066244/mathew, consultado el 20 de abril de 2018.

Código Penal. *Gaceta Oficial de la República de Cuba*. Disponible en https://www.gacetaoficial.gob.cu/html/codigo_penal.html#A10, consultado el 10 de julio de 2018.

Cubadebate (14 de julio de 2017). "Díaz-Canel: Orientar la Internet en Cuba a la gestión del conocimiento". Revista digital *Cubahora*. Disponible en http://www.cubahora.cu/sociedad/diaz-canel-orientar-la-Internet-en-cuba-a-la-gestion-del-conocimiento, consultado el 19 de abril de 2018.

Hernández Barrios, M. A. (6 de junio de 2017). "Los muchachos que marcaron la historia". En Mesa Redonda. Disponible en http://mesaredonda.cubadebate.cu/

mesa-redonda/2017/06/07/acm-icpc-los-muchachos-que-marcaron-la-historia-video/, consultado el 20 de abril de 2018.

López López, C., Cabrera López, O. L. (12 de julio de 2017). "Los Joven Club de Computación y Electrónica en Cuba: un programa único en el mundo". En *Revista Tino*, (56). Disponible en https://revista.jovenclub.cu/los-joven-club-de-computacion-y-electronica-en-cuba-un-programa-unico-en-el-mundo/

Oficina Nacional de Estadística e Información (ONEI) (2016). *Anuario estadístico de Cuba 2016*. Disponible en http://www.one.cu/aec2016/17%20Tecnologias%20de%20la%20Informacion.pdf, consultado el 19 de abril de 2018.

Redacción (29 de marzo de 2016). "21 Buttons, cuando los usuarios son los mejores prescriptores". En Pinker Moda. Disponible en https://pinkermoda.com/21-buttons-una-app-moda/, consultado el 19 de abril de 2918.

Wikipedia. "Wattpad". Disponible en https://es.wikipedia.org/wiki/Wattpad, consultado el 20 de abril de 2018.

Taubaso, D. (23 de mayo de 2017). "Qué es Houseparty, la app que Facebook tiene en la mira". En *Clarín*. Disponible en https://www.clarin.com/tecnologia/apps/houseparty-app-facebook-mira_0_H1kK0T-ZW.html, consultado el 20 de abril de 2018.

Zabala, M. "ASK.fm, la red social de moda entre los adolescentes". En iWomanish. Disponible en: https://www.iwomanish.com/ask-fm-la-red-social-de-moda-entre-los-adolescentes/, consultado el 21 de abril de 2018.

CONCIENTIZACIÓN, MÉXICO Y LA CIBERGUERRA

Carlos Ramírez Castañeda*

* Creador de contenido de la especialidad de Derecho Informático UNADM SEP en temas de ciberseguridad; catedrático de diplomados, cursos y clases dentro de varias universidades de México.

PALABRAS CLAVE *KEYWORDS*

Ciberguerra	*Cyberwar*
Riesgos digitales	*Digital risks*
Cyberseguridad	*Cybersecurity*

Resumen. La carencia de concientización sobre riesgos digitales ha traído consigo una serie de peligros mayores que, hoy en día, dan paso a ser utilizados como armas digitales al alcance de cualquier persona con el conocimiento técnico suficiente. La necesidad de tener un control sobre poblaciones y gobiernos nos ha llevado a un punto de evolución en el cual la guerra ahora se convierte en una ciberguerra; la utilización de *malware*, los ataques a infraestructuras críticas, los vacíos legales y la carencia de una cultura digital apegada a los peligros más allá de un ciberdelito pueden resultar en consecuencias devastadoras. Cuando migramos de un ataque digital a uno con repercusiones tangibles en el mundo físico es donde debemos tener un punto de partida sobre las prospectivas y escenarios que requieren atención más allá de los asuntos políticos del país.

Abstract. The lack of awareness of digital risks has brought a number of major dangers, which today give way to being used as digital weapons available to anyone with sufficient technical knowledge. The need to have control over the populations and governments, has taken us to a point of evolution in which the war now becomes a cyber war; the use of malware, attacks on critical infrastructure, legal gaps and the lack of a digital culture attached to the dangers beyond cybercrime, can result in devastating consequences. When we migrate from a digital attack to one with tangible repercussions in the physical world, its where we must have a starting point on the perspectives and challenges that require attention beyond the political affairs of the country.

SUMARIO:

I. INTRODUCCIÓN

Vivimos en una sociedad dependiente de la tecnología, la cual evoluciona día a día; hemos trasladado nuestra identidad física a un espacio intangible, al espacio digital. Diariamente, alimentamos nuestros perfiles con contenidos multimedia, información a veces sensible, creyendo que está resguardada en un sitio seguro; sin embargo, cuando existe un factor disruptivo a toda la cadena de la ciberseguridad y migramos a un escenario de control y amenazas digitales mayores, no solamente contra el usuario o sistemas, sino contra una población en general o un país completo, estamos ante un escenario de ciberguerra, en el cual nadie está a salvo de las amenazas digitales que se potencian a diario.

Nos encontramos en un escenario donde los riesgos son latentes, donde el nuevo campo de guerra se ha convertido en el ciberespacio. México —ante el panorama previamente mencionado— queda en el limbo y propenso a mayores ciberataques: la ciberguerra es inminente. En este sentido, es importante conocer un poco más acerca de los puntos de afectación que podrían poner en shock a México; sin políticas públicas es necesario conocer el panorama técnico para dar una correcta atención legal.

II. CIBERGUERRA: CONTEXTO GENERAL

La industria de la guerra —a lo largo de la historia— ha sido un medio económico para potencializar naciones. El hecho de estar a la vanguardia en la industria armamentista con los avances, en cuanto a tecnología de punta para los conflictos bélicos, es una necesidad para el resguardo de varios países en el mundo. Con la llegada del internet y la revolución de las TIC, la guerra ha tomado un camino distinto, ya no se trata de causar bajas enemigas para dominar el territorio, se trata de tomar el control de los activos digitales del país antagónico para tener un control certero más allá de la parte militar: ejercer un control social, político e incluso mediático.

El control del ahora conocido como "quinto dominio" es un entorno clave para la seguridad nacional y la ciberdefensa de las naciones. La ciberguerra es una realidad inminente de la que sin ser actores directos somos participes día con día,

pues como usuarios de internet no escapamos de los riesgos ante los que nos podemos ver inmersos en este nuevo conflicto.

La llegada de nuevas herramientas digitales ha potencializado los alcances y rangos de impacto de muchas de las ciberamenazas que en años anteriores habían estado bajo control, como el *ransomware*, cuyo incidente mayor dejó un precedente en el mundo físico en aquellos meses de abril y mayo en el 2017. La masificación de WannaCry[1] dejó en claro que los daños producidos de manera digital tienen repercusiones en el mundo material, pues la pérdida de muchas vidas humanas y la carencia de planes reactivos en algunas infraestructuras críticas, como lo fueron hospitales, es una muestra del poderío de una amenaza digital. Claro está que ante un mal manejo de este tipo de códigos fuente, como el del *ransomware*, un atacante potencial, con el conocimiento debido, podría modificar a su antojo e incluso hacerlo más nocivo. El contraste lo vemos hoy en día ante una implementación para frenar a gobiernos antagónicos con ataques dirigidos a sus sistemas de gestión y, particularmente, a las infraestructuras críticas que hacen girar la vida diaria de un país.

El control de un medio de comunicación, como un canal unilateral de consulta de información como lo es para muchas personas internet, simboliza un gran punto de fractura social para el dominio de una población. No hace falta amedrentar con armas de manera física, el valerse de ciberarmas para el control mediático es un punto para considerar en las filas de la ciberguerra y toda la armamentización digital necesaria para llevarlo a cabo.

El mejor ejemplo de este tipo de control lo podemos constatar en la forma en como los grupos terroristas reclutan nuevos adeptos. Para no ir tan lejos tenemos el caso del narco y la forma en como busca tener control y presencia en redes sociales, dejando en claro una imagen de poderío, riquezas y lujos, por los cuales es una buena causa sumarse a las filas del cártel. Cuanto mayor sea la actividad en las redes sociales, mayor será el nivel de capacidad de supervivencia de una organización criminal.

Si las organizaciones criminales en México presentan una alta actividad en las redes sociales, entonces deberían demostrar un mayor nivel de resistencia a los reveses organizacionales. La organización debería tomar menos tiempo para reanudar actividades ilegales, demostrando un nivel más alto de adaptabilidad e impacto mínimo en sus operaciones

[1] Avast, WannaCry, recuperado de https://www.avast.com/es-es/c-wannacry

cuando se elimina el liderazgo (García, 2018).

La ciberguerra toma un giro vertiginoso al dejar en claro el poderío de una organización criminal que puede atentar contra el Estado o, en su caso, operar a instancias del mismo, todo mediante la conectividad y respuesta de los usuarios por medio de las tic; una opinión puede verse tergiversada en un canal de comunicación creando consigo un punto nuevo para los usuarios que logren familiarizarse con esto. El peligro de la desinformación no solamente consiste en sumar personas a las organizaciones criminales del mundo, sino manipular la opinión de las masas.

La llegada de las noticias falsas o *fake news* trae consigo a la ciberguerra un punto más simple de apoyo; las trincheras del periodismo entre países hacen que la verificación de información se convierta en un reto.

Las transformaciones en la producción y distribución de la información que han introducido las nuevas tecnologías, en especial las redes sociales, han provocado una gran eclosión de fuentes informativas y que el flujo comunicativo sea constante, lo cual ha originado que los medios de comunicación dejen de ser la fuente primaria de las noticias y que se pierda parte del valor añadido que el periodista imprime a sus informaciones: la verificación y contextualización de estas (Alonso, 2019).

El Estado puede modificar las tendencias de muchas redes sociales con la ayuda de *bots*, esto es una realidad que hasta el día de hoy no ha tenido algún tipo de atención, salvo la incorporación de algoritmos por parte de las grandes casas que manejan las compañías de redes sociales. La implementación legal rígida para la atención de noticias falsas y afectaciones de usuarios tipo algoritmo es una necesidad, no hace falta esperar la integración de inteligencia artificial para el combate técnico de riesgos mediáticos, se necesita el parámetro legal para una respuesta cuerda a los futuros ciberincidentes que se desarrollarán a través de las plataformas de redes sociales con el fin de manipulación; la ciberguerra libra otro aspecto, como lo dijimos.

Después de tener un contexto superficial de la ciberguerra y el tipo de control social, entremos en detalles de las ciberamenazas que pueden ser usadas para cometer actos que sobrepasan un ciberdelito común, pues el riesgo y las afectaciones son mayores.

Para tener un control certero de toda actividad, particularmente de periodistas y funcionarios gubernamentales, el ciberespionaje privatizado contratado por instancias gubernamentales, usualmente de seguridad y/o procuración de

justicia, ofertan servicios para tener el control de un móvil, usualmente teléfonos inteligentes de uso común con RAT's (Remote Administration Tools), que permiten tener acceso a los contactos, mensajes, llamadas, escuchar en vivo, activar cámaras frontales y traseras, así como estar a la escucha de toda actividad y ruta trazada de la persona.

Casos sonados de empresas como NSO, DarkMatter, BlackCube, en 2019, pusieron en shock a varios funcionarios con casos de ciberespionaje en sus dispositivos. En este sentido, la privacidad pasa a ser un mito cuando en una ciberguerra interna el Estado planea tener control de toda actividad digital de las personas a su servicio.

Para el caso de gobierno a gobierno, el ciberespionaje utiliza técnicas de *phishing* e ingeniería social mejoradas y potencializadas, por las cuales se busca obtener información sensible, planes de guerra, defensa, etc. Aquí no se busca comprometer un solo dispositivo mediante *malware*, sino un conjunto de sistemas o varios usuarios que podrían tener acceso a este tipo de información altamente confidencial. La necesidad de políticas públicas de manera interna para cada una de las agencias de seguridad —y seguridad nacional— requieren una inminente contemplación del *malware* para ciberespionaje, así como el robustecimiento de medidas de control y accesos de los usuarios para reducir el impacto nocivo que un ataque dirigido podría traer.

El ciberespionaje ha tenido una evolución enorme al poder llevar a cabo ataques dirigidos a protocolos DNS, identificados por algunos CERT, el caso es una alerta temprana del INCIBE (2019).

Desde el Centro Nacional de Ciberseguridad e Integración de las Comunicaciones (NCCIC), parte de la Agencia de Ciberseguridad y Seguridad de Infraestructuras (CISA), se alerta sobre una campaña global de espionaje en la infraestructura de DNS. La información obtenida —gracias a esta campaña— podría permitir a los atacantes redirigir el tráfico hacia una infraestructura controlada por ellos y, de este modo, obtener certificados de las webs de las organizaciones pudiendo realizar ataques de *man-in-the-middle*. El NCCIC recomienda renovar las contraseñas de los registros DNS de las organizaciones, implementar un sistema multifactor de autenticación en las cuentas de dominio de los registradores, realizar auditorías de los registros DNS públicos, así como buscar certificados de cifrado relacionados con los dominios y revocar los certificados solicitados fraudulentamente (INCIBE, 2019).

El peligro puede ser mayor cuando hablamos de una pequeña línea que divide al ciberespionaje con el sabotaje digital. Para el caso, hablaremos de las infraestructuras críticas.

