La Ciberseguridad en México y los derechos humanos en la era digital

Cybersecurity in Mexico and human rights in the digital age

Fuentes-Penna, Alejandro[1]

Gómez-Cárdenas, Raúl

González-Ibarra, Juan de Dios

Enviado: 23 de marzo de 2023

Aceptado: 09 de mayo de 2023

Resumen

A medida que nuestro mundo se digitaliza, las amenazas a la ciberseguridad se han convertido en parte de nuestra vida cotidiana. De manera constante, el gobierno federal, las empresas y los ciudadanos en México se enfrentan a miles de ciberataques, desde los más simples como correos electrónicos de phishing, hasta ataques más sofisticados contra los activos de datos más preciados de la nación. Así, la protección de ciberataques es una actividad cuya importancia se relaciona con el incremento de la digitalización de la información, en donde, a mayor cantidad de datos compartidos, es mayor la necesidad de protección. En este sentido, la ciberseguridad ha demostrado ser una inversión necesaria para los organismos públicos y las empresas. La tecnología ha proporcionado al gobierno nuevas formas de atender e interactuar con los ciudadanos, siendo indispensable crear un marco legal y soluciones de ciberseguridad adecuadas para garantizar que los organismos y los ciudadanos puedan cumplir sus misiones sabiendo que su información está protegida.

Palabras claves: Ciberseguridad, ciberdelitos, México, Derechos Humanos en la era digital.

Abstract

As our world digitizes, cybersecurity threats have become a part of our daily lives. On a constant basis, the federal government, businesses, and citizens in Mexico face thousands of cyberattacks, from the simplest like phishing emails to more sophisticated attacks against the nation's most precious data assets.

Thus, the protection of cyberattacks is an activity whose importance is related to the increase in the digitization of information, where the greater the amount of data shared, the greater the need for protection. In this sense, cybersecurity has proven to be a necessary investment for public bodies and companies.

Technology has provided the government with new ways to serve and interact with citizens, making it essential to create a legal framework and adequate cybersecurity solutions to guarantee that organizations and citizens can fulfill their missions knowing that their information is protected.

Key words: Cybersecurity, cybercrime, México, Human rights in the digital era.

[1]El Colegio de Morelos. Correo-e de contacto: alejandrofuentes@elcolegiodemorelos.edu.mx

I. Introducción

A mediados del siglo XX, los desarrollos científicos y tecnológicos se han dirigido, principalmente, al desarrollo de tecnologías que permiten almacenar y manipular datos para la generación de información y conocimiento. Con la liberación de las computadoras y el acceso ilimitado a una gran cantidad de datos se han transformado los contextos social, laboral, económico y político y con ello, una revolución en dichos ámbitos, siendo el jurídico un ámbito que ha requerido adaptarse a los distintos contextos, desde el tradicional trueque hasta el comercio electrónico.

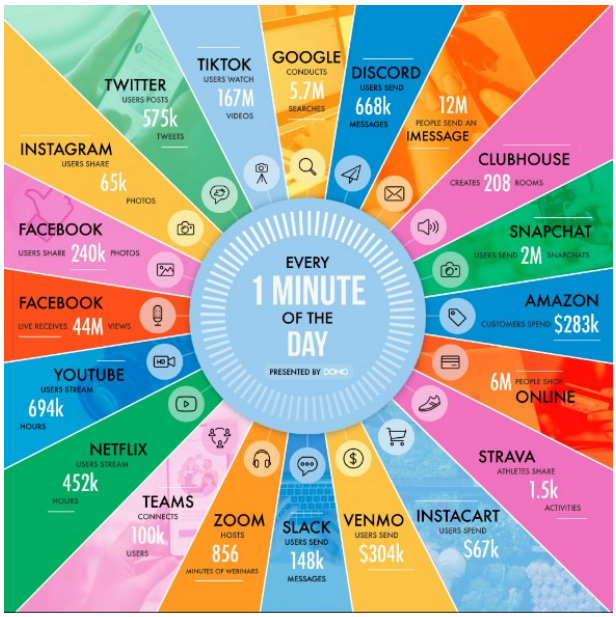
A medida que una mayor cantidad de información se comparte de manera digital, se incrementa el riesgo de pérdida y mal uso de dicha información, por lo que las personas y las organizaciones diseñan e implementan acciones para mejorar la seguridad relativa a este tema, lo que se denomina como ciberseguridad.

De forma particular, Domo (2021) menciona que la pandemia de 2020 transformó muchos aspectos de la vida cotidiana, desde la forma en que nos relacionamos (persona – persona) hasta la forma en que interactuamos con las marcas y el mundo digital. A su vez, menciona que los datos nunca duermen y no muestran signos de desaceleración, es decir, que continúan en un constante crecimiento.

En la novena edición de la infografía titulada *Data Never Sleeps 9.0* (Los datos nunca duermen), presenta el impacto de ha tenido la pandemia COVID19 en la digitalización de la vida cotidiana y cómo la tecnología está ayudando a reinventar el futuro del trabajo, de lo cotidiano y de lo académico. En la figura 1, se presenta lo que ocurre en un minuto de Internet.

Figura 1.

Infografía Data Never Sleeps 9.0 (los datos no duermen 9.0) (Domo, 2021).



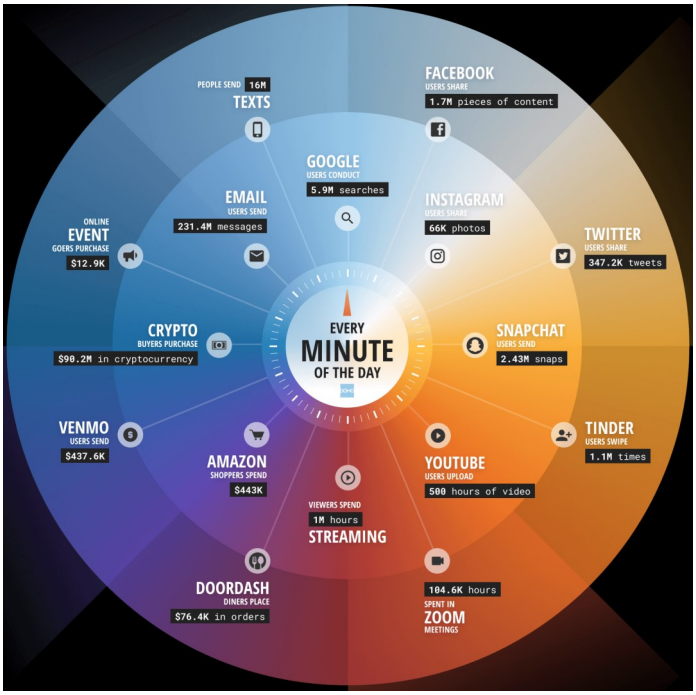
Fuente: Domo, 2021

En contraste, Domo (2022), en su infografía 10, presenta un incremento en todas las categorías, identificando 5 billones de usuarios de internet (figura 2) .

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Figura 2.

Infografía Data Never Sleeps 10.0 (Domo, 2022).



Fuente: Domo, 2022

El mismo autor presenta un comparativo entre la versión 1 y la versión 10, en donde identifica, por ejemplo, que la cantidad de búsquedas en *Google* ha incrementado de 2 millones (2013) a 5.9 millones (2022), en la compartición de fotos por *Instagram* de 3,600 (2013) a 66,000 (2022), el contenido compartido en Facebook incrementó de 684,000 a 1.7 millones, entre otros ejemplos.

Por su parte, el reporte "*Digital 2023: Global Overview Report*" que publican las firmas *We Are Social* y *Meltwater*, establecen que el 49% de la población mundial es usuaria de redes socio digitales (4,760,000,000 personas aproximadamente), accediendo a dichas redes el 92.3% del total de usuarios de Internet.

Ilustrando con el caso de México, dicho reporte señala que los mexicanos en promedio accedemos a 7.8 plataformas digitales, dedicando diariamente a ese fin un promedio de 3 horas con 21 minutos. Esto significa que, del tiempo diario que pasamos en Internet, los mexicanos destinamos el 41.3% a las redes virtuales.

Se consigna también que las redes virtuales más populares mundialmente son: 1. *Facebook* (2,958,000,000), 2.- *YouTube* (2,514,000,000), 3.- *WhatsApp* (2,000,000,000), 4.- *Instagram* (2,000,000,000) y 5.- *WeChat* (1,309,000,000). A pesar de su innegable penetración en los dos últimos años, *TikTok* fue instalada en la sexta posición con 1,051,000,000 usuarios. *Twitter*, en franca decadencia, se ubicó en la décimo cuarta posición con 556,000,000 de usuarios.

