Revista de la Facultad de Derecho de México
Tomo LXXIV, Número Especial 2024
DOI: http://10.22201/fder.24488933e.2024.e.87552

Avances legislativos de la ciberseguridad como derecho en México

Legislative advances of cybersecurityas as a right in Mexico

Rodolfo Guerrero Martínez*

Resumen: El presente artículo enfatiza la necesidad de considerar a la ciberseguridad como derecho en el contexto de la revolución digital considerando la seguridad de toda persona ante las amenazas y los riesgos a los que se exponen en el ciberespacio, derivados del desconocimiento y las afectaciones que ello ocasiona. Brinda además la posibilidad de generar estrategias clave, así como una legislación especial para crear un estado que goce de ejes transversales que tutele la seguridad informática y la protección de los datos personales de la sociedad.

Palabras clave: derecho; ciberseguridad; datos; legislación; estrategia.

Abstract: This article emphasizes the need to consider cybersecurity as a right in the context of the digital revolution, considering the security of every person in the face of the threats and risks to which they are exposed in cyberspace, derived

* Abogado por la Benemérita Universidad de Guadalajara y maestro en derecho con orientación en materia constitucional y administrativo por la misma casa de estudios. Socio fundador y representante legal de la Sociedad Civil Coffee Law. Titular de la Comisión de Legaltech del Ilustre y Nacional Colegio de Abogados de México A.C., Capítulo Occidente. Contacto: <rodolfo.gmartinez@academicos.udg.mx>. ORCID ID: 0000-0003-4943-374X. Fecha de recepción: 22/04/2024. Fecha de aprobación: 22/08/2024.

DOI: http://10.22201/fder.24488933e.2024.e.87552

from ignorance and the effects that this causes. It also provides the possibility of generating key strategies, as well as special legislation to create a state that has transversal axes that protect computer security and the protection of society's personal data.

Keywords: Law; Cibersecurity; Data; Legislation; Strategy.

La dignidad humana es la consagración de los derechos del hombre.

Sergio García Ramírez

I. Introducción

Actualmente las comunicaciones y relaciones sociales se dan a través de los diversos dispositivos electrónicos dentro de un entorno virtual; lo cual, si bien acorta distancias y permite gozar de acceso a una cantidad infinita de contenido en solo segundos, al mismo tiempo representa un grave riesgo para la seguridad de los ciudadanos y una constante amenaza a sus derechos humanos. Asimismo, existe una delgada línea entre la respuesta que brinda el Estado para la protección a la seguridad en el entorno virtual y la simultánea vulneración o indebida limitación a los derechos humanos, tales como la privacidad, la intimidad y la no intervención de comunicaciones privadas, entre otros, que paradójicamente en lugar de brindar soluciones de las amenazas presentadas en el ciberespacio, genera nuevas opciones de riesgos para los usuarios.

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

En el presente artículo tenemos como finalidad realizar diversas aproximaciones a través de reflexiones, comentarios, análisis breves de documentos, reportes, guías, informes e iniciativas legislativas de la ciberseguridad como derecho para generar un impacto positivo en la sociedad.

II. El derecho, la naturaleza de internet y los retos de la cuarta revolución industrial

El contexto de la era digital, donde el impacto de las Tecnologías de la Información y Comunicación (TIC) ha generado que los usuarios de internet en el planeta aumenten un 4%[1], lo cual representa 62,5% de la población mundial (es decir, 7.910 millones de personas). Sin embargo, existe una ausencia critica de seguridad de software que impacta en más de 100 intentos para explotar la vulnerabilidad a cada minuto (Informe de riesgos globales 2022 del Foro Económico Mundial[2]); lo cual enfatiza lo valioso de alfabetizar digitalmente, y por otra parte advierte la dependencia tecnológica al no poder concebir la vida diaria sin la tecnología –telefonía, redes informáticas, internet, radionavegación, geolocalización y telemetría–, ante las bondades que ofrece para comunicarnos y en el desempeño de nuestras funciones laborales, profesionales, escolares, entre otras. En ese marco resulta primordial la aplicación del Derecho, que evoluciona con el desarrollo y los procesos de producción industrial de las sociedades, lo cual demanda el ejercicio de nuevas áreas jurídicas como el Derecho de Telecomunicaciones, Derecho Informático y Derecho Digital.

En 1969 se creó una red de equipos informáticos interconectados, que ilustra el significado de la palabra Internet (interconnected networks o redes interconectadas), posteriormente en años ochenta se generó el *World Wide Web* (www), y en ese momento inicio la incorporación de usuarios privados al internet, otorgando acceso al sector económico y comercial. En el caso de

[1] We are social, Digital Report *"El Informe sobre las tendencias digitales, redes sociales y mobile",* Madrid, 2022. Consultado en: <https://wearesocial.com/es/blog/2022/01/digital-report-2022-el-informe-sobre-las-tendencias-digitales-redes-sociales-y-mobile/>.

