RECOMENDACIÓN QUE EMITE EL VII CONSEJO CONSULTIVO DEL INSTITUTO FEDERAL DE TELECOMUNICACIONES SOBRE LA PARTICIPACIÓN ACTIVA DEL INSTITUTO EN LAS DISCUSIONES EN TORNO A LA CREACIÓN DE LA LEGISLACIÓN EN MATERIA DE CIBERSEGURIDAD PROPUESTA POR DIFERENTES PARTIDOS POLÍTICOS DADAS LAS POSIBLES IMPLICACIONES QUE TUVIERA PARA EL INSTITUTO

El VII Consejo Consultivo del Instituto Federal de Telecomunicaciones emite la presente recomendación al Pleno del Instituto Federal de Telecomunicaciones ("IFT o Instituto"), para intervenir proactivamente en la redacción final de la iniciativa de una Ley Federal de Ciberseguridad dada la importancia que este tema significa para el futuro de las telecomunicaciones, el ordenamiento jurídico nacional aplicable y la actividad del propio Instituto.

I. ANTECEDENTES

1. La Ciberseguridad puede ser entendida como el conjunto de políticas, controles, procedimientos, métodos de gestión de riesgos y normas asociadas con la protección de la sociedad, gobierno, economía y seguridad nacional en el ciberespacio y las redes públicas de telecomunicaciones, en términos de la Estrategia Nacional de Ciberseguridad de 2017[1] (ENA).

El objetivo primordial de la ENA al momento de su creación y publicación era establecer la visión del Estado Mexicano en la materia. Es un concepto que involucra esfuerzos de distinta naturaleza, no únicamente aspectos legislativos o técnicos. Por lo que la normativa sobre ciberseguridad que en su momento se expida a nivel federal, deberá contar con un enfoque integral, principalmente apelando a una

[1] Estrategia Nacional de Ciberseguridad, última vez consultado el día 30 de junio de 2023.

correcta gestión de riesgos y preponderando la visión preventiva más que correctiva y punitiva.

2. Hablando estrictamente de legislación federal, el primer antecedente legislativo que se encuentra aún en vigor, lo podemos encontrar en el Código Penal Federal, en el CAPÍTULO II del TÍTULO NOVENO, artículos 211 BIS I a 211 BIS 7, enfocados a sancionar las conductas de acceso ilícito a Sistemas y Equipos de informática publicado en el Diario Oficial de la Federación el 17 de mayo de 1999[2]. En esa misma Reforma también el legislador se encargó de adicionar el artículo 168 BIS para prever las sanciones aplicables a conductas ilícitas tendientes a descifrar las señales de telecomunicaciones. Esto ilustra que desde hace más de 20 años ha sido de interés del legislador federal abordar y sancionar las conductas ilícitas en contra de los Sistemas de Informática y las Telecomunicaciones, y hace patente que dicha legislación continúa vigente y desmitifica la idea de que no existe legislación aplicable en materia de ciberseguridad.

3. A nivel estatal, podemos destacar amplios esfuerzos legislativos desde el año 2000, por ejemplo, el Código Penal del Estado de Sinaloa, en su Capítulo V artículo 217 sanciona lo que se entiende por Delito Informático; a lo largo del tiempo y de la República Mexicana, los legisladores de distintas entidades federativas han ido reformando y adicionando artículos tendientes a sancionar estas conductas, como ejemplo, presentamos una tabla elaborada con una muestra representativa:

[2] https://www.dof.gob.mx/nota_detalle.php?codigo=4948419&fecha=17/05/1999#gsc.tab=0

ESTADO	ARTÍCULOS	NOMENCLATURA	FECHA DE PUBLICACIÓN
AGUASCALIENTES	ARTÍCULO 181	Acceso informático indebido	Reformado el 28 de noviembre de 2019
BAJA CALIFORNIA	TÍTULO TERCERO, CAPÍTULO SEGUNDO	Delitos Contra la Inviolabilidad Del Secreto y de los Sistemas y Equipos de Cómputo y Protección de los Datos Personales	14 de septiembre de 2007
CHIHUAHUA	CAPÍTULO IV	Del Uso y Acceso Ilícito a los Sistemas y Equipos Informáticos y de Comunicación	19 de noviembre de 2011
COLIMA	Artículo 201	Se equipara al delito de fraude en la fracción VII y se considera como agravante que el sujeto activo cuente con formación o grado relacionado con la informática	22 de noviembre 2016