El estudio realizado por *Back base*, *Engagement Banking* en América Latina en 2022: El avance digital y sus oportunidades para el sector bancario, señala que, de 2020 a 2022, se incrementó en 60% el porcentaje de latinoamericanos que tiene acceso al menos a un producto financiero. (En 2020 era el 51% y en 2022 fue el 81%). Según el informe, este incremento es extraordinario, y acaba con el mito de que el nivel de bancarización de América Latina es muy bajo.

Pero este mismo informe señala que el 34% de los clientes eligen una institución bancaria si ésta le ofrece mayor flexibilidad y eficiencia para acceder a servicios financieros; solo un 15% elige hacer transacciones con alguna institución financiera o no, solo por considerarla segura. Un 14% la elige por tradición familiar.

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Todos estos datos nos indican que existe una necesidad urgente de incrementar la ciberseguridad a todos niveles, tanto a nivel individual como institucional y, especialmente, en las organizaciones gubernamentales, las cuales tienen acceso a una gran cantidad de información de los ciudadanos y resguardan información estratégica.

En el contexto del acceso (legal e ilegal) a la información se han generado diversos problemas, en donde los aspectos legales representan un campo en desarrollo, transformando no sólo su producción jurídica, sino también su filosofía y fundamentos teóricos, como lo describe Piña (2019), en donde su artículo tiene el propósito de "discurrir sobre el panorama teórico-jurídico de las conductas criminales informáticas en el marco de la Sociedad de la Información (SI), así como exponer la política informática y el marco jurídico mexicano vigentes que les son aplicables".

De manera particular Piña (2019) identifica que las Tecnologías de la Información y comunicación (TIC) han replanteado al derecho, dado que, por la masificación del ciberespacio afecta a todas las personas involucradas y requiere, por tal motivo, de una nueva forma para que el Estado puede ejercer su poder.

A partir de este contexto, el presente artículo tiene como objetivo comprender la trascendencia e implicaciones tecnológicas, éticas y normativas de la ciberseguridad, así como aportar lineamientos que fortalezcan la ciberseguridad en la operación cotidiana de las personas, empresas, y dependencias gubernamentales. Para esto, haremos un análisis literario y comparativo de documentos académicos, oficiales y tecnológicos que permitan abordar el tema de la ciberseguridad desde distintas perspectivas tanto teóricas como mediático-prácticas

2. Ciberseguridad y derechos humanos en la era digital

2.1 La ciberseguridad

De acuerdo a IBM (s.f.) la ciberseguridad es considerada como una práctica que consiste en "proteger los sistemas más importantes y la información confidencial ante ataques digitales"; a su vez, menciona que las medidas de ciberseguridad deben diseñarse con base en los tipos de amenazas que se estén previendo, dado que cada una requiere de un tratamiento especial.

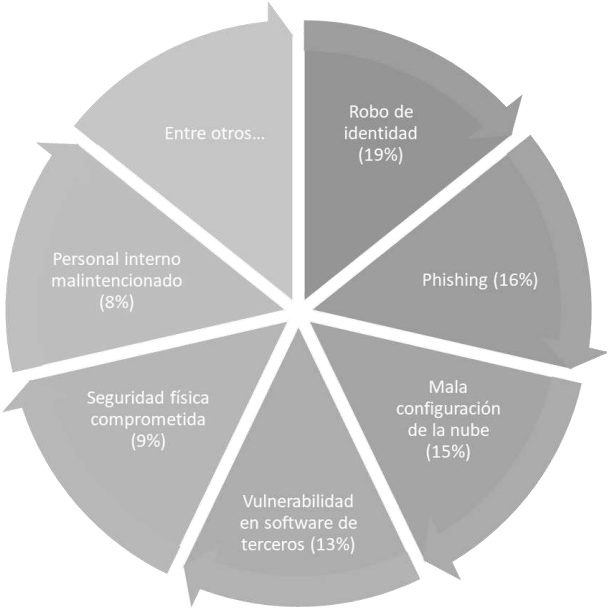
Actualmente, las empresas se han visto obligadas a mejorar la seguridad de la información, dado que, a pesar del esfuerzo global de mantenerse actualizado en este rubro, existe una brecha de seguridad que ha generado millones de pérdidas, estimándose en 3.86 millones de dólares a nivel mundial, siendo el caso particular de Estados Unidos con una pérdida de 8.64 millones de dólares, ello con base en el informe titulado *Cost of a data breach 2022: A million-dollar race to detect and respond* (Costo de una filtración de datos 2022: Una carrera de millones de dólares para detectar y responder) con base en IBM (s.f.).

De manera particular, en este informe, se puede identificar que el robo de identidad tuvo un 19% de afectación en relación al 100% de los ciberdelitos; por otra parte, el segundo ciberdelito fue identificado como *phishing*, con 16%, y el tercer ciberdelito, con 15% de usuarios afectados, fue la intromisión en la configuración (mala o vulnerable) de la nube, siendo este último, una preocupación de los últimos años, dado que la tecnología de la nube es prácticamente reciente. A continuación, se presenta una gráfica (figura 4.) con los porcentajes de los ciberdelitos identificados por IBM (s.f.).

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Figura 4.

Porcentaje de detección de ciberdelitos (IBM, s.f.)



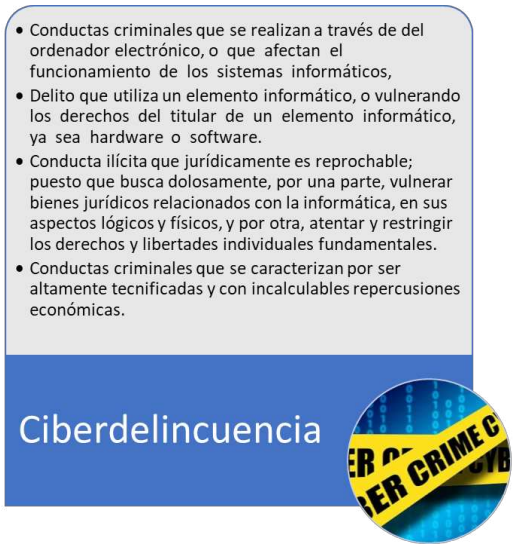
Fuente: IBM

2.2 Ciberdelitos

La ciberdelincuencia es un concepto que se ha traducido a partir de *Computer crime*, en donde, Piña (2019), resume diversas conceptualizaciones del término, las cuales se presentan en la figura 5.

Figura 5.

Definiciones de ciberdelincuencia (Piña, 2019).



Fuente: Piña, 2019

ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

medida que la ciberdelincuencia se incrementa a nivel mundial, han surgido diversas amenazas, en donde IBM (s.f.) identifica las siguientes como las más comunes:

Programas maliciosos: son variantes de software maliciosos como los gusanos, virus, troyanos, *spyware*, entre otros. Anteriormente se enviaba un archivo que contenía el programa malicioso, sin embargo, con el incremento del acceso a internet, la distribución del programa es a través del acceso a páginas Web que los contienen.

Ransomware. Es un tipo de programa malicioso que bloquea un archivo, bloquea el acceso a datos o sistemas, elimina o destruye datos, o publica datos confidenciales. Con esta herramienta, los ciberdelincuentes solicitan un rescate antes de ejecutarlos.

Phishing. Se le denomina a la ingeniería social en donde los usuarios proporcionan datos confidenciales mediante una estafa que, en este caso, es por medios digitales como el correo electrónico, principalmente.

Amenazas internas. Son personas que abusan de los permisos que se le han otorgado al interior de las organizaciones para hacer uso indebido de la información.

Ataque de denegación de servicio distribuido. Son ataques en donde su objetivo es sobrecargar el tráfico para bloquear un servidor, sitio Web o plataforma digital.

Amenazas persistentes avanzadas. Es una forma intrusiva de mantenerse oculto en redes y sistemas para acceder a datos confidenciales.

Ataque de intermediario. Es una forma de ataque en donde el ciberdelincuente intercepta y retransmite datos confidenciales con la intención de no ser detectado.