[2] WEF, Informe de riesgos globales, 2022. Recuperado a partir de: <https://www.zurich.cl/-/media/project/zwp/chile/docs/grr22_executive-summary-esp.pdf>.

México, en 1989 el Instituto Tecnológico y de Estudios Superiores de Monterrey (ITESM) se convirtió en la primera institución de habla hispana en contactarse a internet. En aras de su regulación se reconocen conceptos como derecho de Internet y derecho en Internet que enfatizan una disciplina jurídica autónoma para controlar y regular la informática; y el tratar los derechos y obligaciones nacidos del tráfico jurídico consecuencia de la interacción en la Red.

Precisamente lo anterior reconoce los efectos de la Cuarta revolución industrial, término que tiene origen en Alemania en el año 2011[3], donde explica los efectos virtuosos de las TIC y el impacto de los procesos de producción en el diseño de la industria del futuro[4], comprendiendo que las tecnologías de la información son el último eslabón de la cadena de inventos humanos que va desde el lenguaje hablado, la escritura y la imprenta, hasta nuestros días. El ser humano inventa una tecnología, sea un instrumento material o conceptual, y está de vuelta, lo transforma a él. Podemos encontrar entre pilares y megatendencias[5] en el marco de la industria 4.0

a) *Físicas*: Vehículos autónomos, impresión 3D, robótica avanzada y nuevos materiales.

b) *Digitales*: Permite que todas las cosas tangibles del orbe sean susceptibles de conectar por mandos digitales, tenemos el caso de la materialización digital con el uso de *blockchain*, por ejemplo, entiendolo como un protocolo de registro seguro, ya que facilita que personas no conocidas puedan colaborar entre sí, sin la necesidad de un intermediario que brinden una validación central.

---

3 Hace referencia a una política económica gubernamental basada en estrategias de alta tecnología.

4 Sáez Vacas, Fernando, "Propuesta personal, basada en la SocioTecnología de la Información y la Cultura: Conviene desarrollar una inteligencia Tecnosocial", *Revista Telos*, España, núm. 73, 2007.

5 Schwab, Klaus, *La Cuarta Revolución Industrial*, Madrid, Debate, 2016.

DOI: http://10.22201/fder.24488933e.2024.e.87552

c) *Biológicas*: Mediante las áreas de biología y genética se han realizado avances en la investigación médica que permite visualizar la impresión 3D de órganos humanos.

Adicionalmente, el fenómeno de la realidad aumentada,[6] definido como una visión directa o indirecta de un entorno físico del mundo real, cuyos elementos se combinan con elementos virtuales para la creación de una realidad mixta en tiempo real.

Por otra parte, debemos considerar que el Derecho y los operadores jurídicos requieren comprender la naturaleza del internet y los retos de la cuarta revolución industrial; ya que sin ello no podemos gozar de seguridad y protección de nuestros datos al utilizar el internet y la tecnología ante los servicios que nos ofrecen y brindan el sector público (sujetos obligados) y privado (empresas). Este último creando nuevos modelos de negocios con la hiperconectividad, el *big data*, sistemas ciberfísicos, industria inteligente[7] como lo mencionan diversos expertos en materia de innovación de procesos comerciales y gestión del conocimiento e inteligencia artificial.[8]

Ahora bien, estableciendo las bases conceptuales y alguna referencias históricas importantes, el objeto de estudio que relaciona la ciberseguridad y el derecho nos permite visualizar con mayor precisión el tópico denominado como *Cybersecurity Law*[9], comprendiendo al conjunto de acciones de política pública, re-

---

6 González, Óscar, *Educación aumentada. Centro de conocimiento de tecnologías aplicadas a la educación*, 2013, p.19.

7 Justamente, la colecta de datos generados por los diferentes elementos de la cadena de producción permite igualmente producir una réplica virtual de la totalidad o de parte de esa cadena.

8 Davenport, Thomas, *Big Data at Work*, Boston, Harvard Business School Publishing, 2014.

9 Comprende un conjunto de doctrinas que podrían no coincidir entre los antiguos conceptos de negligencia y el contrato del derecho consuetudinario; prohibiciones de principios del siglo XX de prácticas comerciales desleales y engañosas; delitos que refieren transgresión; legislación; directrices

gulación, normas técnicas, culturales y colaboración de distintos actores y sectores (entes públicos, sector privado, academia y comunidad técnica y sociedad en su conjunto) que tiene como principal objetivo:

- Promoción y fortalecimiento de los derechos y garantías tanto en el ámbito físico como en el ciberespacio, teniendo como base la seguridad de la información: Busca la confidencialidad, disponibilidad e integridad de la información; el modelo de gobernanza que contribuya al desarrollo sostenible de las naciones y coadyuvar a que la convivencia social sea más segura, confiable y resiliente.