Las infraestructuras críticas son todas aquellas estructuras que, a pesar de un desastre natural o provocado, deben estar en funcionamiento 24/7, pues sus servicios son necesarios para que un país funcione con normalidad. Para el caso de México tenemos contemplación en la Estrategia Nacional de Seguridad (ENCS) de 2017, cuyo eje transversal contempla el establecimiento de políticas y acciones que se llevarán a cabo en el marco de la Ley de Seguridad Nacional, y demás instrumentos aplicables en materia de seguridad nacional y en colaboración con las instancias de seguridad nacional (Gobierno de México, 2017). Sin embargo, al hablar de políticas, pareciera que en cada cambio sexenal queda un proyecto en la ambigüedad, sin continuidad y sin adaptación a las necesidades actuales de una sociedad inmersa en el ciberespacio y la tecnología. Hasta el día de hoy, desafortunadamente, no existen pronunciamientos oficiales de actuación y continuidad de una ENCS, dejando a las infraestructuras críticas mexicanas en un punto abierto para ciberataques.

En la ciberguerra, si un acto interno de sabotaje se lleva a cabo sobre, el funcionamiento (retomando el ejemplo de WannaCry) de una IC que trabaje mediante sistemas digitales interconectados y de ello dependan vidas humanas, el resultado sería catastrófico, las consecuencias serían tangibles, a pesar de que el ataque fue de manera digital.

Dejar fuera de funcionamiento una IC mediante un ataque DDoS es una de las maneras más simples por las cuales la intermitencia de un servicio masivo puede verse afectada en cuestión de segundos. Está de sobra mencionar al *cybercrime as service* que a cargo de países antagonistas se podría producir un DDoS de incluso días. Las vulnerabilidades expuestas ante la parte técnica de atención son necesarias, junto con planes internos preventivos y reactivos ante ciberincidentes provocados.

Las IC necesitan formar parte de políticas públicas pues, al tener un acercamiento en pro de la concientización de los ciudadanos con un acervo mínimo de conocimiento digital, estos mismos harían algo para formar parte del ecosistema de cuidado a tan prioritarias unidades de servicios primordiales. Un caso a ejemplificar de carencias de cultura digital fue en Gatwick, dónde un *drone* ocasionó un problema en

el aeropuerto, poniendo en riesgo la vida de muchos usuarios.

Para prevenir incidentes de algo que podría resultar ser un objeto de esparcimiento y recreación, se hizo un pronunciamiento público por parte de las autoridades de Gatwick; el uso de drones está creciendo a un ritmo rápido en el Reino Unido y nuestros cielos son algunos de los más activos en cualquier parte del mundo. Los drones ahora están prohibidos dentro de los 5 km de Gatwick y todos los aeropuertos de Reino Unido. Es ilegal volarlos dentro de esta zona. Cualquier persona que vuele un avión no tripulado debe mantenerse alejado de aviones, aeropuertos y aeródromos. Hay una zona de restricción de vuelo de 5 km alrededor de Gatwick y es ilegal volar cualquier dron no autorizado dentro de esta área. Los drones no deben volar por encima de los 400 pies (aprox. 120 m) en ningún momento. Es un acto criminal romper la zona de exclusión aérea, y el operador podría poner vidas en peligro e ir a prisión por hasta cinco años (Gatwik, 2018). Lo mostrado es parte de políticas públicas para concientizar a la población y prevenir incidentes en sus IC, apegado a la legalidad de un nuevo peligro se adaptó para ser sancionado. El uso de drones en centrales aéreas, marítimas, de agua y electricidad podría causar pérdidas de vidas humanas; es por ello que, retomando el punto clave de concientización, la población usuaria debe estar al tanto de la importancia de las infraestructuras críticas y los daños que podrían provocar.

Ante un escenario incierto de construcciones mexicanas de nuevos puertos aéreos o mejoras a los existentes, la razón de tener contemplación de riesgos simples, que podrían provocar resultados fatales y complejos, hace que la regulación de drones comience desde las tiendas comerciales, pues los lineamientos existentes de la Secretaría de Comunicaciones y Trasportes (SCT, 2017) no son suficientes. Para el arte de la ciberguerra los drones modificados pueden ser los vehículos para cometer atentados terroristas, con un explosivo cargado y con posibilidad de ser detonado a distancia, se convierten en el medio perfecto para causar la pérdida de vidas humanas en todo sentido bélico. No hace falta voltear a Sudamérica con los hechos de atentados perpetrados con drones, sino pensar en prospectiva de los sitios y plazas públicas de México los cuales requieren atención para una correcta regulación sobre los mismos drones y, en el caso más pertinente, incorporar tecnología de *jamming* con cuerpos preparados para la inutilización del artefacto volador que podría convertirse en arma.

El peor de los escenarios para tener un avance y control sobre un Estado completo recaería en el daño de todas las infraestructuras críticas mediante ciberamenazas; pensemos en una central nuclear, el peligro que representa para las cercanías de una población, si esto es atacado por algún tipo de *malware* troyano para tomar el control, el o los artífices del ataque causarían un estallido, liberación de materiales tóxicos que, en consecuencia, provocarían decesos y heridos. La ciberguerra no necesita tanques o armas de grueso calibre, pues una infraestructura crítica puede jugar el papel de una bomba nuclear controlada a distancia sin exponer al atacante.

Las prospectivas planteadas son una realidad. Ya hay evidencia y ejemplos globales para poder ocuparnos, si bien es cierto que el cibercrimen es el negocio ilícito rentable de la actualidad, la industria de la ciberguerra moverá millones en los próximos años, el desarrollo de *malware* intrusivo, los daños a infraestructuras críticas, las denegaciones de servicios más prolongadas y en volúmenes mayores son un peligro latente, si lo sumamos a un impulso con la inteligencia artificial y redes venideras, como los estándares del 5G, tendremos sin duda ataques nunca antes vistos y de mayor impacto junto con la peligrosidad que representan no solamente para el control de un sistema o país, sino a la vida del usuario mismo.

III. CONCLUSIONES

Las carencias de políticas públicas en materia de ciberseguridad y el silencio a la actualización de una Estrategia Nacional de Ciberseguridad, ya cimentada y con buena participación de todos los niveles que la desarrollaron, es un punto vulnerable que requiere atención para estas nuevas amenazas digitales enunciadas a lo largo de este documento.

Los pronunciamientos por parte de la autoridad pertinente son necesarios para poder colaborar y seguir trabajando cada uno desde su propia trinchera, pues son temas que no pueden ser minorizados o dejados a la deriva, ya que la población usuaria de TIC crece día a día.

A nivel de seguridad nacional se entiende la confidencialidad de las autoridades para mantener información a resguardo; sin embargo, el ciberespacio es un medio propicio para que esta se vea filtrada. Lo ideal en un escenario de concientización de parte de la autoridad correspondiente es sumar esfuerzos con los usuarios de manera generalizada y abierta para su correcta participación como eslabones de esta cadena.

Si comenzamos a mejorar la cadena de ciberseguridad con conocimiento para el usuario y creamos sensibilización en los temas prioritarios, o de mayor importancia para la seguridad nacional, el trabajo se verá reducido al hacer que colaboren en el ecosistema digital, por lo que prepararnos para un escenario de ciberguerra es ya una necesidad en esta sociedad hiperconectada 24/7. Los escenarios digitales están iniciando, ¿nos preocupamos o nos ocupamos?

IV. FUENTES DE CONSULTA

Alonso González, M. (2019). "Fake News: desinformación en la era de la sociedad de la información". *Ámbitos. Revista Internacional de Comunicación*. (45). Disponible en https://revistascientificas.us.es/index.php/Ambitos/article/view/8399/8424

Garcia, N. M. (2018). *The Dark Side of Social Media: The Case of the Mexican Drug War.* Miami: Universidad de Miami.

Gatwick (2018). "Drone Safety". Disponible en https://www.gatwickairport.com/business-community/aircraft-noise-airspace/airspace/drone-safety/

Gobierno de México (2017). *Estrategia Nacional de Ciberseguridad*. Disponible en https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

INCIBE (2019). Campaña de espionaje en la infraestructura DNS. Disponible en https://www.incibe-cert.es/alerta-temprana/bitacora-ciberseguridad/campana-espionaje-infraestructura-dns

Lonsdalem D. J. (2004). *The Nature of War in the Information Age*. London: Routledge.

Secretaría de Comunicaciones y Trasportes (SCT) (2017). Circular CO AV-23/10 R4. Disponible en http://www.sct.gob.mx/fileadmin/DireccionesGrales/DGAC-archivo/modulo3/co-av-23-10-r4.pdf

Schreier, F. (2015). *On Cyberwarfare*. Geneva Centre for the Democratic Control of Armed Forces.

LOS NUEVOS MODELOS DE NEGOCIOS Y LA APLICACIÓN DEL PRINCIPIO DE PREVENCIÓN DE OPERACIONES ILÍCITAS: DESAFÍOS Y RESPONSABILIDADES

Graciela Cami Soria*

* Integrante de la Comisión de Derecho Informático y Tecnológico del Instituto de Investigación y Técnica Notarial de la Asociación de Escribanos del Uruguay; miembro de la Asociación de Informáticos del Uruguay (ASIAP). Contacto: escribaniacami@gmail.com

PALABRAS CLAVE *KEYWORDS*

Fintech	*Fintech*
Banca digital	*Digital Banking*
Préstamos entre personas	*Crowdlending*
Lavado de dinero	*Money laundering*

Resumen. La cuarta revolución industrial, junto con el descrédito de la banca tradicional, producto de las últimas grandes crisis y otros fenómenos que se desarrollarán en el presente trabajo, ha venido afectando el sector financiero y propiciado el auge de nuevos emprendimientos y plataformas web vinculados a las finanzas. Se ingresa de esta forma al mundo de los *crowlending*, los *peer to peer lending* y las *fintech*.

Las tecnologías que emplean y la modalidad en cómo operan algunos de estos nuevos modelos de negocios los hace susceptibles de convertirse en instrumentos para el lavado de activos y financiamiento al terrorismo.

En este sentido, se analizan las circunstancias que han facilitado la aparición de esos nuevos modelos de negocios en línea, vinculados al sector financiero.

Abstract. The fourth industrial revolution, together with the discredit of traditional banking, as a result of the last great crises and other phenomena that will unfold in this work, has been affecting the financial sector and led to the rise of new ventures and web platforms linked to finance. In this way, the world of crowlending, peer to peer lending and fintech is opened.

The technologies they use and the way in which some of these new business models operate make them liable to become instruments for money laundering and terrorist financing.

In this sense, the circumstances that have facilitated the emergence of these new online business models, linked to the financial sector, are analyzed.

SUMARIO:

I. INTRODUCCIÓN

En diferentes foros se ha venido hablando de cómo la industria 4.0 impacta en la profesión notarial, así como a tantas otras profesiones, oficios y trabajos en general. De igual forma, el sector financiero se ha visto afectado por esta cuarta revolución industrial a la que hoy asistimos.

Sin embargo, la transformación de la banca no solo se debe a la llegada disruptiva de las nuevas tecnologías, sino que se ha venido gestando también a causa de diferentes fenómenos que han coadyuvado para que esa transformación sea factible.

Uno de esos sucesos clave se verificó hace aproximadamente una década, con la caída del banco de inversiones Lehman Brothers, el cuarto banco de inversión más grande de Estados Unidos, fundado en 1850 y con sede en Nueva York.

En realidad, más que un banco se trataba de un *holding*, es decir, una sociedad financiera que administraba un conjunto de empresas y poseía la mayoría del capital accionario.

Dicho *holding* quebró el 15 de septiembre de 2008; la quiebra constituyó la mayor en Estados Unidos y llevó, casi inmediatamente, a una crisis financiera a nivel mundial.

La quiebra del Lehman Brothers se vinculó a las hipotecas *subprime*, caracterizadas por un alto riesgo de impago; esto suponía un sistema de garantías aparentes, sin respaldo alguno, envuelto en una burbuja de aire que podía estallar en cualquier momento.

Tras la caída de Lehman Brothers, la banca tradicional quedó en una posición desfavorable. Muchos inversores, descontentos, buscaron en nuevos emprendimientos otras alternativas para la colocación de sus fondos.

A lo antedicho se agrega la llegada de las llamadas generaciones *Y* y *Z*, también denominadas respectivamente *milénica* o *millennial* (los nacidos entre 1980 y 1999) y *posmilénica* o *posmillenian* (los nacidos a partir del año 2000). Se trata de una franja etaria entre los 19 y los 39 años que no solo se relaciona socialmente a través de diferentes aplicaciones

y redes sociales, también compran y venden a través de internet (eBay, Amazon, Mercado Libre), alquilan vehículos (Uber), trabajan (*freelancers, influencers*), estudian (aulas virtuales, *webinars*), adquieren pasajes de avión, reservan hoteles, consiguen préstamos personales, etcétera, todo desde su celular, tablet o PC.

Si la realización de un trámite, la contratación de un servicio o la adquisición de un producto tienen su *alter ego* digital —es decir, si existe una aplicación o plataforma digital que les ofrezca la posibilidad de gestionarlo en línea—, difícilmente concurrirán a un lugar físico para obtenerlo: optarán por la vía *online*.