2.2 Derechos Humanos en la era digital

Aunque podemos enfocar muchos tipos de derechos humanos, teniendo como ejemplos el derecho al trabajo, el derecho al voto, el derecho a la atención sanitaria, entre otros; desde la perspectiva digital, lo más obvio es que apliquemos esta lente a los derechos humanos relacionados con la comunicación, el acceso y el control de la información. De manera particular, en el presente artículo, la orientación es hacia dos derechos en particular:

El derecho a buscar y recibir información y

El derecho a la intimidad.

Y lo que es más importante, establecer uno para explorar qué derechos digitales podrían ser necesarios para satisfacer plenamente los derechos humanos. Antes de hacerlo, sin embargo, será útil una revisión básica de la teoría de los derechos humanos.

La orientación del presente análisis está dirigido a una perspectiva de las normas morales con respecto a los derechos humanos, por lo consiguiente se llevará a cabo un análisis ético y no jurídico; Este enfoque se centra en las normas internacionales de derechos humanos, es decir, las normas internacionales de derechos humanos.

De manera particular, Henry Shue (Shue, 1980) considera los derechos humanos como protecciones contra amenazas estándar a intereses humanos importantes; es decir, se tienen derechos humanos porque son necesarios para protegernos de determinadas formas de amenaza, por ejemplo, la violencia, la opresión, la privación de la libertad, el derecho humano a no ser torturado, etc .

Con el advenimiento de las tecnologías, se puede considerar el ejemplo de que el gobierno quiera implantar chips en los ciudadanos para controlar su comportamiento; debido a que esta acción no es una amenaza estándar, entonces no hay un derecho humano específicamente para proteger a la gente de ella.

Es necesario comprender lo que los derechos humanos obligan a hacer a los Estados. Según la tipología tripartita de deberes, un derecho humano obliga a un Estado a actuar para respetar, proteger y cumplir ese derecho (Eide & Universidad de las Naciones Unidas, 1984).

> Cuando los Estados cumplen las tres obligaciones, entonces el derecho está satisfecho. Utilizando esta tipología se puede decir que el derecho que todos tenemos para acceder a Internet, por ejemplo, obligaría a los Estados (Eide & Universidad de las Naciones Unidas, 1984) a lo siguiente:
>
> Respetar la libertad de los ciudadanos para acceder a los contenidos de Internet sin interferencia del Estado.

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Proteger a los ciudadanos de otros que interfieran en la libertad de acceso a Internet

Cumplir el derecho velando por que los ciudadanos tengan acceso a la tecnología necesaria para acceder a Internet.

Para responder a la pregunta planteada por Mathiesen (2014) ¿Qué significaría satisfacer un determinado derecho humano en el ámbito digital?, habría que considerar una serie de cuestiones adicionales:

¿Cuál es el derecho y qué interés imperioso protege?

¿Cómo apoya este derecho a otros derechos?

¿Con qué otros derechos deben sopesarse?

¿Qué nuevas oportunidades crean las tecnologías de la información para satisfacer este derecho?

¿Qué nuevas amenazas suponen las tecnologías de la información para este derecho?

¿Qué disposiciones institucionales podrían tener que modificarse o establecerse para respetar, proteger y satisfacer este derecho en el contexto digital?

Con base en estas preguntas, Mathiesen (2014) presenta ejemplos del derecho a buscar y recibir información, así como del derecho a la privacidad. Muestra cómo responder a este conjunto de preguntas e identificar lo que pueden requerir los derechos humanos en la era digital. En la figura 6, se reflexiona sobre cómo podría funcionar un determinado derecho humano en el actual contexto digital. En la figura 7, nos muestra ejemplos del derecho a controlar el acceso a la información en cuatro documentos clave de derechos humanos.

Figura 6.

El derecho a la información en cuatro documentos clave de derechos humanos (Mathiesen, 2014)

Declaración Universal de los Derechos Humanos	Acceso (General)	Art. 19: Libertad de buscar, recibir y difundir informaciones e ideas por cualquier medio y sin consideración de fronteras. Art. 20: Libertad de reunión y de asociación pacíficas Art. 26: Educación
	Acceso (contenido particular)	Art. 27(1): Participar libremente en la vida cultural de la comunidad, gozar de las artes y participar en el progreso científico y en los beneficios que de él resulten.
Pacto Internacional de Derechos Civiles y Políticos	Acceso (General)	Art 19(2): Libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. Art. 21: Reunión pacífica
	Acceso (contenido particular)	Art. 9(2): Toda persona detenida será informada, en el momento de su detención, de las razones de la misma, y de los cargos que se le imputan. Art. 14: Toda persona acusada de un delito tendrá derecho a, ser informada, comunicarse con un defensor de su elección; ser informada, interrogar o hacer interrogar a los testigos de cargo
Pacto Internacional de Derechos Económico, Sociales y Culturales	Acceso (General)	Art 13(1): Educación
	Acceso (contenido particular)	Art. 11(2): Programas necesarios para mejorar los métodos de producción, conservación y distribución de alimentos. Art. 13(3): Libertad de los padres para escoger la escuela de sus hijos Art. 15(1)(a): Participar en la vida cultural Art. 15(2)(a): Conservación y difusión de la ciencia y cultura

ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Convención sobre Eliminación de las Formas de Discriminación contra la Mujer	Acceso (General)	Art. 10: Igualdad de derechos con los hombres en el ámbito de la educación Art. 14: Garantizar a las mujeres rurales formación y educación formal y no formal, incluida la relativa a la alfabetización funcional,... el beneficio de servicios comunitarios.
	Acceso (contenido particular)	Art. 16(e): Tener acceso a la información, la educación... para que las a las mujeres a ejercer el derecho a decidir libre y responsablemente el número de hijos y el intervalo entre los nacimientos
Declaración Universal de los Derechos Humanos	Acceso (General)	Art. 12: Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia. Art. 27(2): La protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autor.
	Acceso (contenido particular)	Art. 12: Nadie podrá ser objeto de atentados contra su honra y reputación.
Pacto Internacional de Derechos Civiles y Políticos	Acceso (General)	Art. 17(1): Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia o su correspondencia.
	Acceso (contenido particular)	Art. 17(1): Nadie podrá ser objeto de ataques ilegales a su honra y reputación. Art. 20(1): Queda prohibida por la ley toda propaganda en favor de la guerra"; (2): "Queda prohibida por la ley toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia"
Pacto Internacional de Derechos Económico, Sociales y Culturales	Acceso (General)	Art. 15(1)(c): Protección de los intereses morales y materiales que le correspondan por razón de las producciones científicas, literarias o artísticas de que sea autor.
	Acceso (contenido particular)	
Convención sobre Eliminación de las Formas de Discriminación contra la Mujer	Acceso (General)	
	Acceso (contenido particular)	Art. 10(c): Eliminación de todo concepto estereotipado de los papeles masculino y femenino en todos los niveles y en todas las formas de enseñanza...

Fuente: Mathiesen, 2014

El acceso a Internet es un derecho humano que se deriva de los derechos primarios de expresión y acceso a la información. Sin embargo, al considerar qué derechos tenemos en esta nueva era de la comunicación digital, tenemos que ir más allá de pensar sólo en el acceso a Internet. Tenemos que pensar más ampliamente sobre lo que los derechos humanos requieren en el ámbito digital y cómo las TIC pueden mejorar o amenazar nuestra capacidad de respetar, proteger y cumplir una amplia variedad de derechos humanos.

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

En este artículo, sugerimos un marco para pensar cómo pueden aplicarse los derechos humanos al entorno digital. Aunque el debate es preliminar, esperamos que nos lleve a reflexionar más detenidamente sobre lo que los derechos humanos exigen de nosotros en la era digital.

3. Marco metodológico

3.1 Metodología

El presente trabajo está orientado hacia un análisis literario y comparativo de documentos académicos, oficiales y tecnológicos que permitan abordar el tema de la ciberseguridad desde distintas perspectivas tanto teóricas como mediático-realistas. Con ello, se realizará una revisión de acontecimientos que han originado nuevos planteamientos y desafíos para el Estado, respecto a la ciberseguridad y a los derechos humanos en la era digital.

El análisis literario, permite identificar que la historia es una fuente esencial de información, en la que se presentan indicadores y eventos que permiten anticiparse a hechos probables al poner en práctica la teoría.

En este sentido, los países en desarrollo deben conocer los aspectos normativos y tecnológicos que se vinculan a la ciberseguridad, así como entender mejor las implicaciones nacionales e internacionales desde su ámbito legal y tecnológico .