En ese sentido, a medida que el creciendo digital y tecnológico otorgan mayor facilidad y velocidad a las organizaciones para la generación de datos, su almacenamiento y tratamiento en general, surge un gran reto para que el Derecho replante su diseño en las libertades y obligaciones de las personas físicas y morales ante el fenómeno de transmisión, portabilidad y proporción de los datos en el marco de la cuarta revolución industrial. Justamente en esa lógica, la ciberseguridad prioriza considerarse como derecho.

III. La ciberseguridad como derecho

La Asociación de Auditoría y Control sobre los Sistemas de Información (ISACA) nos señala que la ciberseguridad es la protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados.

No obstante, la ciberseguridad no solo debe ser entendida como un concepto técnico que sea enfocado para un ingeniero

de agencias no vinculantes; reglamentos; estándares de la industria; ley de seguridad nacional; y derecho.

DOI: http://10.22201/fder.24488933e.2024.e.87552

o especialista de área informática sino para toda persona y que se comprendido como derecho humano de última generación o derecho digital. En esa lógica, la Carta de los Derechos Digitales 2021 publicada por el Gobierno Español se nos dice que la Ciberseguridad es conforme al ordenamiento jurídico

> el derecho al que toda persona tiene a que los sistemas digitales de información que utilice para su actividad personal, profesional o social, o que traten sus datos o le presten servicios, posean las medidas de seguridad adecuadas que permitan garantizar la integridad, confidencialidad, disponibilidad, resiliencia y autenticidad de la información tratada y la disponibilidad de los servicios prestados […]

No obstante lo anterior, existe preocupación de la comunidad internacional en relación a la imperiosa necesidad de brindar respuestas integrales con pleno respeto a los derechos humanos de los usuarios[10], evitando repercusiones comparables a la confrontación militar tradicional, ya que si bien las amenazas ponen en peligro a los usuarios, es necesario que exista una cooperación entre los usuarios del ciberespacio, con la finalidad de evitar optar por posibles respuestas, que lejos de resolver el problema de la vulneración a los derechos humanos en el entorno virtual, lo agravan, vulnerando de la misma forma los derechos humanos de los usuarios.

Añadiendo el interés de fortalecer lo señalado, en el contexto de América Latina, encontramos organismos en el caso de Argentina[11] desde el año 2011 la elaboración de registros de incidentes y amenazas de ciberseguridad a través del Programa Nacional de

[10] Carlini, Agnese, "Ciberseguridad un nuevo desafío para la comunidad internacional", *Boletín I.E.E.E.*, abril-junio, núm. 2, 2016, pp. 950-966.

[11] Argentina creó el primer Computer Security Incidente Response Team CSIRT nacional en 1994. Recuperado a partir de: <https://csirt.minseg.gob.ar/>.

Infraestrcutura Críticas de Información y Ciberseguridad ICIC e ICIC – CERT (Centro Nacional de Respuesta a Incidentes Informáticos). Por otra parte, observamos en Brasil, la oficina para la represión de la Delincuencia cibernética de la Policía Federal como la principal entidad facultada para investigar los delitos cibernéticos y cuenta con laboratorio forense digital.

Además, localizamos diversos documentos como guías e informes, que priorizan a la ciberseguridad como factor de la tutela de los datos y los derechos de la privacidad, por esa razón se generan y/o elaboran lo siguiente

- Guía de Ciberseguridad de la *Law Society of Scotland* (Sociedad de Abogados de Escocia)[12] con el fin de ofrecer información de amenazas y áreas de riesgo, las consecuencias de una infracción, soluciones y respuesta a incidentes.

- Guía de Ciberseguridad de la Unión Internacional de Telecomunicaciones ITU (2018) que entre sus puntos nos enfatiza la elaboración de la estrategia nacional de ciberseguridad y que permita identificar posibles formas de proceder, incentivar los esfuerzos de ejecución; y efectuar la atribución de los recursos necesarios para hacer posibles todas las actividades.

- Informe anual del Programa de Ciberseguridad y privacidad del Instituto Nacional de Estándares y Tecnología NIST describe las actividades dentro de ocho áreas prioritarias (1. Estándares criptográficos y validación; 2. Medición de Ciberseguridad; 3. Educación y fuerza laboral; 4. Gestión de identidad y acceso; 5. Ingeniería de privacidad; 6. Gestión de riesgos; 7. Redes confiables; y 8. Plataformas confiables) establecidas por el Laboratorio de Tecnologías de la Información ITL y trabajas en coordinación con entidades del sector público y privado.

[12] Law Society of Scotland. Guide to cybersecurity, 2021. Recuperado a partir de: <https://www.lawscot.org.uk/media/371188/lss-cybercrime-with-new-section-v6.pdf>.