II. LOS NUEVOS MODELOS DE NEGOCIOS

En muchos países, la banca tradicional advirtió esta situación y comenzó la digitalización de sus procesos y sistemas; surgieron así los llamados *neobanks* y los *challenger banks*.

Los *neobanks* constituyen bancos tradicionales que ofrecen sus servicios y productos financieros en línea; sus clientes pueden acceder a los servicios del *neobank* a través de dispositivos móviles. Asimismo, cuentan con el respaldo de la entidad bancaria que los generó.

Los *challenger banks*, por el contrario, son modelos de negocios totalmente nuevos; son *startups* que también ofrecen sus servicios en línea, pero que están por fuera del sistema bancario tradicional.

El fenómeno de descrédito de la banca tradicional, junto a la forma como se manejan las generaciones *milénica* y *posmilénica*, propició así el auge de las denominadas *fintech* e *insurtech*.

El término *fintech* es un anglicismo formado por la yuxtaposición de las primeras sílabas de *finance* y *technology*. Básicamente, refiere a las tecnologías aplicadas a las finanzas. Las *insurtech* (*insurance* + *technology*) son las nuevas tecnologías aplicadas al sector seguros.

Las *fintech*, coloquialmente llamadas "Uber financieros", constituyen nuevos emprendimientos, plataformas web, *startups* que, sirviéndose de herramientas tecnológicas, ofrecen sus servicios y productos totalmente *online* y en diversos giros, tales como préstamos de dinero, inversiones, pagos, cambio de moneda, cheques.

En Uruguay existe una importante cantidad de *fintech*; también hay una Cámara Uruguaya de Fintech que a la vez es miembro de la Alianza Fintech Iberoamericana, esta última formada en 2017 e integrada por la Asociación Española de Fintech (AEFI), Colombia Fintech, Fintech México, Fintech Perú, Fintech Centro América y El

Caribe y por la Cámara Uruguaya de Fintech.

Los siguientes son algunos ejemplos de *fintech* uruguayas: Inversionate, Paganza, Bankingly, Ábaco, Socius, Dimo, SHA256 Trading, Fimix, MiCheque, Prezzta, Cámbiame, Efectivo Clic, Prex, Tutyasa, IN Switch y ZirconTech.

Con referencia a los préstamos entre particulares, los anglosajones han acuñado el término *crowdlending* o *P2P* (*peer to peer lending*). El término significa 'préstamos entre particulares', los que se realizan en línea y sin la intervención de la banca tradicional.

Los *crowdlending* son nuevos modelos de negocios desarrollados a través de plataformas web, que conectan a inversores con personas que buscan financiación. No solo median entre la oferta y la demanda, sino que también adoptan un rol más activo, analizando operaciones, aconsejando y ayudando en la toma de decisiones. Intervienen en los movimientos de dinero, es decir, reciben el pago de las cuotas por parte de los deudores y también hacen los pagos de intereses y capital a los inversores.

Es positivo que el sector financiero haya detectado la existencia de segmentos de la población a los que hay que atender en forma *online*. Es bueno que existan emprendimientos tecnológicos que ofrezcan nuevos productos y servicios financieros, porque con ellos se mejora la experiencia del usuario. Las transacciones se vuelven más transparentes y efectivas, y bajan los costos para el cliente final.

Sin embargo, no hay que descuidar los controles; no hay que permitir que estos nuevos modelos de negocios se transformen en instrumentos para la comisión de operaciones ilícitas y el financiamiento al terrorismo.

III. REGULACIÓN DE LOS NUEVOS EMPRENDIMIENTOS TECNOLÓGICO-FINANCIEROS

¿Cómo se controlan y regulan estos nuevos emprendimientos? Para responder a esta interrogante primero se ha consultado el derecho comparado, y encontramos así la ley mexicana que regula las instituciones de tecnología financiera (ITF). Se trata de una ley de orden público, conocida como "Ley de Fintech", publicada el 9 de marzo de 2018, que cuenta con 144 artículos y una serie de disposiciones transitorias.

Dicha ley tiene la particularidad de regular el funcionamiento de las ITF, además contiene disposiciones sobre pagos electrónicos y activos virtuales, así como diversas

disposiciones del mercado de valores y de lavado de activos.

Resulta sumamente llamativa una disposición en particular, el artículo 58 de dicha ley, que establece las obligaciones para las ITF y recoge las políticas de prevención de actividades con recursos de procedencia ilícita.

El giro particular de las ITF y las tecnologías con que operan las hacen propensas a ser empleadas para la comisión de operaciones ilícitas. Por esa razón, la ley mexicana exige a las ITF que establezcan una metodología que les permita llevar a cabo una evaluación de riesgos.

La reglamentación del artículo 58 supuso un texto de 106 artículos y varias disposiciones transitorias más. Básicamente, incorpora todo lo que nosotros, notarios uruguayos, conocemos o hemos venido estudiando en materia de prevención de lavado de activos; en especial, la recomendación 1 del GAFI, esto es, "identificar, evaluar y tomar acciones para mitigar el riesgo de lavado de activos y financiamiento al terrorismo".

Es así que esta reglamentación del artículo 58 recoge la obligación de identificar al cliente y determinar al "propietario real" —usa esta expresión en lugar de beneficiario final—, así como la verificación de si es una persona expuesta políticamente (PEP), la designación de un oficial de cumplimiento, la elaboración de un reporte de operaciones sospechosas y la implementación por parte de las ITF de programas de capacitación —en formato de talleres o cursos— para sus directivos, administradores, funcionarios y empleados al menos una vez al año. También incluye la recomendación de contar con sistemas automatizados que permitan detectar posibles operaciones inusuales del cliente y hacerle seguimiento, garantizando siempre la integridad, confidencialidad y disponibilidad de dicha información (Ley para Regular a las Instituciones de Tecnología Financieras, 2018: art. 58).

Otras legislaciones vienen trabajando en este tema, aunque no muchas poseen un marco regulatorio integral como el caso de México.

El análisis de todos los casos y los países que poseen regulación en esta materia excedería el límite máximo de folios permitidos para esta ponencia, por lo que solamente haré mención a dos países de Latinoamérica: Brasil y Argentina.

Brasil cuenta con una resolución aprobada por el Consejo Monetario Nacional, el 26 de abril de 2018 (resolución número 4656), que regula, entre otras, las sociedades de préstamos entre personas por medio de plataformas electrónicas (SEP, por su sigla de origen) y establece los

requisitos para el funcionamiento de estas.

Con referencia al tema que nos ocupa, es decir, el cumplimiento del principio de prevención de operaciones ilícitas, dicha normativa hace apenas dos sucintas referencias al tema. La primera mención se encuentra en su artículo 31, cuando dentro de los requerimientos para lograr la autorización del Banco Central del Brasil a los efectos de poder operar dispone que deberá presentarse comprobante de origen de los recursos utilizados en el emprendimiento. La segunda referencia se realiza en el artículo 38 numeral 1°, cuando establece las operaciones que se deben comunicar al Banco Central de Brasil y remite al artículo 31 antes referido.

Argentina, por su parte, cuenta con la Ley 27349 del 29 de marzo de 2017, denominada Ley de Apoyo al Capital Emprendedor.

Con el fin de fomentar el financiamiento de capital emprendedor en la República Argentina, esta ley establece la implementación del Sistema de Financiamiento Colectivo a través de las plataformas que, bajo el tipo de sociedades anónimas, conectan a inversores con personas que solicitan financiación. Se trata, entonces, de plataformas en línea que tienen por finalidad destinar fondos a un proyecto de financiamiento colectivo (lo que los anglosajones denominan: *crowdfunding*)

La Resolución General 717-E/2017 de fecha 29 de diciembre de 2017, reglamentaria de la referida ley, establece que la Comisión Nacional de Valores será la autoridad de control, reglamentación y fiscalización de estas plataformas de financiamiento colectivo.

En relación al tema central de este trabajo, es de destacar el artículo 6° de la reglamentación, que entre los requerimientos para la inscripción de estas plataformas establece la obligación de presentar una declaración jurada de prevención de lavado de activos y financiamiento al terrorismo. En dicho documento los responsables de la plataforma deberán indicar si son o no personas expuestas políticamente (PEP), asimismo, declararán que no poseen delitos de lavados de activos y no figuran en las listas de terrorismo del Consejo de Seguridad de las Naciones Unidas.

Los requisitos y documentación para presentar la inscripción a estas plataformas en el registro llevado por dicha comisión son similares a los que impone la circular del Banco Central del Uruguay para la inscripción de las Empresas Administradores de Plataformas de Préstamos entre Particulares, que analizaré en el párrafo siguiente.

IV. NORMATIVA URUGUAYA SOBRE PREVENCIÓN DE OPERACIONES ILÍCITAS CON RELACIÓN A LOS NUEVOS MODELOS DE NEGOCIO

A. LAS EMPRESAS ADMINISTRADORAS DE PLATAFORMAS PARA PRÉSTAMOS ENTRE PERSONAS

¿Qué ha hecho Uruguay en referencia a la regulación y supervisión de estos nuevos modelos de negocios y, particularmente, en este tema para cumplir con los estándares internacionales en materia de prevención de lavado de activos?

Recientemente, con fecha 21 de noviembre de 2018, la Superintendencia de Servicios Financieros del Banco Central del Uruguay (BCU) dictó una resolución, la que fue comunicada por circular n.º 2307, de 23 de noviembre siguiente (también se la puede encontrar en la Recopilación de Normas de Regulación y Control del Sistema Financiero), dada a conocer por circular del BCU n.º 2321, de 17 de enero de 2019.

La circular 2307 incorpora las empresas administradoras de plataformas para préstamos entre personas (título XII, libro I) y las define como "aquéllas personas jurídicas que administren aplicaciones web u otros medios electrónicos diseñados para mediar entre el oferente y demandantes de préstamos de dinero".

Los "clientes" de estas plataformas serán aquellos que se registren para divulgar sus ofertas o sus demandas de préstamos de dinero.

La circular del BCU establece que estas empresas administradoras de plataformas deben organizarse como sociedades comerciales y optar por alguno de los tipos sociales previstos en la ley 16 060; sus socios deben ser personas físicas. Si optaren por organizarse como sociedades anónimas, sus acciones deberán ser nominativas.

Asimismo, la circular les impone la obligación de inscribirse en un registro que a tal efecto llevará la Superintendencia de Servicios Financieros del BCU. La inscripción debe ser previa al inicio de actividades.

Para aquellas empresas que ya se encuentren operativas, la circular contiene una disposición transitoria por la cual se establece un plazo de cuatro meses, contados a partir de la fecha de la resolución —21 de noviembre de 2018—, para que procedan a la inscripción.

A diferencia de los *crowdlending*, mencionados anteriormente, estas empresas administradoras de plataformas para préstamos entre particulares solo podrán mediar entre la oferta y demanda de préstamos; es decir, solo se les estará permitido

"conectar" o "acercar" las partes, pero no asumir obligaciones ni riesgo alguno. Son los prestamistas del dinero quienes asumirán el riesgo de pérdida total o parcial del capital prestado, y quienes serán responsables —en caso— de incumplimiento de la ley 18 212 (tasa de interés y usura). No obstante, la empresa administradora de la plataforma tendrá la obligación de advertir al prestamista de dichos riesgos y responsabilidades.

Tampoco pueden las empresas administradoras de la plataforma manejar el dinero de los préstamos ya que todo el movimiento de dinero, tanto los préstamos, como los pagos de cuotas y de intereses, deben canalizarse a través de las entidades participantes en el Sistema Nacional de Pagos (Abitab, Red Pagos, Correo Uruguayo).

Los requisitos para la inscripción en el registro llevado por la Superintendencia de Servicios Financieros son muchos y variados; entre ellos, destacamos la constitución y el mantenimiento de "un depósito a la vista en el Banco Central del Uruguay no inferior a UI 50.000 (cincuenta mil unidades indexadas), a efectos de atender las obligaciones con dicha institución". Asimismo, se establecen límites en los montos tanto de las inversiones como de los préstamos dentro de la plataforma.

Vinculada al tema de este trabajo, existe una disposición en particular que se encuentra dentro de los requisitos para la solicitud de la licencia —es decir, dentro de la información requerida a estas empresas para su inscripción en el registro del BCU—, y es la que exige la presentación de un Manual del Sistema Integral para prevenirse de ser utilizadas en el lavado de activos y el financiamiento del terrorismo, y la designación de un oficial de cumplimiento.

La reglamentación exige a estas empresas adoptar instrumentos eficaces para verificar la identidad de sus clientes e implementar sistemas para prevenirse de ser utilizadas en el lavado de activos. Están obligadas a contar con procedimientos que les permitan determinar cuándo un cliente o beneficiario final es PEP, familiar o asociado cercano a una PEP. Asimismo, tendrán la obligación de reportar operaciones sospechosas.

Tratándose de clientes que otorguen préstamos de más de 300 mil unidades indexadas al año —aproximadamente 38 mil dólares—, la identidad del cliente deberá verificarse en forma presencial, cara a cara, aunque se deja abierta la posibilidad de que dicha identificación pueda ser realizada por un prestador de servicios de confianza (conforme al artículo 31 de la ley 18 600,

en la redacción dada por el artículo 28 de la ley 19 535).