JALISCO	CAPÍTULO II	La Obtención Ilícita de Información Electrónica	4 de mayo de 2012
QUERÉTARO	CAPÍTULO II	Acceso Ilícito a Sistemas de Informática	22 de abril de 2011
YUCATÁN	CAPÍTULO V TER	Delitos Informáticos	26 de noviembre de 2019

4. Adicionalmente, desde hace más de una década se han promulgado otras Leyes Federales que estipulan de manera preventiva y correctiva, obligaciones en materia de ciberseguridad, algunas de ellas son:

NORMA	**ARTÍCULO (S)**	**NOMENCLATURA**	**FECHA DE PUBLICACIÓN**
Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Artículos 19, 20 y 21 CAPÍTULO XI	Medidas de Seguridad, deberes de seguridad y confidencialidad De los Delitos en Materia del Tratamiento Indebido de Datos Personales	5 de julio de 2010

Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares	Artículo 50 Artículo 52 Capítulo III	Obligaciones del encargado Tratamiento de datos personales en el denominado cómputo en la nube De las Medidas de Seguridad en el Tratamiento de Datos Personales	21 de diciembre de 2011
Ley Federal de Telecomunicaciones y Radiodifusión	Artículos 2, 56, 117, 145, 150, 183, 185, 189, 190,		14 de julio de 2014
Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados	Artículo 3, fracciones XIV, XX, XI, XX, XXIII, Artículo 12 Artículos 30, 31, 32, 33, 34, 35, 36, 37, 38, 39 y 42	 Deber de seguridad	26 de enero de 2017

5. Los ataques a infraestructuras gubernamentales son una de las razones por las cuales se ha hablado de la materia de ciberseguridad como prioridad al final de esta administración del gobierno federal. Ha habido un incremento en el número de ciberataques que han sufrido diversas entidades gubernamentales, tanto federales como estatales, comprometiendo infraestructuras críticas, como fue el caso del ciberataque de *Ransomware* en contra de PEMEX en el 2019[3], varios ciberataques dirigidos al SAT[4] en lo que va del sexenio[5], y aquel del que no ha podido recuperarse CONAGUA[6,7], entre otros. Sin duda alguna, el más famoso que aceleró el debate legislativo en torno a la materia de Ciberseguridad, ha sido el sufrido por SEDENA[8], mejor conocido como Guacamaya *Leaks*[9], de proporciones aún inestimables, por la cantidad de información comprometida, mucha de ella sensible o de seguridad nacional.

6. Estos ciberataques se han cometido a pesar de que existe la legislación vigente tendiente a prevenir y combatir estos delitos. Esta situación deja claro que no es precisamente legislación lo que falta, sino muchos otros elementos, tales como presupuesto, capacitación, enfoque de gestión de riesgos, y correcta implementación de las medidas obligatorias por Ley, entre otras.

---

[3] El rescate por el hackeo a Pemex es el segundo mayor por *ransomware*.

[4] SAT Servicio de Administración Tributaria
[5] SAT ha recibido más ciberataques con AMLO que en otro sexenio.

[6] Conagua, Comisión Nacional del Agua
[7] Conagua bajo ataque cibernético: Resaltando el déficit de la ciberseguridad en el sector del agua en México.

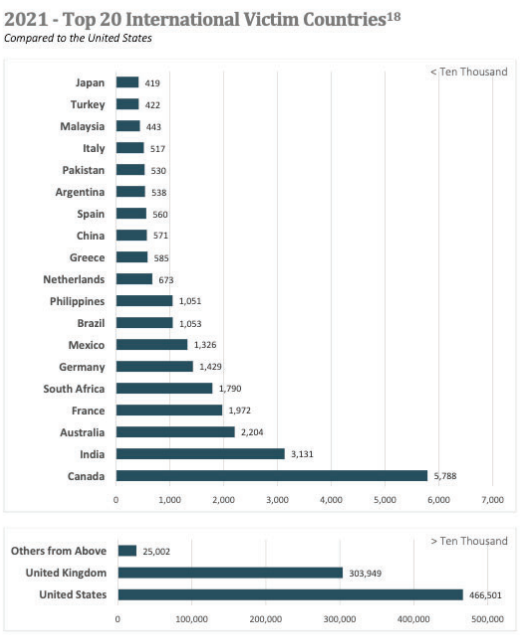
[8] SEDENA Secretaría de la Defensa Nacional
[9] Guacamaya *Leaks*: 5 revelaciones del hackeo masivo que sufrió el ejército de México - BBC News Mundo.