Con este artículo se da inicio a la discusión sobre la pertinencia de contar con una ciberseguridad nacional en México para instrumentar medidas que permitan mitigar los riesgos innecesarios; con ello, es necesario describir los elementos normativos relacionados con la seguridad nacional en nuestro país y los desafíos que representa con base en las normas internacionales y en particular, hacia la conceptualización de los derechos humanos en la era digital.

3.2 La ciberseguridad en América Latina, el caso de México

Arreola-García (2018) expone que los avances relativos a la tecnología que impacta en el Estado enfrentan grandes desafíos, los cuales se relacionan con la falta de protección y al mal uso del ciberespacio. El autor hace referencia a que la seguridad nacional depende de forma directa de las TIC, las cuales han acelerado los procesos de búsqueda de huecos en la seguridad, aumentando las vulnerabilidades. Dadas estas circunstancias, el Estado busca salvaguardar la ciberseguridad mediante la aprobación de medidas políticas, tecnológicas y estratégicas para contrarrestar las amenazas que se presentan en el ciberespacio.

Con ello, se ha observado dependencia de las personas, empresas y gobierno hacia los medios digitales, lo cual ha traído consigo vulnerabilidades relativas al ciberespacio y con ello, hacia los sistemas digitales, lo que ha puesto en riesgo la seguridad del Estado, de los organismos que lo conforman y de forma indirecta a los individuos que laboran en estas organizaciones.

El uso obligatorio de medios digitales ha generado una hiper - conectividad y con ello, nuevos desafíos tanto positivos como negativos relativos a la disposición, integridad y confiabilidad de la información que aseguran y a su vez, ponen en riesgo la seguridad nacional.

Con respecto a la seguridad nacional y, aunada a la dependencia del ciberespacio en el ámbito del Estado y de las actividades que se realizan en éste, se tiene la necesidad creciente de verificar, actualizar e implementar sistemas de ciberseguridad y ciberdefensa en todos los campos que se relacionan con el Estado: salud, educación, servicios gubernamentales, servicios hacia la industria, etc.

En México los eventos relacionados con ciberataques se han incrementado, teniendo como ejemplo los siguientes:

> De acuerdo a IDC (2022), México registró “85 mil millones de intentos de ciberataques” para el mes de octubre de 2022.

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Según *FortiGuard Labs*, México recibió 187 mil millones de intentos de ciberataques en 2022, un crecimiento del 20% frente a 2021, primer lugar en América Latina y el Caribe, por encima de Brasil.

La Universidad de Guadalajara reporta que, durante la pandemia, los ciberataques a México han aumentado, orientados hacia empresas, instituciones gubernamentales y educativas, así como a particulares; esta afirmación fue provista por el responsable del Centro de Operaciones de la Red – Jaime Olmos de la Cruz de la Universidad de Guadalajara (UdG, 2022).

González (2022) presenta los siguientes ciberataques:

30 de septiembre: El presidente de México confirmó un ciberataque por parte del grupo "Guacamaya", en donde obtuvieron información confidencial de la SEDENA (Secretaría de la Defensa Nacional), y sobre de salud del presidente.

Noviembre de 2019: ciberataque a Pemex (Petróleos Mexicanos) y reportan que no hubo pérdidas de información confidencial.

Febrero de 2020: la Secretaría de Economía (SE) detectó un ciberataque en sus servidores e informaron que no hubo consecuencias mayores

2021: Víctor Ruiz (fundador de *SILIKN*) descubrió que "en el mercado negro se comercializan herramientas para atacar a instituciones gubernamentales".

La revista Forbes México informó que en año 2022, de los 156 mil millones de ciberataques en América Latina, 80 mil millones fueron dirigidos hacia México. En el tipo de ataques se detectó principalmente el *Ramsonware* (Forbes, 2022).

El Economista (2023), en su sección de ciberataques, presenta varios ejemplos:

El 8% de las Pequeñas y Medianas Empresas (PyMes) han sido víctimas del ciberataque *ransomware* y el 2% han tenido que pagar rescate

Del metro y los ciberataques, ¿dónde están las mayores amenazas?

Obsolescencia es un riesgo para la Fintech

Hackeo de la Secretaría de Infraestructura, Comunicaciones y Transporte (SICT)

Las amenazas en los entornos digitales y las TIC, que se han presentado en el contexto internacional del siglo XXI, hacen necesario el contar con una seguridad para estos entornos (ciberseguridad) y de una estrategia nacional de seguridad para implementar acciones políticas y jurídicas.

A nivel mundial, y a partir de distintos sucesos históricos como las guerras, los conflictos sociales y la integración de las TIC en los ámbitos políticos, se ha generado un debate para reconceptualizar el término de seguridad nacional e incorporar, con base en la propuesta de Dalby (1997), nuevos ámbitos, actores, factores y temas.

Con esta reconceptualización de la seguridad, se ha identificado la necesidad de incorporar actores y directrices no estatales y temas no militares, ante las nuevas amenazas de un entorno internacional interconectado, el cual requiere la inclusión del ciberespacio como nuevo ámbito de guerra y, por ende, nuevas formas de afrontar las referidas amenazas, que de éste emanan, contra la seguridad del Estado.

De acuerdo a Arreola-García (2018), la ciberseguridad nacional se debe dirigir a proteger a los individuos, a la sociedad y a las instituciones de las amenazas y ataques que se presenten en el ciberespacio. A su vez, el autor menciona la necesidad de establecer una definición precisa sobre la seguridad para evitar incertidumbre.

Menciona que la "seguridad y supervivencia del Estado se fundamenta en el conocimiento profundo de la estrategia y tácticas de guerra, así como en el manejo

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

eficiente de los recursos (materiales, tecnológicos y humanos) para lograr la victoria con el mínimo esfuerzo en el menor tiempo".

En el contexto latinoamericano, la seguridad cibernética se ha introducido como tema principal en la agenda de los países de la región. De acuerdo a (Moreno González Jimena, Albornoz María Mercedes y Solange Maqueo Ramírez María, 2019), Sin embargo, los esfuerzos que se han hecho para consolidar la ciberseguridad han sido desarticulados, persistiendo un desequilibrio en la situación de cada país, tanto en términos de desarrollo como de implementación de políticas de seguridad cibernética .

El Informe Ciberseguridad 2016, citado por el anterior estudio, que es elaborado por el Observatorio de la Ciberseguridad en América Latina y el Caribe, emplea 49 indicadores, para medir el grado o nivel de madurez de la capacidad de seguridad cibernética, con cinco dimensiones: política, sociedad, educación, legislación y tecnología y cinco niveles de madurez para cada indicador: inicial, formativo, establecido, estratégico y dinámico. De acuerdo con este informe, este es el grado de madurez en los distintos países de AL.

Figura 8.

Nivel de ciberseguridad en los países latinoamericanos

Nivel Inicial (17 países)	Nivel Formativo (10 países)	Nivel Establecido (5 países)
1. Antigua y Barbuda 2. Bahamas 3. Barbados 4. Belice 5. Bolivia 6. Ecuador 7. El Salvador 8. Granada 9. Guatemala 10. Guyana 11. Haití 12. Honduras 13. Nicaragua 14. República Dominicana 15. Saint Kitts y Nevis 16. Santa Lucía 17. Venezuela	1. Argentina 2. Brasil 3. Chile 4. Costa Rica 5. Dominica 6. México 7. Paraguay 8. Perú 9. San Vicente y las Granadinas 10. Surinam	1. Colombia 2. Jamaica 3. Panamá 4. Trinidad y Tobago 5. Uruguay

Fuente: Informe Ciberseguridad 2016, Observatorio de la Ciberseguridad en América Latina y el Caribe

En el cuadro anterior se observa que ningún país de Latinoamérica ha llegado a consolidar una política exitosa de ciberseguridad, ubicándose todos, cuando mucho, a media tabla de los niveles establecidos por el informe; no cuentan con marcos legales integrales sobre la materia; la mayoría no cuenta con una estrategia nacional; poca colaboración entre actores clave y se carece de un enfoque interdisciplinario.

México tiene un nivel formativo, según el reporte, es decir, ya cuenta con una estrategia nacional de ciberseguridad y ha establecido procesos de consulta para los grupos de interés clave, con vinculación internacional, de acuerdo al reporte, sin avanzar hacia un marco legal integral, con ni un enfoque interdisciplinario y dinámico que lo lleve a los siguientes niveles.