La circular, además, dispone que las empresas administradoras de plataformas para préstamos entre personas deben mostrar total compromiso con el funcionamiento del sistema preventivo, estableciendo políticas y procedimientos apropiados y asegurando su efectividad.

Esas empresas estarán obligadas a implementar procedimientos que permitan detectar, prevenir y reportar transacciones; deberán exigir al personal un alto nivel de integridad y ofrecerle capacitación permanente acerca de la normativa aplicable y de las pautas para reconocer operaciones sospechosas.

La designación de oficial de cumplimiento deberá recaer en una persona comprendida dentro de la categoría de personal superior; puede ser un socio o un accionista radicado en el país.

El oficial de cumplimiento será el responsable de la implementación, seguimiento y control del adecuado funcionamiento del sistema y será el funcionario de enlace con los organismos competentes. También, deberá documentar la evaluación de riesgos realizada por la empresa y los procedimientos de control establecidos para su mitigación.

Estas empresas, asimismo, deberán adoptar un código de conducta que refleje el compromiso institucional asumido a efectos de evitar que se use el sistema financiero para el lavado de activos.

V. SANDBOX: UNA SOLUCIÓN ALTERNATIVA

Algunas *fintech* han expresado su descontento por la normativa adoptada por el Banco Central del Uruguay alegando que contiene requisitos excesivos para su licenciamiento, los que les impiden continuar con su actividad.

Siendo Uruguay un país con grandes carencias en seguridad, salud y educación, no puede permitirse desviar recursos humanos y económicos en proyectos informáticos que permitan a estas empresas administradoras de plataformas de préstamos entre particulares experimentar con productos financieros, mientras cumplen los requisitos para su licenciamiento. En cambio, otros países desarrollados, como Reino Unido, Suiza, Australia, Emiratos Árabes y Singapur, han implementado una solución alternativa denominada *sandbox* ('caja de arena'). México también posee su *sandbox,* Brasil y España vienen trabajando para poder implementarla.

La *sandbox* consiste en un ambiente virtual de prueba, un ecosistema informático controlado, en el cual estos nuevos emprendimientos

pueden realizar sus actividades, pero bajo la atenta mirada de los reguladores.

Dado que muchas veces es imposible cumplir con todos los requisitos previos al inicio de actividades, la *sandbox* permitiría a estas plataformas desarrollar poco a poco su operativa, acotando los riesgos; por ejemplo, con mínima cantidad de clientes y operaciones de bajo monto, y cumpliendo gradualmente con los requerimientos para la obtención de sus licencias. Al mismo tiempo, permitiría a las autoridades el monitoreo de sus actividades para ir evaluando los riesgos y tomando acciones tendientes a mitigarlos.

VI. REFLEXIONES FINALES

Resultado del avance de la tecnología, el surgimiento de nuevos modelos de negocios, en sana competencia con la banca tradicional, redunda en un beneficio para el usuario final.

No obstante, no hay que descuidar los controles. Es necesario regular, aunque sin ahogar estas nuevas iniciativas, y en este punto justamente radica el verdadero desafío.

Para el cabal cumplimiento del principio de prevención de operaciones ilícitas es necesario tener en cuenta la recomendación número 15 del GAFI sobre nuevas tecnologías; es decir, los países deben identificar y evaluar los riesgos de lavado de activos y el uso de las nuevas tecnologías para modelos nuevos o ya existentes, con el fin de mitigar riesgos y evitar que estas plataformas tecnológicas sean empleadas como instrumentos para cometer ilícitos (lavar activos o financiar el terrorismo).

Asimismo, es responsabilidad de los titulares de empresas administradoras de dichas plataformas web comprometerse con las políticas de prevención de lavado de activos para evitar que sus modelos de negocios sean usados como instrumentos para la comisión de operaciones ilícitas.

VII. FUENTES DE CONSULTA

Asociación Española de Fintech e Insurtech (2018). *Propuesta para la implantación de un* sandbox *en España*. En colaboración con Hogan Lovells, España. Disponible en https://asociacionfintech.es/wpcontent/uploads/2018/03/Informe_Final_Propuesta_Sandbox_Espa%C3%B1a.pdf, consultado el 30 de enero de 2019.

Banco Central del Brasil. Resolución 4656/2018, de 26 de abril de 2018, Brasil. Disponible en https://www.bcb.gov.br/pre/normativos/busca/

download Normativo.asp?arquivo=/Lists/Normativos/Attachments/50579/Res_4656_vl_O.pdf, consultado el 12 de agosto de 2019.

Banco Central del Uruguay. Circular n.º 2321 (Recopilación de Normas de Regulación y Control del Sistema Financiero), de 17 de enero de 2019, Montevideo.

Banco Central del Uruguay. Circular n.º 2307 ("Reglamentación de las empresas administradoras de plataformas para préstamos entre personas"), de 23 de noviembre de 2018, Montevideo.

Banco Central del Uruguay. Circular n.º 2078 ("Empresas de transferencias de fondos. Modificación de la normativa en materia de prevención del lavado de activos y del financiamiento del terrorismo"), de 21 de febrero de 2011, Montevideo.

Banco Central del Uruguay. Resolución 712/2018, de 19 de noviembre de 2018, Uruguay. Disponible en https://www.bcu.gub.uy/Servicios-Financieros-SSF/Resoluciones_SSF/RR-SSF-2018-712.pdf, consultado el 26 de enero de 2019.

Cámara Uruguaya de Fintech. Disponible en https://cafu.org.uy/, consultado el 30 de enero de 2019.

Comisión Nacional de Valores de la Nación Argentina. Resolución General 717E/2017, de 29 de diciembre de 2017, Buenos Aires, Argentina. Disponible en https://www.boletinoficial.gob.ar/detalleAviso/primera/177095/20180103, consultado el 26 de enero de 2019.

Da Silva, M. (14 de septiembre de 2017). "Al 'Uber financiero' le llegó la regulación: BCU regulará a las fintech como mediadores financieros". Diario *El País*, suplemento Negocios. Disponible en https://negocios.elpais.com.uy/noticias/bcu-regulara-fintech-mediadores-financieros.html, consultado el 26 de enero de 2019.

Fundación Wikimedia. "Lehman Brothers". En *Wikipedia, la enciclopedia libre*. Disponible en https://es.wikipedia.org/wiki/Lehman_Brothers, consultado el 26 de enero de 2019.

Redacción (15 de diciembre de 2018). "Plataformas para préstamos: Piden al BCU dejar sin efecto regulación de Fintech". Diario *El País*, suplemento Negocios. Disponible en https://negocios.elpais.com.uy/finanzas/piden-bcu-dehar-efecto-regulacion-fintech.html, consultado el 29 de enero de 2019.

Pozzi, S. (16 de septiembre de 2008). "Crisis financiera mundial; la caída de un gigante de

Wall Street: Lehman presenta la mayor quiebra de la historia con un pasivo de 430.000 millones". Diario *El País*, sección Economía. Disponible en https://elpais.com/diario/2008/09/16/economia/1221516004_850215.html, consultado el 26 de enero de 2019.

LEGISLACIÓN

Cámara de Diputados del Honorable Congreso de la Nación, Secretaría General, Secretaría de Servicios Parlamentarios Estados Unidos Mexicanos (s/f.). Ley para regular las Instituciones de Tecnología Financiera. *Diario Oficial de la Federación*, Ciudad de México, 9 de marzo de 2018. Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LRITF_090318.pdf, consultado el 7 de enero de 2019.

Senado y Cámara de Diputados de la Nación Argentina. Ley 27349 de Apoyo al Capital Emprendedor. Sala de Sesiones del Congreso Argentino, Buenos Aires, 29 de marzo de 2019. Disponible en https://www.senado.gov.ar/parlamentario/comisiones/verExp/80.16/CD/PL, consultado el 12 de agosto de 2019.

Uruguay, Poder Legislativo, Sala de sesiones de la Cámara de Senadores. Ley 18 600 ("Reconócese la admisibilidad, la validez y la eficacia jurídicas del documento electrónico y de la firma electrónica"), de 15 de septiembre de 2009. *Diario Oficial*, Montevideo, 5 de noviembre de 2009.

Uruguay, Poder Legislativo, Sala de sesiones de la Cámara de Senadores. Ley 19 535 ("Rendición de Cuentas y Balance de Ejecución Presupuestal correspondiente al ejercicio 2016"), de 18 de septiembre de 2017. *Diario Oficial*, Montevideo, 3 de octubre de 2017.

VISIONES PARA EL FUTURO

VIDEOJUEGOS Y DELITOS: ¿CORRELACIÓN O SUPERSTICIONES?

Daniel Córdova Herrera*

* Abogado especialista en propiedad intelectual y nuevas tecnologías. Profesor del Tecnológico de Monterrey.

PALABRAS CLAVE *KEYWORDS*

Videojuegos	*Videogames*
Violencia	*Violence*
Crímenes	*Crimes*
Regulación	*Regulation*

Resumen. El artículo busca contestar la pregunta sobre si los videojuegos de contenido violento son capaces de influir en que un individuo cometa acciones delictivas.

Desde el ámbito de la criminología, la psicología y la sociología, ha surgido algunas teorías que refieren la existencia de una correlación entre la exposición continua a la violencia y la comisión de ilícitos. En estas teorías se ha llegado argumentar que los videojuegos violentos pueden ser un predisponentes para el desarrollo de diversos crímenes, masacres u asesinatos. Pero ¿estas aseveraciones tienen sustento? En el presente artículo se analiza la industria actual de videojuego, la cultura de *gamer* desarrollada en torno a éste y la posible o no incidencia del mismo en el ámbito delictivo. Lo anterior a fin de advertir si resulta necesario regularla desde el derecho penal o la política criminal

Abstract. This essay is looking forward to answer if videogames of violent content are capable of influence on an individual to commit criminal actions.

Some psicological, social theories refer the existence of a correlation between continued exposure to violence and the commission of crimes. In these theories it has been argued that violent video games can be a predisposer for the development of various crimes, massacres or murders. But are these claims supported? This article analyzes the current video game industry, the gamer culture developed around it, and the possible or non-incidence of it in the criminal sphere. The above in order to warn if it is necessary to regulate it from criminal law or criminal policy

SUMARIO

I. INTRODUCCIÓN

¿Pueden los videojuegos llegar a influir en la conducta de una persona para que la misma llegue a cometer un delito?

La pregunta que se plantea trae un tema a la mesa bastante polémico y que no solo ha sido objeto de discusión desde el punto de vista jurídico, sino que, además, las cuestiones políticas y morales de determinadas sociedades han tomado la bandera de los videojuegos para capitalizar dicha discusión a los intereses de diversos bandos y posturas ideológicas.

Las recientes masacres de Jacksonville,[1] del Paso y Dayton[2] o en Nueva Zelanda[3] no solo han traído temas tan variados como el supremacismo blanco, la salud mental de los tiradores, el control y acceso de armas, sino que, además, se ha puesto en entredicho en diferentes espacios informativos y noticiosos, así como foros especializados, si los videojuegos juegan un papel importante en la influencia que un sujeto pueda tener a la hora de cometer un delito.

Cabe mencionar que el autor de estas letras es un gran aficionado a los videojuegos, a la cultura que los rodea y a las cosas tan increíbles que se pueden hacer con los mismos, como organizar torneos deportivos, y estar en posibilidades de que los *e-sports*[4] se reconozcan como juego olímpico en el futuro, así como

[1] Cuando David Katz, participante de un torneo de *e-sports*, abrió fuego y mató a uno de los competidores y lesionó a nueve personas más (De Llano, 27 de agosto de 2018).

[2] Donald Trump mencionó que: "Debemos detener la glorificación de la violencia en nuestra sociedad. Esto incluye los videojuegos horripilantes y espeluznantes que ahora son comunes…" (Redacción, 6 de agosto de 2019).

[3] "Un video de diecisiete minutos de una parte del ataque, que rápidamente se divulgó en internet antes de que los censores de las redes sociales pudieran eliminarlo, es uno de los registros en alta definición más perturbadores de la era digital sobre un ataque masivo con víctimas mortales, una muestra grotesca desde la perspectiva del tirador que documenta la capacidad que tienen los seres humanos para ser inhumanos" (Warzel, 16 de marzo de 2019).

[4] El concepto *e-sport* es muy interesante, ya que la definición que nos da la IESF (International Esports Federation, por sus siglas en inglés) en su sitio oficial es que se trata de "un deporte competitivo, realizado a través de un ambiente virtual, en donde habilidades físicas y mentales se ejercitan para crear una condición de victoria a través de reglas generalmente aceptadas. (Esports is a competitive sport performed in a virtual environment in which physical and mental abilities are exercised to create victory conditions through generally accepted rules)". https://www.ie-sf.org/e-sports/, 12/08/2019.

también crear mundos nuevos a través de tecnologías como realidad aumentada, realidad virtual e inteligencia artificial.

Luego entonces, lo que se pretende con este artículo es contestar las siguientes preguntas a la luz no solo del derecho penal, sino también de la misma tecnología, como lo son los videojuegos.

Por lo tanto, los puntos que se piensan abordar son los siguientes:

- ¿Qué son los videojuegos y qué los hace tan especiales para el mundo actual?
- ¿Los videojuegos inciden directamente en la comisión de delitos violentos? Si es así, ¿estar bajo su influjo es una agravante o atenuante de la comisión del delito?
- ¿La industria de los videojuegos debe ser regulada?