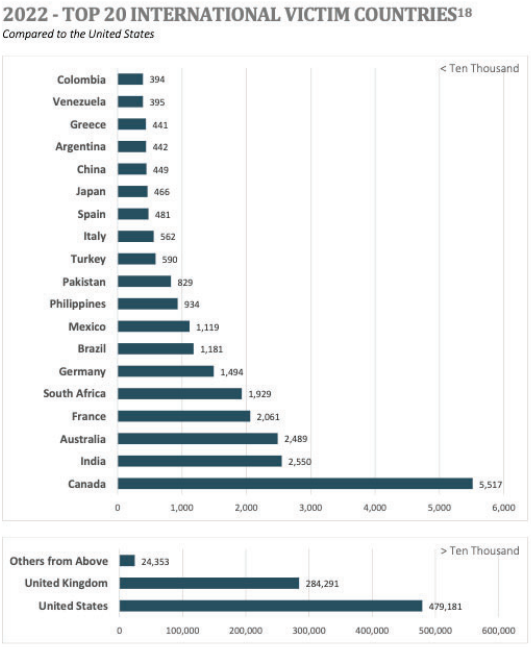
II. SITUACIÓN ACTUAL E INICIATIVAS

2.1 ESTADO DE LA CIBERSEGURIDAD EN MÉXICO

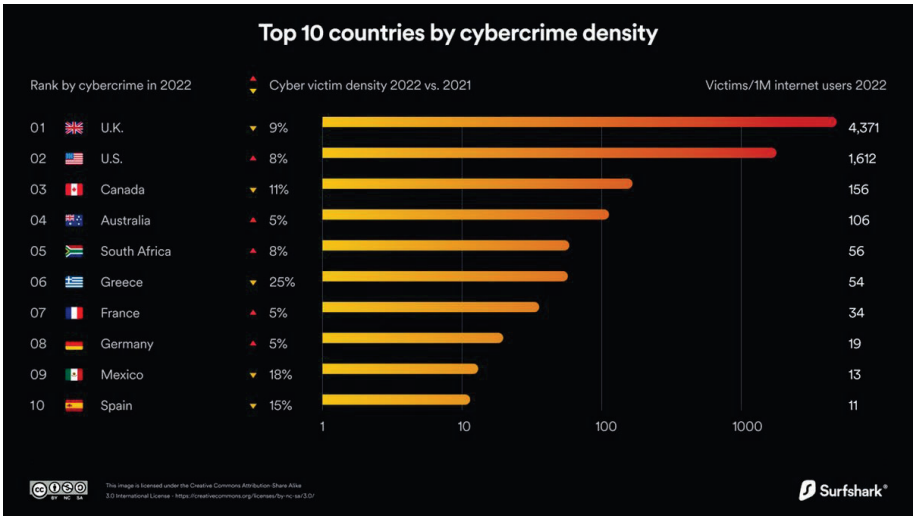
El estado de la ciberseguridad que guarda México actualmente es preocupante tanto del punto de vista nacional como el internacional. Cada año o dos, el FBI[10] publica su "*Internet Crime Report*"[11], el cual es un reporte completo acerca del estado que guarda la ciberseguridad en Estados Unidos en cada uno de sus estados, por tipo de crimen y también frente a otros países, y elabora estadísticas que muestran cuáles son los países que conforman el Top 20 por número de víctimas. En los últimos 3 años, México ha ocupado los lugares 7, 8 y 9 según el año en dicho reporte, junto con Brasil el cual se disputa el lugar año con año, a continuación, mostramos las gráficas de 2020, 2021 y 2022 tomadas de ese reporte:

[10] FBI *Federal Bureau of Investigation*
[11] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf
https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf





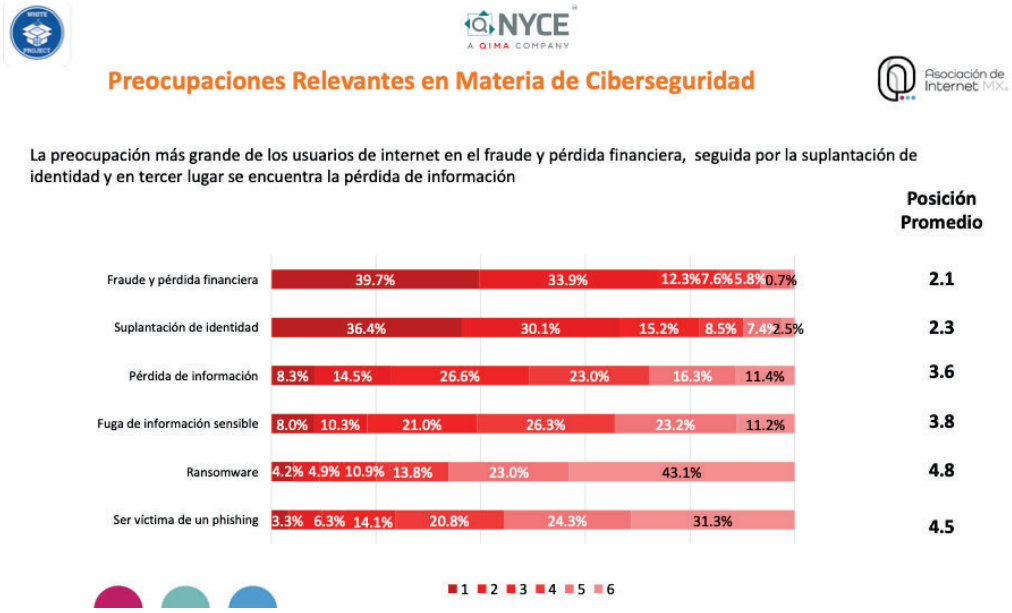
De igual manera, en la siguiente estadística elaborada por Surfshark[12] respecto al 2022, se muestra cómo México forma parte del Top 10 de países por densidad de víctimas del cibercrimen:



[12] https://surfshark.com/research/data-breach-impact/statistics

Respecto a las estadísticas en México, el último reporte de incidencia delictiva a nivel federal al mes julio de este 2023 publicado por el Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública, no muestra específicamente aquellos delitos que hayan sido cometidos a través de Internet o utilizando alguna otra tecnología[13].

Sin embargo, se cuenta con algunos estudios recientes elaborados por la Asociación de Internet MX, entre ellos: el "Estudio sobre ciberseguridad en empresas, personas usuarias de Internet y padres de familia en México"[14] cuya segunda edición contiene las siguientes tablas acerca de las preocupaciones relevantes en materia de ciberseguridad, el número de víctimas reportado por tipo de conducta y las experiencias negativas que se han presentado en menores de edad, entre otros aspectos importantes:

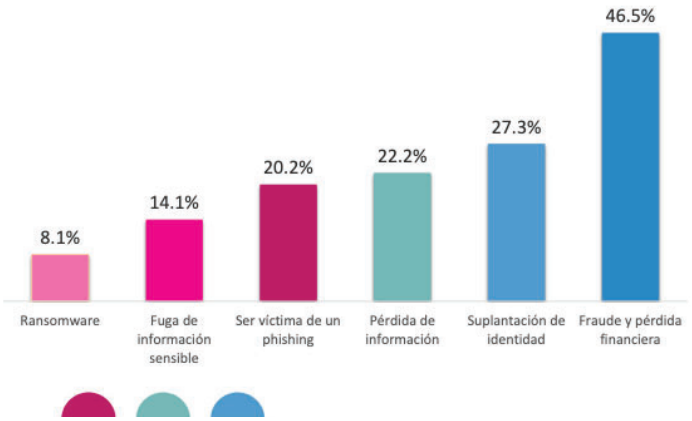


[13] https://drive.google.com/file/d/17tCln7WfBE4O3Ullv1q3AJYmvxehotC-/view
[14] https://irp.cdn-website.com/81280eda/files/uploaded/Encuesta Ciberseguridad 2022 pública 20230119.pdf

Victimas de Alguna Vulneración

Delincuentes han migrado al mundo digital para cometer delitos

- **22.1% de los usuarios han sido víctimas de alguna vulneración en los últimos 12 meses**



Afectaciones reportadas por parte de los usuarios:

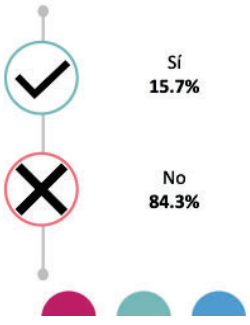
- Principalmente de pérdida de información, fraudes y pérdidas financieras
- 1 de cada 3 víctimas ha sufrido de suplantación de identidad, lo cual puede derivar en otro tipo de problemas legales

Experiencias Negativas con terceros a través de internet por parte de sus hijas o hijos

Baja proporción de menores que perciben haber tenido experiencias negativas mediante internet **(15.7%)**

- Aproximadamente, **7 de cada 10** hijos reportan acoso por parte de otros menores de edad
- Las Redes sociales y los servicios de mensajería son los principales medios por los que se han visto afectados

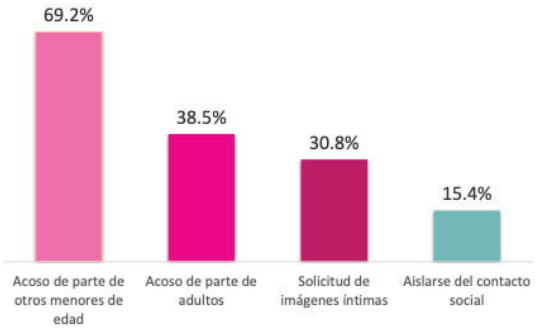
¿Sus hijas o hijos han tenido experiencias negativas con terceros a través de internet?



Sí **15.7%**

No **84.3%**

Experiencias negativas han tenido sus hijas o hijos con terceros a través de internet



Los incidentes con terceros se han dado a través de:

Redes sociales **46.2%**

Servicios de mensajería **46.2%**

Videojuegos en línea **23.1%**

Asimismo, este mismo año se presentó el "Estado de las Políticas Públicas y Regulación sobre la Ciberseguridad para NNA en México. 2022". Ese reporte nos presenta estadísticas muy relevantes de incidencia en ese grupo poblacional[15].

Por lo anterior, podemos concluir en este rubro que el estado que guarda la ciberseguridad en nuestro país es preocupante y debe atenderse desde una perspectiva multifactorial, en lo particular, consideramos de relevancia la actuación del Instituto conforme a su normativa aplicable, en particular la Ley y los Lineamientos para la gestión de tráfico y administración de red a que deberán sujetarse los concesionarios y autorizados que presten el servicio de acceso a Internet.

2.2 INICIATIVAS IDENTIFICADAS

En este momento, tanto nivel federal como estatal se tienen identificadas alrededor de 24 iniciativas en los congresos locales y el federal.

Una de las principales razones por las que, a pesar de haber existido múltiples intentos en otras legislaturas y sexenios por contar con una normativa enfocada al cien por ciento en la materia, es el desconocimiento del funcionamiento de la tecnología, por ejemplo, la presentada en octubre del 2015 por el entonces Senador del PRI Omar Fayad[16], que prácticamente criminalizaba a la tecnología en sí misma al darles el carácter de "arma informática"; pero más aún, atentaba contra derechos fundamentales como la libertad de expresión al incorporar los tipos penales de terrorismo informático, la intimidación, divulgación indebida de información y una recopilación excesiva de información de los

[15] https://irp.cdn-website.com/81280eda/files/uploaded/Internet_Seguro_para_Tod_s_AIMX_octubre.2022.pdf
[16] Omar Fayad retira iniciativa contra ciberdelitos

usuarios. Evidentemente, al ser ampliamente criticada por los medios de comunicación, la industria y los propios usuarios, tuvo que retirar su iniciativa.

Llama la atención que el término Delito Cibernético o Ciberdelito, ya se encuentra definido en el documento de la Estrategia Nacional de Ciberseguridad, que no ha quedado sin efecto o ha sido modificado, entendiendo como éste a las *"Acciones delictivas que utilizan como medio o como fin a las tecnologías de la información y comunicación y que se encuentran tipificados en algún código penal u otro ordenamiento nacional."*

Entonces, la necesidad imperiosa de contar con una normativa enfocada a sancionar estas conductas, que ya se encuentran contempladas en diversos ordenamientos, hace plantearnos la verdadera necesidad de contar con una Ley Federal en la materia, y más importante aún, corroborar que se cuenten con las facultades precisas para un proyecto de norma con alcances tan amplios y dispersos.