DOI: http://10.22201/fder.24488933e.2024.e.87552

En México, el área de ciberseguridad está completamente desregulada para el sector privado y no existe un organismo o agencia especializada encargada de regular aspectos relacionados con la seguridad de la información de las empresas cuando, por ejemplo se vulnera algún sistema que afecte la provisión de bienes y servicios al ciudadano como existe por ejemplo en España, a través del Instituto Nacional de Ciberseguridad de España INCIBE y el Centro Criptologico Nacional (CCN) o en Alemania a través de la Oficina Federal para la Seguridad de la Información (*Bundesamt für Sicherheit in der Informationstechnik* BSI). Sin embargo, resulta importante resaltar el desarrollo del marco jurídico para la integración de la ciberseguridad en México.

A) Antecedentes del avance legislativo en Ciberseguridad en México

12 de abril de 2005: Iniciativa que reforma, adiciona y deroga diversas disposiciones del código penal federal, del código federal de procedimientos penales, de la ley federal contra la delincuencia organizada, y de la ley de la policía federal preventiva, en materia de delitos cibernéticos y de delitos contra menores	28 de marzo de 2012: Proyecto de decreto por el que se reforman y adicionan diversas disposiciones al código penal federal en materia de delitos en contra de medios o sistemas informáticos.	22 de octubre de 2015: Iniciativa con proyecto de decreto por el que se expide la Ley Federal para prevenir y sancionar los Delitos Informáticos.	10 septiembre 2019: Iniciativa que reforma y adiciona diversas disposiciones de la ley federal de protección de datos personales en posesión de los particulares.	01 de septiembre de 2020: Se expide Iniciativa de Ley General de Ciberseguridad.

Fuente: Elaboración propia.

Entonces, destacamos el hecho de que la ciberseguridad en un principio se ocupara de proteger la información de forma reactiva y actualmente, se considere que tienen una posición proactiva, esto es a través de la identificación y gestión de riesgos que amenazan a los usuarios en el uso del ciberespacio[13]. Y comprendemos entre sus objetivos principales:

1. La cadena de suministro: Debe garantizar la inclusión de aquellas terceras partes que participan de forma importante en el negocio y cada uno de sus procesos. Adicionalmente extender el marco de aplicación y de control a otros actores y proveedores, integrando a las evaluaciones las licitaciones, contratos y relaciones con terceros en materia de ciberseguridad.

2. El Cumplimiento: Aplicar adecuadamente la integración de la normativa vigente junto a las directrices transicionales, de buenas prácticas o estándares de la industria. Entiendo además que la relación con los responsables es fundamental para generar un programa de ciberseguridad de una compañía u organización.

3. La Valoración del negocio o business valuation: La reputación es el activo más valioso y complejo, sin embargo, la ciberseguridad puede contribuir para su protección. En ese sentido, las capacidades de ciber-resilencia son relevantes para la valoración de una organización.

4. Análisis de datos y de la información: Las funciones de la ciberseguridad fortalecen el proceso de la recopilación, tratamiento, evaluación y consolidación de información en tiempo real. Precisamente, lo anterior comprende datos de los clientes, empleados, de los sistemas y del negocio.

[13] Fojón Chamorro, Enrique y Sanz Villalba, Ángel F., "Ciberseguridad en España: una propuesta para su gestión", *Boletín Elcano*, 2010, pp. 1-8. Consultado en: <https://www.files.ethz.ch/isn/118153/ARI102-2010_Fojon_Sanz_ciberseguridad_Espana.pdf>.

DOI: http://10.22201/fder.24488933e.2024.e.87552

B) Seguridad de la Información para las Versiones Públicas para el Poder Judicial en México

En el Estado Mexicano se tienen diversas obligaciones para el Poder Judicial en el marco de hacer transparente y accesible la información, –pero también debe considerar la seguridad de la información (que no sigue siendo un gran problema)–. Esto acorde a la Ley General de Transparencia y Acceso a la Información Pública, por ejemplo, en su artículo 73 se nos señala como requisitos indispensables:

- Versiones públicas de todas las sentencias emitidas.
- Versiones estenográficas de las sesiones públicas.
- Los procesos por medio de los cuales fueron designados los jueces y magistrados.
- Lista de acuerdos que se publiquen diariamente.

Entonces, a partir de lo dicho, encontramos que una versión pública elimina la información clasificada como de acceso restringido en su modalidad de reservada o confidencial para permitir su acceso, lo cual comprende algunos datos como

- Datos identificativos: Nombre, domicilio, teléfono particular, celular, firma, clave del Registro Federal de Contribuyentes.
- Datos electrónicos: Correo electrónico no oficial, dirección IP[14], dirección MAC[15], así como el nombre de usuario y contraseña.
- Datos biométricos: Geometría de la mano, huella dactilar, ADN, características de iris y retina, tipo de sangre.

[14] Protocolo de Internet.

[15] Dirección Media Access Control o dirección de control de acceso al medio.