II. ¿QUÉ SON LOS VIDEOJUEGOS Y QUÉ LOS HACE TAN ESPECIALES PARA EL MUNDO ACTUAL?

El ecosistema *gamer*[5] define a los videojuegos como:

> … un juego electrónico que se practica a través de un controlador y en el que pueden participar una o más personas. Por supuesto, la definición de videojuego incluye un dispositivo que muestra las imágenes de video mediante las cuales podemos ejecutar nuestras acciones. (Gorria, 29 de julio de 2018)

Por lo anterior, podemos ver que los videojuegos son simples mecanismos para entretener a una o un grupo de personas, mediante el uso de herramientas digitales y en algunos casos hasta de internet.

Por otro lado, cabe aclarar que este trabajo no pretende hacer historia de los videojuegos y establecer cuál fue el primero, pero si nos gustaría mencionar que desde que nació el Atari,[6] por allá de los 70, la industria de los videojuegos empezó una carrera económicamente boyante, en la que, a pesar de algunas crisis, hoy en día se trata de una las actividades económicas más rentables en el mundo.

De esta manera, videojuegos icónicos como Pac-Man o Mario Bros (en todas sus versiones en distintas plataformas: NES, SNES, Nintendo 64, Wii, etcétera), así como también franquicias exitosas: Halo, GTA, Gears of War, God of War,

[5] Un *gamer* es un aficionado o un individuo que disfruta jugar varios tipos de juegos en versión *online* o digital: "A *gamer* is a hobbyist or individual that enjoys playing various types of digital or online games". https://www.techopedia.com/definition/1912/gamer, 18/08/2019.

[6] "Atari fue creado por Nolan Bushnell y Ted Dabney en 1972 y se convirtió en pionero de juegos arcada, consolas domésticas de videojuegos y computadoras para el hogar (Atari was created by Nolan Bushnell and Ted Dabney in 1972 and became a pioneer in arcade games, home video game consoles and home computers)". https://www.atari.com/about-us/, 18/08/2019.

y recientemente juegos como *Fortnite* o *Cuphead* hacen de la industria del videojuego no solo un negocio de miles de millones de dólares al año, sino que no se vislumbra que en el futuro próximo pueda existir una caída en el consumo que dicha industria reporta año con año.

En efecto, no puede pasarse por alto que para 2019 se estima que la industria de los videojuegos genere ganancias en alrededor de 151.9 miles de millones de dólares, cifras que casi triplican lo de industrias como el cine y la música combinadas.[7]

No solo la industria de los videojuegos tiene un futuro brillante, sino que lo que se genera de forma adicional a la misma, como el *streaming*[8] o el fenómeno de los *e-sports*,[9] hace que esta industria no solo crezca, sino que aumente y amplíe el rango de consumidores que puedan acercarse a la misma.

III. ¿LOS VIDEOJUEGOS INCIDEN DIRECTAMENTE EN LA COMISIÓN DE DELITOS VIOLENTOS? SI ES ASÍ, ¿ESTAR BAJO SU INFLUJO ES UNA AGRAVANTE O ATENUANTE DE LA COMISIÓN DEL DELITO?

Ahora bien, ya se puntualizó que la industria de los videojuegos hoy en día vale miles de millones de dólares anuales y que, además, trae consigo una infinidad de fenómenos adicionales que solo hacen que el espectro de consumidores directos e indirectos sea mucho mayor. Por lo que es importante saber si en verdad los videojuegos, por sí mismos, logran

[7] No solo las triplican, sino que, además, dichas industrias se encuentran en una crisis de identidad por fenómenos como la piratería o la falta de guiones o ideas creativas, mientras que los videojuegos siguen ascendiendo. Como comparación, *Avengers: Infinity War,* que se estrenó en 2018 y tuvo un debut en taquilla de 257. 6 millones de dólares, mientras que *Grand Theft Auto V*, que se lanzó en 2013 y en 24 horas vendió 11 millones de unidades, registró ingresos por 817 millones de dólares, llegando a 1000 millones de dólares en solo 3 días. ("When comparing the best movie premieres in cinema history with the best game launches, Hollywood may have more glamour, but it doesn't have more money. On April 27th, 2018 the premiere of the Avengers: Infinity War generated $257,698,183, leading the best opening box office of any movie up to date, followed by Star Wars: The Force Awakens on December 18th, 2015, with earnings of $247,966,675.

"In the meantime, on the parallel universe of video games, Grand Theft Auto V came out on September 17th, 2013 and in only 24 hours it sold over 11 million unities, reaching $817,5 million in sales. In just 3 days, the game registered revenue of 1,000 million dollars. It went on to become the highest grossing entertainment product of all time"). https://lpesports.com/e-sports-news/the-video-games-industry-is-bigger-than-hollywood, 18/08/2019

[8] *Streaming* significa escuchar música o ver videos en tiempo real, en lugar de descargar el archivo a la computadora y verlo después. En el caso de los videojuegos, se ha puesto de moda el ver a través de plataformas, como Youtube o Twitch a *gamers* o *youtubers* famosos el jugar videojuegos o hasta torneos de algún juego en particular. ("Streaming means listening to music or watching video in 'real time', instead of downloading a file to your computer and watching it later"). http://www.bbc.co.uk/webwise/guides/about-streaming 18/08/2019

[9] Famosa fue la noticia del *gamer* que ganó el torneo de Fortnite a los 16 años y se llevó una bolsa acumulada de $3 millones de dólares. Shannon, L. (29 de julio de 2019).

influir en la mente de una persona para cometer acciones violentas que puedan traducirse en delitos.

Lo anterior cobra relevancia ya que, como se menciona en la introducción de este trabajo, existen sectores que pugnan por que los videojuegos son los responsables de la comisión de conductas violentas, como lo son, por ejemplo, el caso de las masacres que fueron señaladas con anterioridad.

Por lo tanto, es necesario intentar saber si realmente un videojuego es capaz de controlar e influir en el estado de un sujeto de derecho para hacer que este cometa acciones violentas en contra de otras personas o propiedades, o si, por el contrario, dicha afirmación es solo un buen pretexto para que otros grupos desvíen la atención mediática de otros temas que verdaderamente podrían considerarse como las causas para la comisión de delitos en contra de un determinado grupo de personas.

Ahora bien, las conductas delictivas que lleva a cabo una persona se determinan en una primera instancia por el *iter criminis*,[10] por lo que para que una persona lleve a cabo una determinada conducta delictiva, la misma debe delinear el camino para ejecutarla, con el objeto de materializar en la realidad dicho acto, independientemente que al final las consecuencias fueran o no las deseadas por el sujeto que hubiere realizado dicha conducta.

En este sentido, y atendiendo a que se trata de determinar si los videojuegos pudiesen hacer que una persona decidiera cometer una conducta antijurídica, cabe preguntarse si los mismos pudieran tener un papel en el *iter criminis* de la conducta catalogada como delito. Es decir, habría que saber si efectivamente, a la hora en que el hecho punible es planeado y después materializado por el sujeto, los videojuegos tuvieron un papel preponderante en la conducta del sujeto para realizar la conducta antijurídica.

Esto es importante porque —como se verá más adelante— la defensa de una persona que haya cometido un delito pudiera alegar que, al estar influenciado bajo los efectos de los videojuegos, el sujeto pudiera ser inimputable o buscar una atenuante al respecto. Por

[10] Sobre este concepto, diversos penalistas han mencionado que el *iter criminis* es "el estudio de las diversas fases recorridas por el delito desde su ideación hasta su agotamiento" (Pavón Vasconcelos, 1961); el camino que recorre el hecho punible doloso que va desde que surge la decisión de cometerlo hasta la consecución de las metas últimas pretendidas con su comisión, pasando por su preparación, comienzo de la ejecución, conclusión de la acción ejecutiva y producción del resultado típico (Muñoz Conde, 2002); "el camino del crimen, el sendero o ruta que recorre desde su iniciación hasta su total agotamiento" (Castellanos, 1959). Nosotros coincidimos más con la postura de Muñoz Conde, ya que, al ser de corte funcionalista, consideramos que el *iter criminis* empieza con la decisión del sujeto que desea cometer un delito, más allá que los resultados obtenidos sean los esperados o no.

consiguiente, existe en la actualidad un debate bastante encarnizado sobre si los videojuegos pudieran ser factores que ejercieran un control sobre una persona para la comisión de un delito

Entre las posturas más fuertes que alegan que los videojuegos inducen a las personas a cometer delitos, se encuentra la de la Asociación Americana de Psicología, la cual menciona que existe "una relación entre el jugar videojuegos violentos y que se incrementen conductas agresivas, así como la falta de empatía y compromiso moral".[11]

Por otro lado, existen estudios interesantes respecto a que cuando salen al mercado contenidos violentos, las conductas catalogadas como delitos tienden a decrecer. En este sentido, Seth Stephens-Davidowitz, en su libro *Everybody lies: what the internet can tell us about who we really are*, menciona que, de un estudio de *big data*[12] realizado por dos economistas, Gordon Dahl y Stefano DellaVigna, encontraron un patrón bastante interesante.

Dicho patrón fue descubierto al unir tres bases de datos distintas, donde se descubrió que cuando una película violenta era estrenada, los índices de conductas delictivas bajaban, a diferencia de cuando una película no violenta era estrenada.[13]

Ahora bien, el estudio anterior se hizo para películas violentas, más no así para videojuegos, y aquí se podría estar en el campo de la especulación, ya que se deberían hacer estudios para determinar si cuando se lanza un videojuego violento y que es popular las tasas de criminalidad también pudieran bajar.

[11] "Considerando que muchos factores son de riesgo para un mayor comportamiento agresivo, cognición agresiva y afecto agresivo, y un comportamiento prosocial reducido, empatía y compromiso moral, y el uso violento de videojuegos es uno de esos factores de riesgo (Whereas many factors are known to be risk factors for increased aggressive behavior, aggressive cognition and aggressive affect, and reduced prosocial behavior, empathy and moral engagement, and violent video game use is one such risk factor). (APA, 2015).

[12] "*Big data* es un término que describe el gran volumen de datos, tanto estructurados como no estructurados que inundan una empresa en el día a día. Pero no es la cantidad de datos lo que importa. Lo que tiene importancia es lo que hacen las empresas o las organizaciones con los datos y lo que se descubre de los mismos. Los grandes datos se pueden analizar para obtener información que conduzca a mejores decisiones y movimientos estratégicos de negocios. (Big data is a term that describes the large volume of data —both structured and unstructured— that inundates a business on a day-to-day basis. But it's not the amount of data that's important. It's what organizations do with the data that matters. Big data can be analyzed for insights that lead to better decisions and strategic business moves)". https://www.sas.com/en_us/insights/big-data/what-is-big-data.html, 24/08/2019

[13] Dos economistas, Gordon Dahl y Stefano DellaVigna, unieron tres bases de datos de *big data* de los años 1995 a 2004: Datos de crímenes por hora del FBI, números de taquilla y la medida de violencia en cada película desde el sitio: kids-in-mind.com… Descubrieron que en los fines de semana que se exhibía una película violenta y que era popular, el crimen bajaba. (Two economists, Gordon Dahl y Stefano DellaVigna, merged together three Big Datasets for the years 1995 to 2004: FBI hourly crime data, box-office numbers and a measure of the violence in every movie from kids-in-mind.com… They found that on weekends with a popular violent movie, crime dropped)". (Stephens Davidowitz, 2017: 191-192)

Sin embargo, sí podemos decir que lo que fue encontrado en el estudio antes mencionado, y lo que se puede interpretar al respecto, es que un material violento que es estrenado puede servir de medio catártico para personas que tengan una mayor predisposición a la violencia.

La realidad es que hoy en día ni las posturas que abogan por trasladar la culpa del aumento de la violencia a los videojuegos, o que, por el contrario, los videojuegos pueden ser medios para lograr reducir la violencia, al ser una especie de terapia para sujetos con tendencias violentas, pueden ser demostradas del todo, ya que ningún estudio ha logrado ser del todo concluyente.

En este sentido, y atendiendo a que se debe tomar una postura al respecto, consideramos que los videojuegos, como tal, no hacen que una persona decida cometer un delito, sino que más bien pudieran —en algún punto— ser una influencia indirecta, como las hay también por parte de libros, películas, canciones, una obra de arte o hasta un personaje famoso, sin que al final se decida condenar a dichas influencias como responsables de la comisión de delitos.

Luego entonces, los videojuegos, como tal, no son los responsables de que una persona decida cometer un delito y, por lo tanto, podría alegarse que uno se encontraba "bajo los efectos de un videojuego", para tratar de lograr atenuar una posible pena, por ejemplo, mencionado que se encontraba en estado de emoción violenta conforme a lo establecido por el artículo 136 del Código Penal para el Distrito Federal que establece lo siguiente:

> **Código Penal para el Distrito Federal**
> ARTÍCULO 136. A quien en estado de emoción violenta cometa homicidio o lesiones, se le impondrá una tercera parte de las penas que correspondan por su comisión. Existe emoción violenta cuando el sujeto activo del delito vive una intensa conmoción del ánimo que provoca un desorden del comportamiento, la pérdida del dominio de su capacidad reflexiva y la disminución de sus frenos inhibitorios, que desencadenaron el delito.