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

La actualización del informe sobre ciberseguridad en América Latina en 2020 (OCALC, 2020), señala que, aunque las cosas no cambiaron en la clasificación señalada en la figura 8, hay avances notables: el "Marco legal y regulatorio" es la dimensión más desarrollada, pero hay una mejoría significativa en la de "Estándares, organizaciones y tecnologías". Dado que todas las dimensiones presentan niveles similares de madurez en ciberseguridad, se puede pensar que los países de la región están abordando la ciberseguridad desde una perspectiva integral. Uruguay fue el país calificado con la madurez más alta de la región en cuatro de las cinco dimensiones.

En el mencionado estudio (Moreno et al. 2019), se establece la necesidad de que los gobiernos informen y sensibilicen a la ciudadanía respecto a los riesgos y vulnerabilidades ligados al uso de las TIC, medidas a tomar para protegerse, ya que hay mucho desconocimiento del tema en la ciudadanía.

En este sentido, hay propuestas que hacen énfasis en que la educación en ciberseguridad de los sectores público, privado y de la ciudadanía debe ser implementada de manera obligatoria en las escuelas, además de reglamentar que cada computadora posea un tipo de antivirus (Jiménez, Morales y Patiño, 2022).

Se destaca el ejemplo de Chile, el cual crea una estructura para que todos los nacionales que se encuentren en el entorno cibernético sean educados sobre el funcionamiento de la comunidad de internet y sus riesgos, asegurándose de que disfruten de ciertos derechos que son protegidos por el gobierno chileno. Esto se extiende a través de la cooperación con otros países de la región. En Chile, las amenazas más significativas se dirigen a su sector bancario y tienen una motivación económica (Jiménez et al. 2022).

El uso de contraseñas seguras, la instalación de antivirus, el acceso a páginas confiables, la conexión a redes seguras (privadas preferentemente), hacer copias de seguridad de los datos del usuario, el uso de la autenticación, tener cuidado con correos o enlaces maliciosos, y el conocer las formas de interacción y el funcionamiento de la red, son algunos de los lineamientos básicos de una educación en ciberseguridad para los usuarios .

En 2018, el Instituto Federal de Telecomunicaciones (IFT, 2018) propuso el Plan de Acciones en Materia de Ciberseguridad (PAMC) con su objetivo principal orientado hacia "fortalecer los beneficios derivados de una mayor inclusión social digital y de una mayor competencia en el sector de las telecomunicaciones y, favorecer la innovación y la economía digital".

En el PAMC presenta en su justificación, la necesidad de establecer la ciberseguridad debido a los riesgos relacionados con el ámbito del ciberespacio:

México como segundo país más atacado en América Latina

56% de las empresas encuestadas han tenido un ciberataque

49% de las empresas encuestadas han analizado sus vulnerabilidades

A su vez, se menciona en el PAMC que la "legislación vigente en Telecomunicaciones, ha permitido realizar diferentes cambios para establecer los fundamentos constitucionales y legales para crear una nueva arquitectura jurídica, institucional, regulatoria y de competencia y libre concurrencia en el sector de las telecomunicaciones y de la radiodifusión".

El estudio ya mencionado (Jiménez, Morales y Patiño, 2022) señala que la cercanía de México con Estados Unidos, lo hace un país altamente atractivo para someterlo a crímenes cibernéticos y de utilizar servidores en su territorio para cometer crímenes en los Estados Unidos. En este sentido, México se enfoca en identificar a los actores de estas nuevas actividades ilegales y las formas en las que se puede trabajar para debilitar y detener algunos de los crímenes que tienen lugar en el ciberespacio.

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Con respecto a la estrategia nacional de ciberseguridad en México, se creó la Subcomisión de Ciberseguridad (SC) presidida por la SG (Secretaría de Gobernación) mediante la Comisión Nacional de Seguridad (CNS) y cuyas actividades estarán dirigidas hacia dar seguimiento y administrar la coordinación en el proceso de implementación de la Estrategia Nacional de Ciberseguridad (ENC) (IFT, 2018). En la figura 9 se presentan los ejes transversales de la ENC.

Figura 9.

Ejes Transversales de la ENC (IFT, 2018).

Fuente: Estrategia Nacional de Ciberseguridad

A su vez, la ENC presenta los objetivos estratégicos con un "enfoque basado en riesgos, una perspectiva de derechos humanos y la colaboración multidisciplinaria y de múltiples actores" (IFT, 2018), los cuales se presentan en la figura 10.

Por otra parte, la ENC (IFT, 2018) ha establecido diferentes acciones basadas en las temáticas:

Estrategia Nacional de Ciberseguridad

Prospectiva Regulatoria

Colaboración en Materia de Seguridad y Justicia

Puntos de Intercambio de Tráfico de Internet (IXP)

Transición a IPv6

Información al usuario

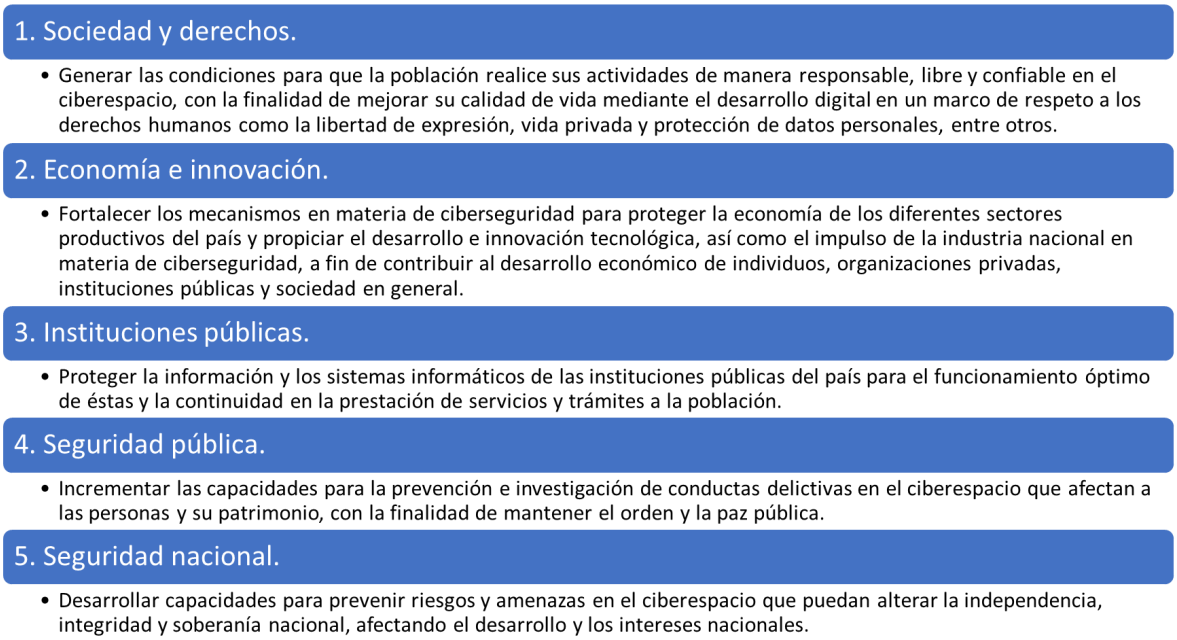
Norma Mexicana de Comercio Electrónico

Tratados y Acuerdos Internacionales

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Figura 10.

Objetivos Estratégicos de la ENC (IFT, 2018).



Fuente: Estrategia Nacional de Ciberseguridad

Se prevé en el ENC, llevar a cabo el Plan de Acciones en materia de Ciberseguridad, el cual tiene como propósito "robustecer los beneficios derivados de una mayor inclusión social digital, de una mayor competencia en el sector de las telecomunicaciones, así como fomentar la economía digital". Para ello, el Plan de Acciones (PA) en el área de Ciberseguridad estableció cinco Objetivos Estratégicos Institucionales (IFT, 2018), los cuales se presentan en la figura 11.

En México, existen tres propuestas de creación de una Ley general de Ciberseguridad. La del senador Miguel Ángel Mancera, busca establecer bases de integración y acción coordinada de instituciones y autoridades encargadas de preservar la ciberseguridad; establecer los tipos penales en la materia así como definir forma y términos de colaboración entre entidades federativas, municipios y la Federación, para garantizar el derecho de acceso a las tecnologías de la información y comunicación, y de los servicios de telecomunicación, en forma segura (…) así como establecer la obligación del Estado de tomar medidas para monitorear, prevenir y manejar los riesgos, peligros y amenazas de ciberseguridad[2].