Por otra parte, localizamos otros datos que son susceptibles de supresión en el caso de nombre, pseudónimos, alias; el nombre de los quejosos o actores citados en los precedentes de las tesis jurisprudenciales y tesis aisladas que se invocan en la sentencia; todos los datos concernientes a menores; el número de registro de una patente o marca; los números de expedientes de primera instancia y en su caso del juicio o procedimiento del cual no se derive el acto impugnado[16].

Con respecto a la seguridad de la información, es indispensable garantizar que las versiones publicas desempeñadas por los Poderes Junciales locales fortalezcan e incluso replantean el actual sistema en que operan, el *Test Data*.[17]

Lo anterior, debido a que falta comprender e incorporar un sistema más efectivo respecto a los niveles de seguridad, tal y como se proponía con SARCOEM (Sistema de Acceso, Rectificación, Cancelación y Oposición de Datos Personales del Estado de México). En este sentido, el sistema protege los datos personales bajo tres niveles o capas de seguridad:

1. Nivel de seguridad: Se conforma por dos hardware, el primero es el *Fortywall* encargado de detener ataques, y el segundo es el *Firewall* el cual bloquea los ataques externos;

[16] Una versión pública es un documento en el que se elimina información clasificada como de acceso restringido en modo reservado o confidencial para permitir el acceso. Recuperado a partir de: <https://www.poderjudicialcdmx.gob.mx/unidadtransparencia/versiones-publicas/>.

[17] Es un software libre para uso como programa de escritorio de computadora, que asiste a los sujetos obligados en la elaboración de versiones públicas, con estricto apego a los "Lineamientos generales en materia de clasificación y desclasificación de información, así como para la elaboración de versiones públicas" emitidos por el Sistema Nacional de Transparencia, cuya labor es facilitar y homologar la eliminación de las partes o secciones con información clasificada como confidencial o reservada en los documentos públicos. Recuperado a partir de: <https://transparencia.guadalajara.gob.mx/Generador-de-Versiones-Publicas>.

2. Nivel de seguridad: Utilización del certificado HTTP, en donde la información que se envía a través de este dominio viaja encriptada;

3. Nivel de seguridad: Archivos que se envían están cifrados por el sistema desarrollado por el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios INFOEM, dicho cifrado constado de 512 caracteres (4,000 bits).

IV. Control y contemplación legal sobre materia de ciberseguridad en México

En la medida en que integramos el uso de las tecnologías digitales en todos los aspectos de nuestra vida diaria, incrementamos de forma exponencial el flujo de datos a través de redes y dispositivos, con lo que aumenta, en la misma medida, la exposición a riesgos, amenazas y ataques cibernéticos, representando un desafío sistemático para la seguridad de la información.

Entonces la ciberseguridad, se convierte en factor crucial para garantizar el acceso universal, fiable y equitativo, por lo que, en esta era digital, la confianza lo es todo[18], por ello, resulta valioso que las organizaciones evolucionen a la par de la transformación digital. El exhorto es dirigido a las organizaciones públicas y privadas, las cuales deben llevar a cabo acciones y desarrollar capacidades que permitan el uso y aprovechamiento de las TIC de manera responsable. En el caso de la esfera pública[19], permite repensar la institucionalización de un amplio dominio (considerando las

[18] Función de la UIT en el fomento de la confianza en la utilización de las TIC [en línea]. Disponible en: <https://www.itu.int/es/mediacentre/backgrounders/Pages/role-of-ITU-in-building-confidence-and-trust-in-the-use-of-ICTs.aspx>.

[19] Moya, Eugenio, "La emergencia del pronet@riado", *Revisión Crítica del Concepto Habermasiano de Esfera Pública. Revista de Filosofía*, vol. 37, núm. 2, 2012, p. 23.

tecnologías de la telecomunicación) logrando ir más lejos de un *counterpublic sphere*[20], lo cual crea además una cultura política de la red que facilitar las nuevas formas de participación de los sistemas de gobierno.

Entre las recomendaciones del Banco de Desarrollo Interamericano, señala que "Resulta indispensable reforzar la confianza en los servicios digitales de cara a incentivar la adopción de la banda ancha. Para ello, deberá garantizarse la protección de los consumidores, la gestión de riesgos de la seguridad digital y la protección de la privacidad." [21].

Por otra parte, el Estado Colombiano nos indica a través del documento CONPES[22] 3701 que la ciberseguridad es "la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos ante amenazas o incidentes de naturaleza cibernética".

En ese sentido, con la finalidad de promover una transición segura hacia la digitalización del país, el 13 de noviembre de 2017, el Gobierno mexicano presentó la Estrategia Nacional de Ciberseguridad, sin embargo, esta se ha quedado en el papel. Si bien, existen algunos esfuerzos por parte del Gobierno para contar con un marco normativo que promueva la seguridad digital, de acuerdo con el Reporte sobre Ciberseguridad 2020 del BID, México[23] se encuentra entre los países de América Latica que aún no cuenta con un marco legal sobre delitos informáticos y muestra un alarmante rezago en cuanto a regulación sobre seguridad. Actualmente,

---

20 Múltiples y superpuestas, esferas públicas dentro de las cuales aquellos excluidos o marginados por la esfera pública burguesa pueden hacerse oír.