Al respecto, se podría argumentar que, de ser el caso, al menos en México, si una persona cometiera, por ejemplo, el delito de homicidio y alegara que se encontrara en una emoción violenta al estar bajo el influjo de los videojuegos para cometer dicha conducta, se tendría que demostrar la relación entre el videojuego y el estado de emoción violenta, a efectos de que el juez decidiera imponer una pena reducida por la comisión de dicha conducta.

Sin embargo, consideramos que lo anterior sería bastante difícil de probar, ya que la parte esencial sería demostrar el que una persona que haya jugado un determinado

videojuego fuera el factor que desencadenó que emocionalmente haya vivido una intensa conmoción y que, por lo anterior, le fuera provocado un desorden del comportamiento, la pérdida del dominio de su capacidad reflexiva y la disminución de sus frenos inhibitorios, y, por ende, le llevó a cometer el delito.

Más aun, podría ser una agravante, pues el defenderse y argumentar que uno se encontraba bajo el influjo, en este caso de los videojuegos, para cometer un determinado delito no eximiría de responsabilidad al sujeto, puesto que este se puso en dicha situación al consumir o jugar algo que sabía podría provocarle que se decidiera a cometer la conducta delictiva.

La realidad es que hasta el día de hoy se desconoce si en el tipo de casos como el antes planteado pudiera alegarse un estado de emoción violenta como atenuante o si, por el contrario, se consideraría un agravante que se manifestara estar bajo el influjo de un determinado videojuego sin embargo, en algún momento esto podría suceder, y sería interesante saber qué se decidiría al respecto.

IV. ¿LA INDUSTRIA DE LOS VIDEOJUEGOS DEBE SER REGULADA?

Finalmente, hemos llegado a la cuestión sobre si la industria de los videojuegos debiera ser regulada, que se prohibieran algunos títulos o si, por el contrario, no debería existir ningún tipo de regulación. Se dejó al final de este ensayo esta cuestión, ya que resulta hasta ocioso tratar de responderla, pues en realidad la industria de los videojuegos ya se encuentra regulada.

En efecto, los videojuegos siguen un sistema de clasificación de contenido, donde se sectoriza por edad lo que está permitido que contenga el mismo y qué sector de la población puede acceder o comprar dicho videojuego.[14]

Luego entonces, no se trata de si deba estar regulado o no, sino contestar la pregunta de si los videojuegos de contenido violento deberían prohibirse o censurarse.

Nuestra postura es que no debiera prohibirse bajo ningún motivo cualquier tipo de videojuego, ya que con la clasificación por edad que se hace de estos cada persona es libre de decidir qué comprar, y eso es más que suficiente, ya que, de lo

[14] Por ejemplo, en el caso de México y Estados Unidos, se utiliza el sistema Entertainment Software Rating Board (ESRB). Para saber más se puede consultar la siguiente página: https://www.esrb.org/about/

contrario, entraríamos en un tema de libertad de elección y prohibicionismo absurdo.

Por lo anterior, no se puede pasar por alto que en la práctica muchos niños y jóvenes adquieren videojuegos que se encuentran clasificados para personas de mayor edad, pero esa situación es la que debería de corregirse, no el hecho de prohibir el videojuego por sí mismo, sino buscar mecanismos para que menores de edad no tengan ni siquiera la oportunidad de jugar un título que sea clasificado para mayores de edad.

Es decir, el adquirir un videojuego que sea clasificado por ejemplo como M[15] o AO,[16] debería ser prohibitivo para su venta a menores de edad que no acrediten que legalmente puedan adquirir el videojuego, y, por otro lado, también un tema para los padres o tutores es el no fomentar y comprar títulos clasificados de esa manera y dárselos a quien no ha cumplido con los requisitos del estándar de clasificación.

Por lo anterior, podría hacerse una campaña tal como se ha hecho con el tema de los cigarros o el alcohol, donde no se le pueden vender dichos productos a menores de edad, y establecer sanciones fuertes a quien incumpla con dichas regulaciones.

El atender lo anterior implicaría realmente afrontar un tema complejo y bastante álgido, pero con soluciones inteligentes y determinadas para que una industria que genera miles de millones de dólares, así como empleos de forma mundial, siga floreciendo sin necesidad de censurarla o prohibirla, sino solo de aplicar de forma correcta la ley y las regulaciones de edad necesarias.

V. FUENTES DE CONSULTA

APA Council of Representatives (2015). "Resolution Violent Video Games". En American Psychological Association. Disponible en https://www.apa.org/about/policy/violent-video-games, consultado el 23 de agosto de 2019.

Asamblea Legislativa del Distrito Federal. Código Penal para el Distrito Federal (16 de julio de 2002). *Gaceta Oficial del Distrito Federal.* Última reforma publicada el 16 de julio de 2016.

Castellanos, F. (1959). *Lineamientos Elementales de Derecho Penal*. México: Porrúa.

De Llano, P. (27 de agosto de 2018). "Un tirador deja dos muertos y

[15] Mature o Maduro Contenido para mayores de 17 años, ya que puede contener violencia intensa, sangre, lenguaje ofensivo o contenido sexual. https://www.esrb.org/ratings-guide/.

[16] Adults Only o Solo Adultos. Puede contener escenas prolongadas de violencia, contenido sexual gráfico o apuestas. https://www.esrb.org/ratings-guide/.

11 heridos tras abrir fuego durante un juego de videojuegos en Florida. En *El País*. Disponible en https://elpais.com/internacional/2018/08/26/actualidad/1535308945_111530.html, consultado el 12 de agosto de 2019.

Gorria, A. (29 de julio de 2018). "Qué son los videojuegos y cómo evolucionaron". En *Hablamos de gamers*. Disponible en https://hablamosdegamers.com/analisis/que-son-los-videojuegos/, consultado el 18 de agosto de 2019.

Pavón Vasconcelos, F. (1961). *Derecho Penal Mexicano*. México: Porrúa.

Muñoz Conde, F. (2002). *Derecho Penal Parte General*. España: Tirant Lo Blanch

Redacción (6 de agosto de 2019). "'Los videojuegos no son culpables' de la matanza de e El Paso: el sector desmiente los ataques de Trump". En *El diario es cultura*. Disponible en https://www.eldiario.es/cultura/videojuegos/videojuegos-matanza-Paso-Trump_0_928457393.html, consultado el 12 de agosto de 2019.

Stephens Davidowitz, S. (2017). *Everybody Lies: Big Data, New Data, What the Internet Can TellX Us about Who We Really Are*. Reino Unido: Dey Street Books

Shannon, L. (29 de julio de 2019). "Un adolescente de 16 años gana US$3 millones en campeonato de Fortnite". En CNN. Disponible en https://cnnespanol.cnn.com/2019/07/29/un-adolescente-de-16-anos-gana-us-3-millones-en-campeonato-de-fortnite/, consultado el 18 de agosto de 2019.

Warzel, C. (16 de marzo de 2019). "Cuando el terrorismo es concebido para ser viral". *The New York Times*. Disponible en https://www.nytimes.com/es/2019/03/16/masacre-christchurch-nueva-zelanda/, consultado el 12 de agosto de 2019.

PÁGINAS WEB

Atari. "About us". Disponible en https://www.atari.com/about-us/

ESRB. "About ESRB". Disponible en https://www.esrb.org/about/

ESRB. "Ratings Guide". Disponible en https://www.esrb.org/ratings-guide/

IESF. "About Esports". Disponible en https://www.ie-sf.org/e-sports/

Techopedia. "Gamer". Disponible en https://www.techopedia.com/definition/1912/gamer

Webwise (10 de octubre del 2012) "What is streaming". Disponible en http://www.bbc.co.uk/

webwise/guides/about-streaming
SAS. "Big data". Disponible en https://www.sas.com/en_us/insights/big-data/what-is-big-data.html

LOS ESTADOS, LAS CRIPTOMONEDAS Y LA CIBERSEGURIDAD*

Humberto Martín Ruani**

* Texto presentado en el XXIII Congreso Iberoamericano de Derecho e Informática —FIADI— Sao Paulo 2019.

** Presidente de la Asociación Argentina de Informática Jurídica.

PALABRAS CLAVE *KEYWORDS*

Criptomonedas	*Cryptocurrencies*
Delitos informáticos	*Cibercrime*
Delitos económicos	*Economic crimes*
Comercio electrónico transfronterizo	*Cross border e-commerce*

Resumen. Este trabajo aborda la situación actual de los activos conocidos como criptomonedas. Se realiza un análisis de sus antecedentes, objetivos y mecanismos de acción. A su vez, se propone un criterio ético que concluye en una serie de recomendaciones para su regulación a nivel internacional.

Abstract. This work is about the actual situation of the assets known as cryptocurrencies. It is an analysis of their background, objectives and mechanisms of action. In turn, an ethical criterion is proposed, which concludes in a series of recommendations for its regulation on an international level.

SUMARIO:

I. INTRODUCCIÓN

Hoy día es innegable el valor que han adquirido las criptomonedas, y cualquiera que haya operado con las mismas puede dar fe de que este mecanismo es la practicidad hecha dinero. Aparte quedan temas como si es una inversión segura o rentable. La realidad es que poder enviar dinero a casi cualquier parte del mundo, en cuestión de segundos y con un costo ridículo, como pueden ser la cantidad de 0,02 dólares por transferencia (Ethgasstation, 2019), sin impuestos, sin tasas ni contribuciones, sin controles de ningún tipo, es una realidad que hasta hace apenas una década atrás pareciera inalcanzable.

Por otro lado (el lado oscuro) es usual que, tras el desarrollo de nuevas tecnologías, aparezcan personas que adapten las mismas en función de obtener un beneficio propio. El problema real se da cuando ese beneficio es en perjuicio de otros. En este sentido, precisamente, las ventajas que ofrecen las criptomonedas, como el anonimato, la falta de control de un ente centralizado y la falta de regulación a nivel internacional, hacen que sea una excelente vía para la ejecución de delitos administrativos y económicos, ya que no hay un registro formal de las operaciones, ni identificación fehaciente de las partes.

Aquí, lo que realmente hace ruido es que, en el desarrollo de una herramienta como esta, en la cual no se identifican las partes, se transfieren créditos con valor pecuniario a cualquier parte del mundo, sin que se registren las operaciones, sin que los sistemas fiscales e impositivos puedan controlar los ingresos y egresos de las personas, *¿podría hipotéticamente haberse creado para usuarios que cumplen con sus declaraciones de impuestos y con la normativa fiscal de sus países?*

Bueno, en Argentina y otros países de habla hispana utilizamos a menudo la frase: "Se inventó el avión a chorro y el chorro afana en avión". La respuesta al párrafo anterior quedará a criterio de cada uno pero, en mi opinión, pareciera que en vez de inventarse el avión a chorro y que el "chorro" después "afanara" en avión, aquí más bien se inventó un arma digital y después se le disfrazó de avión.

Mucho podemos hablar de la ciberseguridad, de la aplicación de la tecnología y de los beneficios de poder realizar transferencias seguras —y lo haremos más adelante—, pero muchas veces podemos estar frente a un arma de doble filo cuando las herramientas desarrolladas sirven para agilizar tanto actividades lícitas como ilícitas.

II. DEFINICIÓN Y ANTECEDENTES

A. CONCEPTO DE CRIPTOMONEDAS

La denominación de criptomonedas define este concepto *per se*; se trata de una moneda encriptada, codificada. Básicamente, es una red de datos protegida con fuerte seguridad, que permite controlar la creación de unidades originarias y adicionales. También permite verificar la transferencia de activos, pero sin la necesidad de un intermediario formal, es decir, que tienen un control descentralizado, a diferencia de los bancos y entidades financieras.

Otra diferencia con el sistema tradicional es que las transacciones de criptomonedas no se realizan en forma individual, sino que se agrupan varias transacciones y se conforma un bloque que se controla al cerrarse y se adjunta a otros bloques, controlados y cerrados, formando así las conocidas cadenas de bloques o, en inglés, *blockchain*, que son el equivalente a un registro público de transacciones, con la salvedad de que aquí no hay nombres, ni identificación de personas humanas.

La última gran diferencia que tendremos en cuenta es que, con las monedas tradicionales, la única manera de obtenerlas es a través de una transacción comercial o laboral; mientras que las criptomonedas, como necesitan de trabajo humano para revisar las transacciones, pagan por ello. De esta manera, aquellos que tienen algunos conocimientos específicos pueden obtener criptomonedas como pago por su ayuda para con el sistema. Estos constructores de paquetes, que preparan los bloques para que viaje la información, son conocidos como mineros.

Este sistema de procesar información que utilizan miles de usuarios y ordenadores genera una enorme red de seguridad, la cual, si bien es matemáticamente quebrantable, requeriría de una capacidad de procesamiento realmente grande; de hecho tendría que ser mayor que el de todo el entramado (red-enjambre) de todos los mineros del sistema, y aun así solo tendría una probabilidad de éxito del 50% (núm. de ronda de autenticación).