III. CONSIDERACIONES GENERALES

De manera general consideramos que cualquier regulación que se genere o modifique el marco regulatorio existente debe ajustarse a ciertos criterios basados tanto en la Constitución Política de los Estados Unidos Mexicanos como en instrumentos internacionales de los que México es parte, así como en algunos ejemplos de derecho comparado. Por lo anterior, sería deseable:

1. Generar la normativa conforme al ámbito de competencias previsto en el artículo 73 Constitucional fracción XXI, cuidando que no se invadan competencias del fuero común, por lo que se estima

relevante que se orienten los trabajos hacia una Ley General y no una Ley Federal;

2. Que conforme al artículo 1 Constitucional párrafos segundo y tercero, se respeten, protejan y garanticen los derechos humanos de conformidad con los principios de universalidad, interdependencia, indivisibilidad y progresividad favoreciendo en todo momento la protección más amplia;
3. Que su redacción no genere duplicación, antinomias o conflictos de aplicación normativa, al pretender incorporar materias especiales que ya se encuentran debidamente reguladas, tales como la protección de datos personales, la propiedad intelectual y las telecomunicaciones;
4. Que se delimite perfectamente el ámbito de facultades y competencias de las autoridades que pretendan crearse, respetando el ámbito de las existentes, con la finalidad de prevenir una futura controversia constitucional, hacer un uso eficiente de los recursos públicos, y
5. Que se garantice el respeto al derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal conforme a las obligaciones contraídas por el Gobierno de México en el Convenio 108 (Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal).

En particular nos inquieta la premura que se ha manifestado públicamente para que en el presente periodo de sesiones se dictamine y posteriormente vote en el pleno una Ley de Ciberseguridad, siendo que no se tiene un proyecto debidamente analizado y maduro.

En primer lugar consideramos que se debe definir si será una propuesta de Ley de carácter federal que contempla la incorporación de diversos tipos penales que no son facultad exclusiva del legislador federal o que incluso ya se encuentran tipificados en los ordenamientos locales, podrían generar un entorno óptimo para el planteamiento de controversias constitucionales, además esto se refuerza al invadir las esferas de competencia de los Órganos Constitucionales Autónomos como el IFT o el Instituto Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI).

Estudiando las iniciativas que se encuentran en este momento analizándose, no queda claro si en realidad se tratará de una Ley General o Federal.

En una de las iniciativas más socializadas, le son supletorias, entre otras, las leyes en materia de protección de datos personales y la Ley Federal de Telecomunicaciones y Radiodifusión, sin embargo, plantea cuestiones que invaden el ámbito de facultades constitucionales otorgadas al IFT, por ejemplo, en el TÍTULO CUARTO, PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES CAPÍTULO I.

Aunado a lo anterior, se menciona en la exposición de motivos que "*Contar con una Ley Federal de Ciberseguridad es imprescindible para dar atribuciones jurídicas a la entidad encargada de la ciberseguridad en el país y certidumbre jurídica a ciudadanos y autoridades para la atención de los delitos cibernéticos.*"

Lo cual es impreciso, ya que las policías cibernéticas llevan operando más de diez años, incluso, el sexenio pasado se creó el Modelo Homologado de Unidades de Policía

Cibernética[17] para profesionalizar a todas las unidades del país y que trabajaran de forma estandarizada.

Asimismo, miembros de diversas organizaciones tales como la Cámara Internacional de Comercio, la propia Asociación de Internet MX y la CANIETI[18] que albergan a algunos de los sujetos regulados, han manifestado públicamente a través de un comunicado[19] el día 5 de septiembre, sus inquietudes respecto de esta iniciativa y de la urgencia con la que pretende aprobarse en este período de sesiones con base en la Agenda Legislativa del Partido MORENA[20].