21 OCDE/BID (2016), Políticas de banda ancha para América Latina y el Caribe: un manual para la economía digital, OECD Publishing, Paris. Consultado en: <http://dx.doi.org/10.1787/9789264259027-es>.

22 Consejo Nacional de Política Económica y Social.

23 OEA/BID (2020), Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe. Consultado en: <http://dx.doi.org/10.1787/9789264259027-es>.

localizamos en discusión cuatro iniciativas en el Congreso de la Unión que buscan crear leyes sobre ciberseguridad.

A) Consideraciones de ciberseguridad para el marco normativo

a) *Definiciones*. Actualmente, no existe consenso respecto a la definición de ciberseguridad y las iniciativas de ley sometidas al Congreso difieren entre sí al respecto. Al no ser la ciberseguridad un asunto exclusivo del Estado y al tratarse de un tema que repercute a nivel internacional, es importante que la definición de ciberseguridad considere definiciones propuestas o adoptadas en la agenda internacional. Esto debería aplicar, también a diversos conceptos utilizados en este tema, con lo que, además, se facilitaría para México la cooperación internacional en el futuro.

b) *Institución Responsable*. Con la finalidad de asegurar el cumplimiento de las Leyes, se hace necesaria la creación de una Institución con competencias, independencia y recursos suficientes para coordinar, implementar y dar seguimiento a los mecanismos de ciberseguridad.

c) *Cooperación*. A efecto de impulsar acciones integrales y de un impacto amplio, es preciso establecer los mecanismos de cooperación entre el sector público, el sector privado, la academia y demás actores de la sociedad. Esto permitirá promover espacios de discusión y cooperación que construyan un entorno digital más seguro.

d) *Tipificación*. Se debe disponer la obligación de tipificar en los diversos códigos penales (federal, estatal) el ciberdelito a través de sus diversas conductas (fraude, acceso ilícito, robo de identidad, robo de datos, etc.), así como las sanciones respectivas.

e) Procedimientos. Las leyes deben establecer las competencias y procedimientos para llevar a cabo las investigaciones y sanciones derivadas de su incumplimiento. Así mismo, deberán establecerse los procedimientos papara participar y adherirse a convenios in-

ternacionales, así como para cooperar con instancias internacionales (asistencia, extradición y compartición de información).

f) *Capacitación*. Las Leyes deben contemplar acciones enfocadas educar y concientizar a la población en materia de ciberseguridad. Esto, a través de instituciones educativas y medios de comunicación. Incluir la ciberseguridad en los planes de estudio de todos los niveles educativos tendría que ser obligatorio.

g) *Derechos Humanos*. Todas las disposiciones contempladas en las Leyes deberán tener un enfoque basado en el respeto irrestricto de los Derechos Humanos, anteponiendo, en todo momento el bienestar de la persona y la inclusión universal.

Precisamente el Estado Mexicano, a través de sus tres poderes y de sus instituciones autónomas (órganos constitucionales autónomos), debe poner como prioridad en su agenda la ciberseguridad, uniendo esfuerzos con los diversos actores de la sociedad; empresas, academia y sociedad civil, debido a que la ciberseguridad debe tratarse transversalmente.

Además, al tratarse de un tema de alcance global, es importante que las iniciativas que se discutan y aprueben en el Congreso, consideren ideas y conceptos acordados por otros países y organismos internacionales. Es decir, que sea un marco normativo sólido que procuré crear un entorno digital seguro y confiable en México para gozar de un proceso de idóneo de transformación digital.

V. Propuestas legislativas en materia de ciberseguridad en México

Es importante reflexionar sobre la importancia de implementar un control y regulación en materia de ciberseguridad en México, desde el rubro legislativo, tomando en cuenta el marco normativo actual, su alcance, limitaciones y área de oportunidad que surge

DOI: http://10.22201/fder.24488933e.2024.e.87552

de lo anterior para regular una materia trascendental en la presente época para la seguridad y economía del país.

Previo a referir las propuestas de reforma y/o iniciativa de ley sobre ciberseguridad, es preciso partir de la Constitución Política de los Estados Unidos Mexicanos CPEUM, la cual contempla en su artículo Tercero, Fracción V que "toda persona tiene derecho a gozar de los beneficios del desarrollo de la ciencia y la innovación tecnológica", y en su artículo Sexto, donde se establece que "el Estado garantizará el derecho al acceso a las tecnologías de la información y comunicación", lo cual en teoría se refuerza con el apoyo económico y operativo a la investigación e innovación científica, humanística y tecnológica. En tanto, la CPEUM es el primer parámetro para dar pauta a las leyes secundarias en la materia que regulen los aspectos específicos que conllevan la innovación tecnológica.