[2]Senador Miguel Ángel Mancera Espinoza, Iniciativa de la Ley General de Ciberseguridad, 1 de septiembre 2020.

ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Figura 11.

Objetivos Estratégicos Institucionales (IFT, 2018)

Fuente: Estrategia Nacional de Ciberseguridad

Por su parte, la propuesta de la diputada Juanita Guerra Mena, busca establecer los ámbitos de competencia de las autoridades en la materia; determinar las bases para la generación de estrategias, políticas públicas y acciones de la ciberseguridad; así como establecer el marco normativo para la coordinación de acciones entre particulares y autoridades para la prevención, investigación y persecución de los ciberdelitos[3].

Existe una iniciativa más, planteada por la senadora Jesús Lucía Trasviña, que define a la Ciberseguridad como una función a cargo de la Federación, las Entidades Federativas y Municipios, que tiene como objetivo salvaguardar el uso seguro y responsable de las redes, los sistemas de información y comunicaciones, mediante la prevención, detección y respuesta a los ciberataques, con medidas específicas para la promoción de un ciberespacio seguro y fiable[4].

Ninguna de ellas ha sido aprobada y, por tanto, no hay una normatividad específica de ciberseguridad en nuestro país. Por tanto, hay distintos aspectos de la ciberseguridad que se consideran, de manera aislada, en los siguientes ordenamientos: Código Penal Federal, de la Ley General del Sistema Nacional de Seguridad Pública y de la Ley de Seguridad Nacional[5].

3.3 Desarrollo digital y vulnerabilidad de los derechos humanos.

El costo de los incidentes derivados de la ciberdelincuencia a nivel mundial fue de 3 billones de dólares en 2015 y la expectativa es que en 2021 llegue a 6 billones *(Cybersecurity Ventures*, 2016). A medida que el mundo se interconecta mediante el uso de redes digitales más rápidas y grandes, la Organización de los Estados Americanos (OEA) busca mejorar las políticas que protegen a los gobiernos y a la sociedad civil contra las actividades cibernéticas ilícitas. La Secretaría de Seguridad Multidimensional -concretamente a través del Comité Interamericano contra el Terrorismo (CICTE)- trabaja para coordinar los esfuerzos de los países miembros y reforzar la cooperación regional en materia de seguridad.

[3]Diputada Juanita Guerra Mena, Iniciativa de la Ley General de Ciberseguridad, revista parlamentaria, 6 de octubre 2022.
[4]Senadora Jesús Lucía Trasviña Waldenrath, Proyecto de decreto por el que se expide la Ley General de Ciberseguridad, 23 de marzo de 2021.
[5]Senador Miguel Ángel Mancera Espinoza, Iniciativa de la Ley General de Ciberseguridad, 1 de septiembre 2020.

ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.
Espacios Públicos

Luis Almagro, Secretario General de la OEA, reconoció que las tecnologías de la información y la comunicación (TIC) y sus múltiples usos siguen evolucionando a gran velocidad en la región y que los países son muy vulnerables a ciberataques potencialmente devastadores[6].

.Según el Informe sobre Ciberseguridad 2016 de la OEA y el BID (Banco Interamericano de Desarrollo), 4 de cada 5 países de la región no cuentan con estrategias o planes de ciberseguridad para proteger las infraestructuras críticas, y 2 de cada 3 de ellos no disponen de un centro de mando y control ni capacidad para perseguir los ciberdelitos. Con base en ello, han estimado que la ciberdelincuencia cuesta alrededor de 575 millones de dólares al año, lo que representa el 0.5% del PIB mundial, y en América Latina alcanza los 90 millones de dólares[7].

Según el reporte de FortiGuard Labs, México recibió 187 mil millones de intentos de ciberataques en 2022, lo que representa un crecimiento del 20 por ciento frente a 2021. Con esta cifra, México se coloca en el primer lugar en América Latina y el Caribe, por encima de Brasil.

El gobierno, el sector privado y la sociedad civil deben estar a la altura de la constante innovación en el sector de las Tecnologías de la Información (TI), tanto como usuarios como posibles blancos de ataques. México ocupa el segundo lugar, después de Brasil, entre los países que envían spam a la red; estos dos países más Colombia envían el 75% de los spams del continente latinoamericano[8].

La Unión Internacional de Telecomunicaciones identifica 17 Equipos Nacionales de Respuesta a Incidentes de Seguridad Informática (CSIRT por sus siglas en inglés) en América Latina y clasifica la preparación de México para las amenazas cibernéticas en 18 de 29 puntos. México es miembro del Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST por sus siglas en inglés) y tiene interacción con la comunidad internacional en materia de ciberseguridad, la cual está representada principalmente por el Equipo de Respuesta a Emergencias Informáticas de México (CERT-MX) creado en 2010. CERT-MX agrupa a expertos de los sectores gubernamental, comercial y académico con el fin de preparar a México para responder a ciberataques y participa en la protección de infraestructuras críticas. La Policía Federal se encarga de investigar los ciberdelitos a nivel nacional[9].

Por otra parte, en la clasificación de la Unión Internacional de Telecomunicaciones (UIT) sobre el uso general de Internet y el porcentaje de penetración de Internet en la sociedad identifica que Argentina destaca con un 85%, mientras que México tiene un estimado del 72%. Al desglosar el porcentaje de usuarios de Internet por grupos de edad, se observa que el grupo de edad más activo es el de 15-24 años, con un 90% en México[10].

En relación a las competencias digitales, sólo el 20-31% de la sociedad tiene competencias básicas, mientras que del 2-12% del total tiene competencias avanzadas. Esto supone una presión para la sociedad que hace que las personas sin suficientes competencias digitales estén expuestas a ciberataques y vulnerables dentro de su contexto digital. En contraparte, el valor del mercado digital en América Latina muestra una tendencia creciente. En 2019, su valor fue de 12.9 mil millones de USD y se estima un incremento a 26.2 mil millones USD para 2025. Esta tendencia creciente tendencia creciente está muy expuesta a los ciberataques que causan daños que pueden medirse en el coste medio de las violaciones de datos.

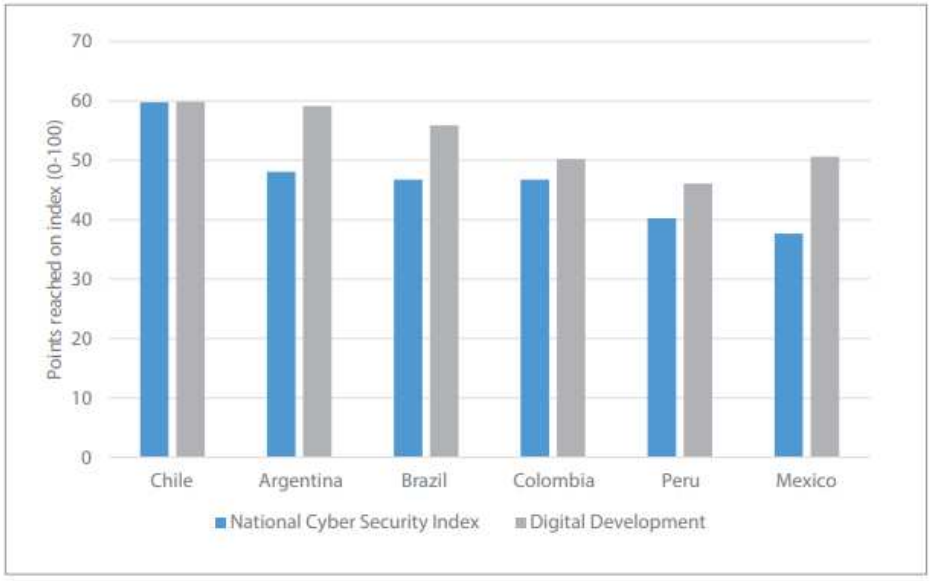
Urbanovics (2022) presenta un marco del estudio para profundizar en los diferentes aspectos incluidos en el Índice Nacional de Ciberseguridad y el Índice de Desarrollo Digital, los cuales presenta en la figura 12.