B. ORIGEN DE LAS CRIPTOMONEDAS

Como muchos otros inventos, incluso internet, las criptomonedas no se generaron por una única idea en un momento determinado, sino que han tenido su evolución en distintos momentos. Básicamente, podemos remontarnos a 1983, cuando el criptógrafo David Chaum desarrolló un sistema criptográfico monetario electrónico llamado *ecash*, nombre que, al menos en Argentina, aún utiliza una empresa de pagos electrónicos. Más de 10 años después, desarrolló *digi cash*; este sistema, bastante más similar al concepto de criptomonedas actuales, utilizaba la criptografía para dar anonimato a las transacciones de dinero. Este sistema contaba con un software que, al tomar dinero de una entidad financiera, codificaba y encriptaba las operaciones antes de que pudieran transferirse a alguien más y, de esta manera, conseguía evitar que se rastreara el trazado del dinero. Sin embargo, carecía de algo esencial que tienen las criptomonedas actuales y es, precisamente, la descentralización del control, ya que las operaciones de dicho sistema requerían un control central.

Más allá de los antecedentes referidos en el párrafo anterior, muchos —la mayoría— identifican la primera publicación de la idea actual de criptomonedas con el ingeniero informático Wei Dai, quien, en 1998, propuso crear un nuevo tipo de dinero, cuya plataforma no fuera física y, principalmente, una herramienta de intercambio económico que no dependiera de un organismo central, sino que se regulara de manera descentralizada.

El ingeniero Dai propuso que una de las formas de darle seguridad a dicha herramienta era la utilización de la criptografía como medio de control. Unos años más tarde, bajo el pseudónimo de Satoshi Nakamoto, se creó el conocido por todos Bitcoin, entre 2008 y 2009, que más adelante desató una enorme controversia por el anonimato detrás del pseudónimo, así como también lo hizo por el hecho de tratarse de un código abierto que cualquier persona, con conocimientos de programación y desarrollo de software, puede revisar y comprender. Es más, este sistema permite modificaciones en su código sin que un ente central las apruebe o rechace. La única condición es la aprobación de los demás usuarios.

III. LEGALIDAD Y LEGITIMIDAD

Estos dos conceptos, que suenan tan parecidos, tienen definiciones similares toda vez que la primera definición, según la Real Academia

Española (2019), es precisamente que algo legítimo es aquello acorde a la ley. Sin embargo, cuanto más indagamos respecto de este vocablo, más nos encontramos con una idea de lo que es debido, de lo lógico, de lo correcto; mientras que lo legal sigue estrictamente la letra de la normativa escrita y la adecuación de las conductas a dicha normativa.

El conocido principio de legalidad nos indica que "todo lo que no está prohibido, está permitido". En otras palabras, es tan importante la seguridad jurídica que aun cuando la lógica indique que una acción es socialmente negativa, si la misma no está prohibida expresamente por la normativa vigente, entonces será legal y, por lo tanto, no reprochable por el sistema de administración de justicia.

En esta inteligencia, el uso de las criptomonedas estará en sí mismo permitido, siempre y cuando no esté prohibido. Ahora bien, saltando la parte de definir las criptomonedas y siguiendo el principio de la primacía de la realidad, en el cual nos encontramos que resultan ser bienes intangibles, susceptibles de apreciación pecuniaria, independientemente de la legalidad que puedan alcanzar, no es menos cierto que debieran cumplimentar con todas las formalidades que en cada país regulan este tipo de bienes.

Por otro lado, el uso de estas criptomonedas, que de por sí puede ser cuestionado en cuanto a su específico diseño formulado para ser impersonal y favorecer el anonimato, es también con frecuencia utilizado en actividades ilegales, además de imposibilitar el establecimiento de políticas impositivas sobre transacciones realizadas a través de dicho medio por parte de los gobiernos.

IV. LA CIBERSEGURIDAD Y LAS CRIPTOMONEDAS

En la actualidad, es realmente amplio el campo de la ciberseguridad y, como dijimos anteriormente en la introducción, es mucho lo que se puede hablar de esta disciplina. Es que, tratándose de un producto netamente digital, las criptomonedas realmente se destacan en este campo. Están concebidas no solo para resistir ataques, sino también para ser escrutadas por los usuarios e interesados. En algunos casos, incluso poseen un código abierto a través del cual la misma comunidad de usuarios es capaz de modificar el funcionamiento del *software* con la condición de que dicha modificación sea aceptada por los demás usuarios. Esto, por un lado, otorga una confiabilidad y transparencia envidiable, mientras que por otro expone completamente su

mecanismo y eventuales vulnerabilidades.

En este sentido, resulta imposible a esta altura garantizar la seguridad de un sistema operativo en un cien por ciento. Así como uno puede en su casa colocar una reja, un sistema de alarmas, un custodio en la puerta o mudarse a una isla, permanentemente se está aumentando el nivel de seguridad, pero en ninguno de los casos se podría evitar la muerte ante la caída cercana de una bomba atómica. Esta exageración —tal vez algo burda— es un ejemplo claro de cómo, con ciertas medidas, podemos "achicar ventanas", reducir riesgos, evitar ciertos tipos de ataques y prevenir eventuales accidentes.

El concepto de "achicar ventanas" es una metáfora que define muy aproximadamente el objetivo de la seguridad en general y que aplica específicamente a la ciberseguridad. En este sentido, tanto en lo que refiere al *software* como incluso al *hardware*, siempre podemos elevar el nivel de seguridad; aunque a veces no podamos prevenir o resistir un ataque nuclear, posiblemente podamos evitar otros ataques menores, pero a la vez más probables o frecuentes.

En el caso de las criptomonedas consideremos que hay gran diversidad de sistemas, como hemos visto anteriormente, pero que se trata de un valor que hasta hoy es incluso más valioso y apetecible que los datos personales. Estamos hablando de dinero *contante y sonante*, dinero que persiguen aquellos que desarrollan una plataforma de moneda electrónica, o al menos —con seguridad— lo persiguen quienes hacen uso de estos medios.

Podría ser redundante decir que el eslabón más débil, generalmente, es el humano, ya que cuando se trata de información protegida intencionalmente con asesoramiento de profesionales en la materia, no es tan sencillo romper las barreras de seguridad del *software* o del *hardware*. Pero la realidad es que una vez más, tratándose de criptomonedas, el eslabón más débil es el mismo que en el resto de las situaciones.

La amenaza más vigente no ataca directamente el *software* de la criptomoneda, ni las cuentas de los usuarios. En el universo de las monedas electrónicas, donde existen actividades que producen *per se* una renta activa, la violación de seguridad más común refiere a la utilización, no autorizada e ilícita, de la capacidad de procesamiento de ordenadores, teléfonos o dispositivos afines, ajenos a quien realiza la actividad. Por ejemplo, mientras yo estoy durmiendo con mi teléfono al costado de la cama, cargando su batería para el día siguiente, resulta que el smartphone ha sido

hackeado y alguien está utilizando su capacidad de procesamiento para llevar adelante actividades de minería, produciendo así un rédito en criptomonedas que luego podrá ser canjeado por bienes, servicios o incluso monedas de curso legal.

Naturalmente, con el tamaño y la implicancia del objeto víctima de un ciberataque, concurre una exponencial capacidad de daño. Recordemos que las criptomonedas, partiendo de la base de que son una forma de financiamiento prácticamente imposible de rastrear, pueden formar parte de un ciberataque desde la concepción llana y simple de una forma de pago.

V. INTERVENCIÓN DE LOS ESTADOS Y DERECHO COMPARADO

Haciendo un muy breve resumen en atención a la extensión del presente artículo y a la constante variación de la normativa internacional al respecto, podemos decir que:

Bolivia se ha convertido en el primer país americano en prohibir explícitamente el uso de criptomonedas. En este sentido, el Banco Central de Bolivia, el 6 de mayo de 2014, emitió la Resolución 044/2014 que en su art. 1 indica:

> A partir de la fecha queda prohibido el uso de monedas no emitidas o reguladas por estados, países o zonas económicas, y de órdenes de pago electrónicas en monedas y denominaciones monetarias no autorizadas por el Banco Central de Bolivia en el ámbito del sistema de pagos nacional. (Marty, 2014)

Esta autora señala también que:

> El documento, firmado por el directorio del Banco Central, explica que esta resolución, como todas las realizadas por esta entidad, tienen como objeto 'procurar la estabilidad del poder adquisitivo interno', y que con ese fin se llevan a cabo las políticas monetarias. (Marty, 2014)

Aunque, sin embargo, también contempla la posibilidad de que estos criptoactivos sean precisamente un resguardo de los eventuales desequilibrios monetarios que los Estados pueden ejecutar —en algunos casos— de manera voluntaria para perseguir diversos objetivos.

Brasil es uno de los tantos países que venían evaluando la regulación de estos activos y, finalmente, este año la Receita Federal do Brasil dictó la Instrução Normativa N° 1888/2019, cuyos efectos no habían comenzado a ser obligatorios al momento de escribir este artículo, pero sí debieran serlo al momento de la publicación de este trabajo, ya que a partir del mes de agosto de 2019, los brasileros deberán declarar sus operaciones de criptomonedas.

Esto no es un dato menor. Un estudio de abogados (Machado Meyers Advogados) cita la Consulta Pública RFB nº 6/2018, cuyo resultado indica, según la fuente citada, que el movimiento de estos activos durante 2018 fue de entre 18 y 45 billones de reales, solo en bitcoins (entre 4.7 y 12 billones de dólares aproximadamente).

El caso más controversial es el del gran gigante asiático, China, que supo liderar el mercado mundial de criptomonedas, hasta que en 2017 comenzó una categórica prohibición de venta anticipada de monedas, que se complementó con la prohibición del intercambio de yuanes por criptomonedas, impactando negativa y sustancialmente en el valor de estos activos y repartiendo su liderazgo, luego, entre Japón y Corea del Sur. Si bien el mercado espera que esta prohibición caiga de un momento a otro, no es menos cierto que la principal plataforma social y de pagos We Chat, en mayo de 2019, cambió su política de pagos, dejando de aceptar transacciones en criptomonedas por considerar dichas operaciones ilegales.

El análisis de la situación en España no puede hacerse con independencia de la Comunidad Europea, por lo que resumidamente diremos que si bien las Cortes Generales no han aprobado ninguna ley sobre las criptomonedas, es decir, que no existe regulación legal local de las monedas virtuales en la actualidad que provengan de este país, la realidad es que sí hay un marco normativo general. Por ejemplo, el Tribunal de Justicia de la Unión Europea (TJUE), en la sentencia de fecha 22 de octubre de 2015, asunto C-264/14. (Tribunal Superior de la Comunidad Europea, Sala Quinta, 2019), decretó que:

> … la divisa virtual de flujo bidireccional «bitcoin», que se intercambiará por divisas tradicionales en las operaciones de cambio, no puede calificarse de «bien corporal» en el sentido del artículo 14 de la Directiva del IVA, puesto que, como puso de manifiesto la Abogado General en el punto 17 de sus conclusiones, no tiene ninguna finalidad distinta de la de ser un medio de pago. (Tribunal Superior de la Comunidad Europea, 2019)

Finalmente, en sus conclusiones, la referida jurisprudencia indica en el punto 2 que:

> 2) El artículo 135, apartado 1, letra e), de la Directiva 2006/112 debe interpretarse en el sentido de que constituyen operaciones exentas del IVA con arreglo a dicha disposición unas prestaciones de servicios como las controvertidas en el litigio principal, consistentes en un intercambio de divisas tradicionales por unidades de la divisa virtual «bitcoin», y viceversa, y realizadas a cambio del pago de un importe equivalente al margen constituido por la diferencia entre, por una parte, el precio al que el operador de que se trate compre

> las divisas y, por otra, el precio al que las venda a sus clientes. (Tribunal Superior de la Comunidad europea, Sala Quinta, 2019)

En resumidas cuentas, el TSJ de la Comunidad Europea determina, mediante este fallo, que el empleo de la moneda bitcoin y, consecuentemente, las criptomonedas quedarán exentas del tributo del Impuesto al Valor Agregado (IVA).

Asimismo, en junio de 2018, se aprobó la Directiva 2018/843/UE, la cual será de obligatorio cumplimiento para los países miembros a partir del 10 de enero de 2020 y cuya finalidad es combatir el blanqueo de capitales. Además, determina la obligación de las sociedades intermediarias de criptomonedas de desarrollar medidas de diligencia debida, como la identificación de sus usuarios con un documento oficial de identidad. Siendo sujetos obligados los proveedores de servicios de cambio de moneda virtual en moneda fiduciaria y los proveedores de servicios de custodia de monederos electrónicos, entre otros. Debiendo informar las actividades sospechosas y restringiendo —al menos parcialmente— el anonimato que permiten las criptomonedas. (Parlamento de la Unión Europea y Consejo, 2019).

Lo anteriormente mencionado, como hemos dicho, son ejemplos de las directrices europeas que condicionan el marco regulatorio de España, pero ya adentrándonos concretamente en este país podemos tomar como referencia las disposiciones de la Agencia Estatal de Administración Tributaria que, ya en enero de 2018, publicó en el *Boletín Oficial de España* un Plan de Control Tributario y Aduanero, donde se establecen directrices para el control de modelos de negocio por internet y pagos a través de medios como los monederos electrónicos.