En ese orden de ideas, las leyes secundarias que regulan la materia, antes a entrar en la reflexión y propuestas de acción y regulación por medio de diferentes conceptos claves y demás elementos, en México cuenta con leyes que indirectamente dan pautas para combatir los delitos informáticos como son los Tratados Internacionales en materia de Derechos Humanos, el Código Penal Federal CPF, la Ley de Seguridad Nacional, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares LFPDPPP, la Ley General de Protección de Datos en Posesión de Sujetos Obligados LGPDPPSO, entre otras.

Estos ordenamientos ofrecen en su texto herramientas para combatir acciones que atenten contra la seguridad informática de las personas, desde aplicar sanciones y penas por relevar, divulgar, utilizar, modificar, destruir o provocar pérdidas indebidamente sobre información de terceros sin autorización y en su perjuicio, como el caso del Código Penal Federal que contempla el delito informático en su Capítulo II titulado Acceso ilícito a sistemas y equipos de informática en su artículo 211 bis 1 al 7 manifestándolo como "Al que sin autorización modifique, destruya o provoque

pérdida de información contenida en sistemas o equipos de informática del Estado […] (art. 211 bis 2)".

Así también considera aquellos actos tendientes a crear sistemas cuyo objeto sea crear sistemas informáticos cuya finalidad esté dirigida a dañar dispositivos electrónicos de protección de programas de cómputo, hasta dotar a los titulares de datos personales de herramientas, como los derechos acceso, rectificación, cancelación y oposición (ARCO) esto previsto en la LFPDPPP y que instruye que debe contender la solicitud en su artículo 29; y finalmente de establecer las bases de integración y acción coordinada de las instituciones y autoridades encargadas de preservar la seguridad nacional, en sus respectivos ámbitos de competencia, a nivel federal, estatal y municipal.

No obstante, en un mundo en donde la gran parte de los activos, datos personales, información privilegiada y recursos económicos se mueven en el espectro digital, es primordial contar con un marco legislativo específico sobre ciberseguridad, en virtud también de las limitaciones y lagunas legales de las leyes secundarias. Las limitaciones de las leyes secundarias no parece que sean "mayores", ya que representan un adelanto hacia una política pública que se interesa por la seguridad informática y el combate a la ciberdelincuencia. De manera tal, que las iniciativas propuestas en el tema señalado desarrollan el concepto de ciberespacio y la articulación para la aplicación del Convenio de sobre delitos cibernéticos o de Budapest, además de otros conceptos fundamentales, a continuación, resaltaremos algunos aspectos de últimos proyectos de ley presentados.

A) Aspectos de la Propuesta de Ley General de Ciberseguridad 2020

El primero de septiembre de 2022 el senador Miguel Ángel Mancera, coordinador del Grupo Parlamentario del Partido de la Revolución Democrática PRD presentó una iniciativa de Ley General de Ciberseguridad con la pretensión de realizar cambios

DOI: http://10.22201/fder.24488933e.2024.e.87552

al Código Penal Federal, a la Ley General del Sistema Nacional de Seguridad Pública, la Ley de Seguridad Nacional, entre otras. Entre otros detalles podemos resaltar:

- La creación del Centro Nacional de Ciberseguridad;
- Una comisión permanente de ciberseguridad en el interior del Consejo Nacional de Seguridad Pública, que se encargará de darle seguimiento al cumplimiento de las acciones del Centro Nacional de Ciberseguridad;
- La actualización del catálogo de cibercrímenes y sus penas.

Sin embargo, advertimos en un análisis brevísimo a la presente iniciativa que la creación de distintos delitos podría criminalizar la libertad de expresión en internet debido a:

La monitorización del servicio de internet por parte de los proveedores de este se contempla en el artículo 30 de dicha propuesta de ley, y abarca la vigilancia del tráfico y la difusión de información considerada prohibida, sin que se defina lo que se entenderá por "información prohibida".

> Artículo 30.- Los operadores de red gestionarán la información publicada por las personas usuarias y, al descubrir que está prohibida la publicación o transmisión, deberán detener inmediatamente la transmisión de esa información, evitar la difusión de la información, guardar registros e informar de forma inmediata a las autoridades competentes.