[6]KOBEK, Luisa Parraguez. The State of Cybersecurity in Mexico: An Overview. *Wilson Centre's Mexico Institute, Jan*, 2017.
[7]Organization of American States & Interamerican Development Bank. (2016). Cybersecurity: Are we Ready in Latin America and the Caribbean? Retrieved on December 1, 2016 from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-inLatin-America-and-the-Caribbean.pdf .
[8]CISCO Systems Inc. (2016). Spam Overview. Retrieved on December 15, 2016 from: https://www.senderbase.org/static/spam/#tab=4
[9]ANNA, Urbanovics. Cybersecurity Policy-Related Developments in Latin America. *AARMS–Academic and Applied Research in Military and Public Management Science*, 2022, vol. 21, no 1, p. 79-94.
[10]Statista: Value of the Cybersecurity Market in Latin America in 2019 and 2025. https://www.statista.com/topics/7126/cybersecurity-in-latin-america

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Figura12.

Puntuaciones obtenidas en el Índice Nacional de Ciberseguridad y en el Índice de Desarrollo Digital (Urbanovics, 2022).



Fuente: Índice Nacional de Ciberseguridad y en el Índice de Desarrollo Digital

Aunque la privacidad está consagrada como un derecho fundamental en la Declaración Universal de Derechos Humanos, el Convenio Internacional de Derechos Civiles y Políticos y las constituciones de más de 150 países, la tecnología ha erosionado considerablemente tanto la noción de privacidad como la capacidad de las personas para proteger sus datos personales del uso indebido por parte de gobiernos, empresas y delincuentes[11].

Desde los teléfonos inteligentes hasta el Internet de las cosas, pasando por el GPS, estamos accediendo voluntariamente a una innumerable variedad de agentes privados y públicos el acceso a todo lo que compramos, dondequiera que vamos, a detalles íntimos sobre nuestra salud, nuestro uso de Internet, nuestro historial financiero, nuestras opiniones políticas, nuestras familias y amigos, y mucho más.

No debería sorprender en absoluto que esta avalancha de datos digitales, biométricos y geoespaciales se utilice a menudo de forma que perjudique a los económicamente desfavorecidos. Los consumidores que viven en códigos postales con altos índices de delincuencia o bajos ingresos medios se ven bombardeados con anuncios digitales de hipotecas de alto riesgo, préstamos de día de pago y universidades con ánimo de lucro. El escrutinio digital también explica por qué las tasas de hipotecas y seguros son más altas y los tiempos de respuesta de la policía más lentos en estos barrios.

Complejos algoritmos rechazan a los solicitantes de empleo en función de los riesgos de salud previstos o de las bajas puntuaciones crediticias. Los jueces de varios estados utilizan modelos de datos para fijar fianzas y sentencias. Investigaciones recientes han descubierto que estos algoritmos imponen penas más duras a los acusados de color, reflejando los sesgos policiales que se producen en el mundo no virtual[12].

Cuando el trabajo a distancia se convirtió en la norma durante la pandemia del COVID-19, el uso y las críticas a estas tecnologías se intensificaron enormemente al desaparecer los límites entre el lugar de trabajo y el hogar. Mientras que los empleadores consideraban estas medidas como una forma adecuada de garantizar la productividad de los empleados que ya no

[11]William F. Schulz and Sushma Raman, The Coming Good Society: Why New Realities Demand New Rights (Cambridge, MA, 2020), 81–82.
[12]Cathy O'Neill, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (New York, 2016); Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (New York, 2019).

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

podían ser observados en la oficina, los empleados que se dieron cuenta de la vigilancia electrónica la consideraron más bien orwelliana, como si se tratara de un sistema de vigilancia de los datos privados almacenados en computadoras personales.

Las redes sociales, por su parte, han contribuido en eliminar la separación entre aspectos personales y laborales mediante el uso de algoritmos que "obligan" a los usuarios a estar en constante publicación y revisión de cuestiones personales en donde, mediante encuestas y revisión de los distintos datos que genera cada usuario mientras está conectado a dichas redes sociales, incrementan la cantidad de información que permite a toda persona con acceso a estos datos, a establecer patrones de comportamiento.

A medida que la inteligencia artificial, entendida como "sistemas que actúan como humanos"[13], sigue abriéndose paso en nuestra vida cotidiana, su propensión a interferir en los derechos humanos no hace sino agravarse. Muchas de las cuestiones que surgen al examinar este ámbito no son nuevas, pero se ven exacerbadas en gran medida por la escala, la proliferación y el impacto en la vida real que facilita la inteligencia artificial. Por ello, el potencial de la inteligencia artificial tanto para ayudar como para perjudicar a las personas es mucho mayor que el de las tecnologías anteriores.

Aunque ya hemos visto algunas de estas consecuencias, los impactos sólo seguirán creciendo en gravedad y alcance. Sin embargo, si empezamos ahora a examinar qué salvaguardias y estructuras son necesarias para abordar los problemas y los abusos, los peores daños -incluidos los que afectan de manera desproporcionada a las personas marginadas- pueden prevenirse y mitigarse. Hay varias lentes a través de las cuales los expertos examinan la inteligencia artificial.

El uso de la legislación internacional sobre derechos humanos, sus normas e instituciones bien desarrolladas para analizar los sistemas de inteligencia artificial, puede contribuir a las conversaciones que ya están teniendo lugar, y proporcionar un vocabulario universal y foros establecidos para abordar las diferencias de poder.

Además, las normas de derechos humanos aportan un marco de referencias que constituyen potenciales soluciones a esta amenaza:

- Normas de protección de datos para proteger los derechos en los conjuntos de datos utilizados para desarrollar y alimentar los sistemas de inteligencia artificial;
- Salvaguardias especiales para los usos gubernamentales de la inteligencia artificial;
- Salvaguardias para el uso de los sistemas de inteligencia artificial por parte del sector privado
- Inversión en investigación para examinar el futuro de la inteligencia artificial y sus posibles interferencias con los derechos humanos.

Los beneficios de basar las decisiones en cálculos matemáticos pueden ser enormes en muchos sectores de la vida. Sin embargo, confiar demasiado en la Inteligencia Artificial (IA) implica inherentemente determinar patrones más allá de estos cálculos y, por tanto, puede volverse en contra de los usuarios, perpetrar injusticias y restringir los derechos de las personas.

De hecho, la Inteligencia Artificial puede afectar negativamente a una amplia gama de nuestros derechos humanos. El problema se agrava por el hecho de que las decisiones se toman sobre la base de estos sistemas, mientras que no hay transparencia, responsabilidad y salvaguardias sobre cómo están diseñados, cómo funcionan y cómo pueden cambiar con el tiempo.

La tensión entre las ventajas de la tecnología de IA y los riesgos para nuestros derechos humanos se hace más evidente en el ámbito de la privacidad. La privacidad es un derecho humano fundamental, esencial para vivir con dignidad y seguridad.

[13]IBM, página electrónica. Señala que "es un campo que combina la ciencia informática y los conjuntos de datos robustos para permitir la resolución de problemas. (…) Estas disciplinas están compuestas por algoritmos de IA que buscan crear sistemas expertos que hagan predicciones o clasificaciones basadas en datos de entrada." https://www.ibm.com/mx-es/cloud/learn/what-is-artificial-intelligence

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Pero en el entorno digital, incluso cuando utilizamos aplicaciones y plataformas de redes sociales, se recopilan grandes cantidades de datos personales que pueden utilizarse para elaborar perfiles nuestros y predecir nuestros comportamientos.

4. Conclusiones

Con el creciente número de ciberataques y la importancia cada vez mayor del ciberespacio, las estrategias nacionales y la creación de unidades especiales de ciberseguridad se han convertido en una necesidad. El gobierno de México se ha comprometido a reforzar la conciencia social y cultural en el ámbito cibernético y cooperar regionalmente para mejorar sus capacidades y compartir información y buenas prácticas. A este respecto, México es uno de los países más vulnerables a los ciberataques debido al número creciente de usuarios de Internet y de los medios sociales, y a un marco institucional, infraestructural y reglamentario insuficientemente preparado.

Para comprender la trascendencia de la ciberseguridad, debemos recordar que el acceso a Internet es un derecho humano que se deriva de los derechos primarios de expresión y acceso a la información. Pero la ciberseguridad debe ir más allá del solo acceso a internet. En este artículo presentamos ejemplos del derecho a buscar y recibir información, así como del derecho a la privacidad. Las implicaciones de la ciberseguridad como protección de un derecho humano obligan los Estados a fortalecerla jurídicamente y de facto.

Se puede concluir que en México no hay una normatividad específica de ciberseguridad, aunque se han presentado varias iniciativas de ley al respecto que hasta el momento no han sido aprobadas. En cambio, hay distintos aspectos de la ciberseguridad que se consideran, de manera aislada, en los siguientes ordenamientos: Código Penal Federal, Ley General del Sistema Nacional de Seguridad Pública y Ley de Seguridad Nacional .