Las obligaciones establecidas varían según el tipo de transacción y los beneficios por el intercambio de criptomonedas, debiendo también ser declaradas y tributar en su carácter de patrimoniales. Por lo que beneficios y pérdidas obtenidos en las operaciones de compra y venta de estos activos tributarán como ganancia o pérdida patrimonial en el IRPF, tomando como modelo los criterios de valoración de las operaciones con acciones. Recientemente y en igual sentido, el 20 de junio de 2019 el tribunal supremo, a través de su Sala de lo Penal, mediante Sentencia núm. 326/2019 al Recurso casación /998/2018, manifestó expresamente que las criptomonedas, en este caso bitcoins, no son en modo alguno dinero; también afirmó que se trata de "un activo patrimonial inmaterial".

En cuanto a la minería de criptomonedas hay obligación de

darse de alta en el Impuesto sobre Actividades Económicas, asimilando las actividades relacionadas con criptomonedas a las propias de los servicios financieros.

Por su parte, Estados Unidos ha publicado el 9 de mayo de 2019, a través de la Red de Control de Delitos Financieros de Estados Unidos (FinCEN), una guía de interpretación que incluye una parte importante de los modelos de negocios con criptomonedas, dentro de la Ley de Secreto Bancario (BSA), estableciendo pautas necesarias para cumplir con la política conocida como "KYC", por sus siglas en inglés, que se traducen en "conozca su cliente". Esto afectaría a casas de cambio y aplicaciones que trabajen con transferencias de dinero, y la finalidad es principalmente el control de ciertas personas o empresas que puedan estar bajo sospecha para las autoridades de ese país.

Rusia, por su parte, ya tiene proyecto de ley desde el 2018, que fue aprobado en su primera lectura y, posteriormente, pese a tener el apoyo total del ejecutivo, ha debido dar un pequeño paso atrás, ya que el Grupo de Acción Financiera Internacional (GAFI) le solicitó que ampliara su proyecto legislativo, ya que este omitía temas centrales como la minería, por ejemplo. Razón por la que ha vuelto a la primera lectura. Se espera que Rusia respete las indicaciones del GAFI, ya sea en el actual proyecto de ley o complementando este proyecto con otro nuevo en el corto plazo. Sin embargo, la agencia rusa Fontanka informó en su portal, el pasado 16 de mayo de 2019, que el primer ministro ruso, Dmitry Medvedev, ha manifestado que este tema no es una prioridad para el Gobierno ruso y que el motivo de esta situación es la pérdida de popularidad de las criptomonedas en ese país.

Por otro lado, en Venezuela, donde se ha llegado a arrestar en 2017 a varias personas que realizaban explotaciones de "minería" por legitimación de capitales, enriquecimiento ilícito, delitos informáticos, financiamiento al terrorismo, fraude cambiario y daños al sistema eléctrico nacional, a partir del 9 de abril de 2018, por medio de decreto, la Asamblea Nacional Constituyente legalizó toda existencia y creación de todo criptoactivo, incluyendo al "petro". También permite que cualquier persona natural o jurídica, privada o pública, pueda publicar su propio "Libro Blanco", siendo el primer paso para iniciar el proceso de registro y control de la nueva criptomoneda a crear ante el Ejecutivo nacional. Así mismo, se ordena a todos los entes del Estado a preparar su estructura burocrática a fin de recibir y pagar con las

criptomonedas que estén debidamente registradas.

VI. CONCLUSIONES

- A nivel práctico, las criptomonedas juegan un rol superlativo en cuanto a transacciones se refiere. Se producen intercambios con un alto nivel de seguridad, dentro de un marco transparente por su código abierto (caso Bitcoin), los cuales tienen un cortísimo plazo de acreditación y no reconocen fronteras. Por si esto fuera poco, el dinero de las comisiones va en parte a usuarios que facilitan el control de las transacciones, y la única manera de modificar los protocolos del sistema es, ni más ni menos, que con el acuerdo necesario de todos los usuarios. Poco más se les podría pedir.

- Con relación a la legalidad, evidentemente dependerá de cada Estado, entendiendo que es tal la magnitud del impacto que han tenido estas monedas electrónicas que, eventualmente, terminará por normalizarse legislativa o jurisprudencialmente en la inmensa mayoría de los países. (https://www.fontanka.ru/2019/05/15/073/)

- En cuanto a la legitimidad, es realmente dudosa. ¿Cuál es el objeto de hacer una herramienta comercial que favorezca y permita el anonimato si se pretende cumplir con las normativas de cada Estado? ¿Cuál es el objetivo de generar una red punto a punto, donde se manejan enormes cantidades de dinero y en la que no exista un responsable por las operaciones? Uno se pregunta si es posible que, al momento de desarrollar el sistema, puede haberse omitido el hecho de que trasladar bienes susceptibles de apreciación pecuniaria de un Estado a otro y sin posibilidad de control por parte de los Estados infringiría necesariamente sus normativas.

- Cabe concluir que, aun cuando los Estados puedan permitir su uso, es difícil creer que estas criptomonedas hayan sido desarrolladas con la mira en actividades lícitas. Por otro lado, hemos dicho que su practicidad resulta extraordinariamente conveniente. Pareciera que la mejor alternativa viable será considerar la posibilidad de una reglamentación paulatina, que ya han comenzado algunos Estados y que, progresivamente, se promueva la unificación y complementación de las diferentes normativas. Un

ejemplo de avance, en este sentido, es el consorcio desarrollado para averiguar cómo aprovechar la cadena de bloques en los sistemas financieros tradicionales. Uno de los primeros problemas de la aplicación de este esquema es el anonimato que proporciona el diseño de la cadena de bloques, algo que han resuelto con el llamado "libro de contabilidad autorizado" (*permissioned ledger*), una variante muy peculiar de la cadena de bloques de bitcoin, por ejemplo, que sí identifica a los usuarios que añaden bloques y que hace que las transacciones del sistema solo puedan consultarse por ciertas partes.

Como una última conclusión, y posiblemente la más relevante, es que las criptomonedas no pueden escapar de la vista de los Estados. Hablamos de un sistema que permite desde defraudaciones tributarias y hackeos de celulares, para la obtención de créditos por minería utilizando procesadores ajenos, hasta el financiamiento del terrorismo de manera inmediata y anónima. Por eso entendemos que su regulación no es solo conveniente, sino extremadamente necesaria.

VII. *DE LEGE FERENDA*

Ha quedado claro que difícilmente estas monedas hayan sido creadas con objetivos legítimos y en muchos casos resulta dudosa incluso su legalidad, pero suponiendo que se sortearan esos obstáculos y que quedará en cada uno la responsabilidad por sus actos, lo cierto es que las criptomonedas tienen un valor pecuniario y, por lo tanto, pueden ser objeto de derecho. Entonces, la segunda cuestión es cómo debiera regularse su utilización y, en caso de que tributen, la otra gran pregunta es a quién. Supongamos que, en un avión de American Airlines, sobrevolando algún país de Sudamérica, desde un celular con conexión satelital, transfiero dos millones de dólares (en criptomonedas) a España. ¿Corresponde tributar en algún país?, ¿en todos?, ¿debe tributar el que recibe el dinero o el que lo envía?, ¿cómo se establece el precio de las criptomonedas a los fines de grabarlos impositivamente?, ¿qué tributos, tasas o impuestos deben grabar estos bienes?

Muchas preguntas y pocas respuestas. En principio la recomendación de este capítulo es seguir el concepto de que quien dispone del objeto, en este caso criptomonedas, debe tributar según corresponda en la jurisdicción desde donde se realiza el acto de disposición. Es decir que, si bien las criptomonedas no

están en un lugar específico, sino en un complejo software; también es cierto que, en el ejemplo del párrafo anterior, la disposición se estaría efectuando desde la jurisdicción de los Estados Unidos, por ser la bandera de la aerolínea. Por esta razón entenderíamos —según esta recomendación— que deberían realizarse las declaraciones pertinentes: pago de impuestos y justificación de ingresos, según la normativa de ese país para criptomonedas y por el acto de la transferencia, con independencia de los tributos que correspondan a las personas en sus respectivos países, por las criptomonedas como activos patrimoniales por el período que hayan poseído estos dentro de su patrimonio.

Seguramente, distintos países tendrán diversa normativa al respecto. En algunos países se tendrá que justificar el origen del capital de manera más rigurosa, en otros será más alta la tasa impositiva por disponer del capital, etcétera. Sin embargo, resultaría posible y deseable que los países y bloques económicos pudieran acordar —al menos— las pautas de qué jurisdicción deban ser aplicables para que resulte posible hacer uso de esta herramienta sin que se defraude a la administración pública y, también, se elimine el anonimato que conlleva una motivación para el movimiento de capitales provenientes o destinados a actividades ilícitas por estos medios. De esta manera podría preservarse una fuente de trabajo (mineros), una herramienta eficiente, rápida y económica para el movimiento de capitales y a su vez salvaguardar la buena práctica, la razonabilidad y, sobre todo, transformar este sistema en una herramienta legítima y legal.

VIII. FUENTES DE CONSULTA

Cristensen, K. D. (2004). "La piratería informática en el ciberespacio: Recursos jurídicos y tecnológicos para combatirla". En Cabanellas De Las Cuevas, G. *Derecho de Internet*. Buenos Aires: Heliasta.

Ethgasstation. (16 de JUNIO de 2019). *ETH GAS STATION*. Obtenido de HTTP://ethgasstation.info

Perrit, H. H. (2004). "Internet ¿Una amenaza para la soberanía?" En Cabanellas De Las Cuevas, G. *Derecho de Internet*. Buenos Aires: Heliasta.

Real Academia Española. (21 de JULIO de 2019). *Real Academia Española*. Disponible en www.rae.es

Tribunal Superior de la Comunidad Europea, Sala Quinta. (22 de Julio de 2019). *Infocuria*. Disponible en http://curia.europa.eu/juris/document/document.jsf?docid=170305&doclang=ES

Marty, B. (10 de julio de 2014). "Bolivia, el primer país americano en prohibir el Bitcoin". En *Panam Post. Noticias y análisis de las américas*. Disponible en https://es.panampost.com/belen-marty/2014/06/19/bolivia-el-primer-pais-americano-en-prohibir-bitcoin/

Cómo publicar en

REVISTA MEXICANA DE CIENCIAS PENALES

REVISTA MEXICANA DE CIENCIAS PENALES publica artículos que son el resultado de investigaciones científicas originales sobre ciencias penales y, en especial, acerca de la reflexión, el estudio y análisis del sistema acusatorio adversarial y el cambio cultural que este implica para la construcción de una cultura de la legalidad. Los trabajos deberán ajustarse a los siguientes lineamientos:

ENVÍO ELECTRÓNICO

Los trabajos deben entregarse en formato Microsoft Word, en letra Times New Roman de 12 puntos, con interlineado de 1.5, en hoja tamaño carta, con márgenes superior e inferior de 2.5 cm, y derecho e izquierdo de 3 cm, a la dirección: publicaciones@inacipe.gob.mx

ESPECIFICACIONES

Los documentos deberán ser colaboraciones originales que no hayan sido publicadas en ningún otro medio. Asimismo, incluirán, en su primera página, título, índice, resumen analítico (de 100 palabras aproximadamente) y 4 palabras clave; en relación con el autor o autores, se incluirá su nombre completo, adscripción institucional y correo electrónico. El texto deberá ser como mínimo de 10 cuartillas y no debe rebasar las 25, tomando en cuenta las características del formato señaladas en el punto anterior. Esta extensión, en casos extraordinarios, puede variar dependiendo de las observaciones en el dictamen correspondiente o del acuerdo entre el autor y el Comité Editorial. Las referencias bibliográficas de los artículos deberán apegarse a las normas ISO 690:2010, consultables en https://www.iso.org/standard/43320.html

CALENDARIO

La fecha límite para la recepción de las colaboraciones será dos meses antes de la temporalidad de la publicación, por lo tanto, al ser *Revista Mexicana de Ciencias Penales* una revista trimestral, la cual comprende los periodos de enero a marzo, de abril a junio, de julio a septiembre y de octubre a diciembre, los trabajos se recibirán en noviembre, para el primer número anual; en febrero, para el segundo; en mayo, para el tercero, y en agosto para el último número del año.

PROCESO DE DICTAMINACIÓN

Los trabajos se someterán a la evaluación del Comité Editorial siguiendo el sistema doble ciego. Los autores recibirán información de la eventual aceptación o rechazo de sus colaboraciones mediante el resultado del dictamen, el cual puede ser "publicable", "no publicable" o "publicable con observaciones". Dicha información se hará llegar a los autores un mes antes de la periodicidad de la revista, esto es, en diciembre, para el primer número anual; en marzo, para el segundo; en junio, para el tercero, y en septiembre, para el último número del año. La inclusión de los originales aceptados queda sujeta a la disponibilidad del correspondiente número de la publicación.

DERECHOS

Es condición indispensable para la revista que el autor o autores cedan en exclusiva los derechos de reproducción. Si acaso surgieran peticiones del autor o de terceros para la reproducción o traducción completa o parcial de los artículos en otros medios o publicaciones, será competencia del Comité Editorial la autorización de dicha solicitud. En este sentido, se deberá indicar que la obra ha sido publicada previamente en el correspondiente número de la revista.

DOMICILIO POSTAL

Los artículos podrán ser entregados, de igual modo, en respaldo impreso y en archivo electrónico (en un disco) a la siguiente dirección postal: calle Magisterio Nacional número 113, colonia Tlalpan Centro, Alcaldía de Tlalpan, C.P. 14000, Ciudad de México.