B) Aspectos de la Propuesta de Ley General de Ciberseguridad 2022

El día 6 de octubre, en la Gaceta Parlamentaria, se publicó una nueva propuesta de Ley General de Ciberseguridad, en este caso presentada por la Diputada Federal Juanita Mena Guerra del

Partido Movimiento Regeneración Nacional MORENA. En el documento podemos resaltar lo siguiente:

- Observancia general en todo el país.
- Legislación supletoria solo de seguridad, sin considerar ordenamientos existentes en ámbitos: financiero, propiedad intelectual, privacidad y educativo.
- Propone una definición de "ciberdelito" y la fundamenta refiriendo sólo al Código Penal del Distrito Federal, hoy Ciudad de México (CDMX), ignorando la reforma de 1999 al CPF, previsto en demás entidades federativas, así como en la legislación especial.
- Define TIC, ciberamenaza, ciberriesgo y vulnerabilidades orientando el tema sólo a infraestructura más no a información, lo cual en el contexto nacional actual debería de ser el principal bien jurídico a proteger.
- Define *pharming* de forma incorrecta, ya que este redirige tráfico web, no al tráfico de la red como señala la iniciativa con proyecto.
- Propone una Fiscalía Especializada en Ciberseguridad con Ministerios Públicos y jueces especiales en ciberseguridad.
- Para ser juez en la materia debes tener 5 años en litigio penal y en temas especializados con las TIC.
- Reitera la definición ciberdelito siendo que existe ya una conceptualización en el artículo 5, sin embargo, en el artículo 19 se menciona en sentido distinto.
- El Sistema Educativo que ante la discusión de la NOM237SE2020 señalo no tener competencia para atender temas de ciberseguridad, se indica que deberá si entender sobre ello.

C) Propuesta personal de Ley General de Ciberseguridad

La Propuesta de Ley General de Ciberseguridad que planteamos de forma general debe ser reglamentaria del artículo 21, y del artículo 6 en el párrafo tercero y en el párrafo cuarto del apartado B en su fracción I, de la Constitución Política de los Estados Unidos Mexicanos, es decir, se establece en la materia de seguridad pública en el ámbito del ciberespacio.

Precisamente, reconociendo que la seguridad pública, es una cualidad de los espacios públicos y privados, que se caracteriza por la inexistencia de amenazas que socaven o supriman los bienes y derechos de las personas y en la que existen condiciones propicias para la convivencia pacífica y el desarrollo individual y colectivo de la sociedad[24].

Ahora bien, por medio de nuestro objeto de estudio, establecemos una aproximación a la ciberseguridad como derecho, en la cual advertimos que la ley general en la materia tendrá entre sus disposiciones ser de orden público e interés social y de observancia general en todo el territorio nacional. Comprendiendo además, una serie de títulos que versen sobre las instancias de coordinación y distribución de competencia del Consejo Nacional de Ciberseguridad, recursos y fondos federalizados hasta instalaciones estratégicas.

VI. Conclusión general

Definitivamente los beneficios otorgados por la evolución de la tecnología son innumerables y esto nos debe obligar a conocer estas tecnologías de manera no sólo teórica/superficial sino prác-

[24] García Ramírez, Sergio, "En torno a la seguridad pública. Desarrollo penal y evolución del delito", en Peñaloza, Pedro José y Mario A. Garza Salinas (coords.), *Los desafíos de la seguridad pública en México*, Universidad Iberoamericana, UNAM-PGR-México, 2002, p. 81.

tica/ de fondo, para que la bondad de conectarnos y acceder a la información sea a favor y no en contra de nuestra convivencia, desarrollo y seguridad.

La ciberseguridad deberá ser un derecho fundamental primordial en el contexto de la revolución digital, que integre una serie de estrategias, metodologías y tecnologías para protegernos de amenazas tecnológicas. Además de considerar como pilar fundamental la educación de las generaciones actuales y futuras para tener un mejor estado, país y mundo con una eficaz mitigación de riesgos, logrando una ciberresilencia y el establecimiento de una política internacional coherente del ciberespacio con valores esenciales.

Actualmente lo nuevos modelos representan un gran desafío para el mundo jurídico ante la reconfiguración de los diseños normativos, así como nuevas propuestas como la de *Cibersecurity Law* que dote a las autoridades del seguimiento oportuno que evite las actuaciones de las redes criminales para acceder a los datos personales sensibles de los usuarios. Además, que contemple de forma idónea en los ordenamientos el tratamiento de datos y los derechos tanto en el espacio físico como digital.

En suma, en México es indispensable la generación de procesos homologados en su normativa para que ello permita disminuir de forma gradual el impacto de la delincuencia cibernética que a lacerado el patrimonio de un gran número de personas físicas y morales. Y que su vez establezca lo necesario para la transformación digital por medio de un replanteamiento al modelo actual con la incorporación tecnológica.

Cabe destacar, en estas últimas líneas que los aportes de grandes juristas son indispensables para los trabajos desarrollados en el presente artículo, de manera que, exhorto a seguir los aportes del ilustre jurista mexicano Sergio García Ramírez, referente en la materia de derechos humanos, derecho penal y seguridad pública que permitan apreciar y entender los escenarios de la disrupción tecnología bajo el crisol del derecho, procurando la paz, la justicia y la armonía para el Estado.