La Estrategia Nacional de Ciberseguridad que aquí se analizó es la respuesta del gobierno mexicano al reto de establecer los mecanismos necesarios para la defensa cibernética de la nación, planteando en ella lineamientos y acciones en torno a tres principios rectores u objetivos estratégicos: Derechos Humanos, gestión de riesgos y Colaboración multidisciplinaria y de múltiples actores. Sin embargo, podemos considerar que la estrategia está en una fase inicial en cuanto al nivel de eficacia que se requiere de acuerdo a la problemática y retos aquí expuestos. Fue la pandemia del COVID19 la que obligó a la acción gubernamental inmediata pero la falta de una ley u ordenamiento integral, como se mencionó anteriormente, es una sensible omisión en la búsqueda de consolidación de la ciberseguridad.

La tensión entre las ventajas de la tecnología de IA y los riesgos para nuestros derechos humanos se hace más evidente en el ámbito de la privacidad. La privacidad es un derecho humano fundamental, esencial para vivir con dignidad y seguridad. Pero en el entorno digital, incluso cuando utilizamos aplicaciones y plataformas de redes sociales, se recopilan grandes cantidades de datos personales que pueden utilizarse para elaborar perfiles nuestros y predecir nuestros comportamientos.

Sin embargo, el balance respecto a la ciberseguridad en México sigue siendo insuficiente. Los lineamientos esbozados en este trabajo pretenden guiar y consolidar los esfuerzos legales, prácticos y educativos que habrán de llevarnos a su implementación y consolidación. Estas últimas constituyen reflexiones orientadoras para el desarrollo de nuevas investigaciones.

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

Referencias

Arreola-García, A. (2018). Ciberseguridad Nacional en México y sus desafíos (National Cybersecurity in Mexico and its Challenges). Instituto de investigaciones estratégicas de la armada de México (Strategic Research Institute of the Mexican Navy), 17.

Cybersecurity Ventures. (2016). Hackerpocalypse: A Cybercrime Revelation. https://www.herjavecgroup.com/hackerpocalypse-cybercrime-report/

Backbase (2022). El avance digital y sus oportunidades para el sector bancario (Digital advancement and its opportunities for the banking sector). Engagement Banking in Latin America https://www.backbase.com/es/insights/reports/ami-research-2022

Belmonte, L. (2023). Can Human Rights Survive Technology? Diplomatic History, 47(1), 1-18.

Cathy O'Neill, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy (New York, 2016); Virginia Eubanks, Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor (New York, 2019).

CISCO Systems Inc. (2016). Spam Overview. Retrieved on December 15, 2016 from: https://www.senderbase.org/static/spam/#tab=4

Dalby, S. (1997). Contesting an essential concept: Reading the dilemmas in contemporary security discourse. Critical security studies: concepts and cases, 3, 31.

IBM (s.f.). ¿Qué es la ciberseguridad? (what is cybersecurity?). https://www.ibm.com/es-es/topics/cybersecurity

Digital (2023). Digital 2023: Global Overview Report. https://datareportal.com/reports/digital-2023-global-overview-report,

Guerra Mena, . (2022) Iniciativa de la Ley General de Ciberseguridad (General Cybersecurity Law Initiative). revista parlamentaria, 6 de octubre 2022.

Domo (2021) Data Never Sleeps 9.0. https://www.domo.com/learn/infographic/data-never-sleeps-9

Domo (2022) Data Never Sleeps 10.0. https://www.domo.com/data-never-sleeps#

Eide, A., & United Nations University. (1984). Food as a human right. Tokyo, Japón: United Nations University.

El Economista (2023). Ciberataques (Cyberattacks). https://www.eleconomista.com.mx/tags/ciberataques

Jiménez Almeira, G. A. Morales Lince, M. P. & Patiño Sánchez, I. (2022). Ciberseguridad: una mirada a los métodos y estrategias de anticipación al avance del cibercrimen en Colombia y la región. En P. A. Sierra -Zamora, T. L. Fonseca-Ortiz, & F. Coronado-Camero (Eds.), De los delitos transnacionales, las Fuerzas Armadas y el tratamiento jurídico de la seguridad y defensa nacionales (pp. 137-155). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602120.0

Gob (2017). Estrategia Nacional de Ciberseguridad, México (National Cybersecurity Strategy, Mexico). https://www.gob.mx/cms/uploads/attachment/file/411729/Memoria_y_Recomendaciones_ENCS.pdf

Leyva-Reus, J. (2023). México, el favorito de los hackers (México, the favorite of hackers). El financiero.https://www.elfinanciero.com.mx/opinion/jeanette-leyva/2023/02/28/mexico-el-favorito-de-los-hackers/

Forbes (2022). México registra 80,000 millones de intentos de ciberataques en 2022 (México records 80 billion attempted cyber-attacks in 2022). https://www.forbes.com.mx/mexico-registra-80000-millones-de-intentos-de-ciberataques-en-2022/

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.

González, A. (2022). Historial de ciberataques en el actual Gobierno de México (History of cyber-attacks on the current Mexican Government). https://dplnews.com/historial-de-ciberataques-en-el-actual-gobierno-de-mexico/

IBM (s.f.). Cost of a Data breach 2022. https://www.ibm.com/reports/data-breach

IFT (2018). Plan de Acciones en Materia de Ciberseguridad (Cybersecurity Action Plan). Unidad de Política Regulatoria Dirección General de Regulación Técnica (Regulatory Policy Unit Directorate General of Technical Regulation). https://ciberseguridad.ift.org.mx/files/guias_y_estudios/5_upr_planaccionesciberseguridad.pdf

Kobek, L. P. (2017) The State of Cybersecurity in Mexico: An Overview. Wilson Centre's Mexico Institute, Jan, 2017.

Mathiesen, K. (2014). Human rights for the digital age. Journal of Mass Media Ethics, 29(1), 2-18.

Organization of American States & Interamerican Development Bank. (2016). Cybersecurity: Are we Ready in Latin America and the Caribbean? Retrieved on December 1, 2016 from: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Cybersecurity-Are-We-Prepared-inLatin-America-and-the-Caribbean.pdf

Piña Libién, H. (2019). Cibercriminalidad y ciberseguridad en México (Cybercrime and cybersecurity in México). Ius Comitialis, *2*(4), 47-69. doi:10.36677/iuscomitialis.v2i4.13203

Mancera Espinoza, M.A. (2020) Iniciativa de la Ley General de Ciberseguridad (General Cybersecurity Law Initiative). https://sil.gobernacion.gob.mx/Archivos/Documentos/2020/09/asun_4064516_20200902_1599062884.pdf

Moreno González Jimena, Albornoz María Mercedes y Solange Maqueo Ramírez María; Ciberseguridad: estado de la cuestión en América Latina. Revista de Administración Pública INAP No.148, Vol. LIV No. 1 2019. P.p. 23-46

Observatorio de la Ciberseguridad en América Latina y el Caribe, Ciberseguridad. ¿Estamos preparados en América Latina y el Caribe? Informe Ciberseguridad 2016 y 2020, Organización de los Estados Americanos y Banco Interamericano de Desarrollo. file:///C:/Users/rgome/Downloads/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Trasviña Waldenrath, J. L. (2021) Proyecto de decreto por el que se expide la Ley General de Ciberseguridad (Draft Decree enacting the General Cybersecurity Law). https://forojuridico.mx/analisis-de-la-iniciativa-que-expide-la-ley-general-de-ciberseguridad-presentada-el-25-03-2021/

Statista: Value of the Cybersecurity Market in Latin America in 2019 and 2025. topics/7126/cybersecurity-in-latin-america

UdG (2022). Ciberataques en México aumentaron durante la pandemia (Cyberattacks in México increased during the pandemic). https://www.udg.mx/es/noticia/ciberataques-en-mexico-aumentaron-durante-la-pandemia

Urbanovics, A. (2022). Cybersecurity Policy-Related Developments in Latin America. AARMS–Academic and Applied Research in Military and Public Management Science, 2022, vol. 21, no 1, p. 79-94.

William F. Schulz and Sushma Raman, The Coming Good Society: Why New Realities Demand New Rights (Cambridge, MA, 2020), 81–82.

Espacios Públicos ISSN: 2954-4750, año 24, núm. 61, enero-marzo 2023.