A continuación, se presenta una tabla con observaciones precisas que consideramos importantes:

ARTÍCULO	CONTENIDO	OBSERVACIONES
Artículo 1 fracciones IX y X	Establecer las bases para sancionar conductas ilícitas en materia de Ciberseguridad; y	Estas conductas ya se encuentran tipificadas en diversos ordenamientos jurídicos estatales, lo cual además de ser redundante

[17] Modelo homologado de unidades de policía cibernética

[18] Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la información (CANIETI)

[19] https://newsreportmx.com/2023/09/05/la-pone-en-riesgo-derechos-humanos-e-incumple-obligaciones-internacionales-en-la-materia/

[20] https://infosen.senado.gob.mx/sgsp/gaceta/65/2/2023-02-09-1/assets/documentos/Angenda_Legislativa_MORENA_2do_Ano_de_Ejercicio.pdf

	Penalizar actividades cibernéticas ilegales y otorgar atribuciones a las autoridades encargadas de perseguirlas, con respeto a las garantías procesales, el derecho a la intimidad, las libertades civiles y los derechos humanos	generaría un conflicto competencial nocivo para los sujetos pasivos y para el Estado de Derecho.
Artículo 3	Glosario o definiciones de la Ley	Remitir a las leyes que han previamente definido estos conceptos o bien, a estándares internacionales evitaría generar confusión en la aplicación de la norma.
CAPÍTULO I DE LA COMISIÓN INTERSECRETARIAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN, Y DE LA SEGURIDAD	Artículo 10. La Comisión podrá invitar a sus sesiones, a propuesta de cualquiera de sus integrantes, a: I. Titulares de Tecnologías de Información y Comunicaciones, y Seguridad de la Información o	Si bien está previsto invitar a representantes de los Órganos Constitucionales Autónomos, el Instituto Federal de Telecomunicaciones debería incorporarse por Ley como invitado permanente; ya que, por sus atribuciones su

DE LA INFORMACIÓN	equivalentes de otras entidades de la Administración Pública Federal; II. Representantes de los órganos constitucionales autónomos;	participación es fundamental en las tareas encomendadas a esta CITICSI.
CAPÍTULO II **DE LA AGENCIA NACIONAL DE CIBERSEGURIDAD**	Artículo 13. La Agencia Nacional de Ciberseguridad, dependerá directamente del Titular del Ejecutivo Federal. La Agencia contará con las siguientes atribuciones: XIX. Integrar y mantener actualizado un Catálogo Nacional de Infraestructuras Críticas de Información; así como salvaguardar su confidencialidad, integridad y disponibilidad;	Hay una invasión de competencias del Instituto Federal de Telecomunicaciones y una duplicación de actividades. Lo anterior es contrario a la eficiencia para el uso de recursos públicos y tiene otras desventajas operativas; por ejemplo, no establece reglas claras para la baja inmediata de proveedores de servicio o administradores, de direcciones IP, aplicaciones, dominios y sitios de internet.

	XXV. Establecer mecanismos permanentes de comunicación con los operadores de las Infraestructuras Críticas de Información para, en su caso, promover la emisión de alertas tempranas; XXX. Solicitar la baja inmediata a proveedores de servicio o administradores, de direcciones IP, aplicaciones, dominios y sitios de internet a través de los cuales se realicen conductas ilícitas; y	Esto derivaría también en potenciales actos de autoridad inconstitucionales, así como en posibles conflictos competenciales.
CAPÍTULO III **DE LA ESTRATEGIA NACIONAL DE CIBERSEGURIDAD**	Artículo 14. Corresponderá a la Agencia Nacional de Ciberseguridad, formular, conducir e impulsar el cumplimiento de una Estrategia Nacional de Ciberseguridad, misma que será actualizada de acuerdo con el Sistema Nacional de Planeación, y contendrá al menos, lo siguiente:	De estas disposiciones también se vislumbran posibles conflictos competenciales.

	VII. Acciones de capacitación, asistencia, intercambio de información, tecnología y cualquier otro fin relacionado con el análisis y desarrollo de esquemas estandarizados de Ciberseguridad, así como con el uso y protección de las Tecnologías de la Información y Comunicaciones; VII. Acciones para la prevención de riesgos, amenazas y vulnerabilidades de los sistemas informáticos, digitales y de las telecomunicaciones tanto públicas como privadas; Artículo 15. Las acciones contempladas en la Estrategia Nacional de Ciberseguridad serán de carácter obligatorio para las dependencias y entidades de la Administración Pública Federal y de carácter indicativo para las entidades federativas, municipios, demarcaciones territoriales de la Ciudad	

	de México y para los tres órdenes de gobierno, órganos constitucionales autónomos y particulares.	
TÍTULO CUARTO PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES CAPÍTULO I DE LOS DERECHOS Y OBLIGACIONES	Artículo 44. Conforme a los derechos consignados en la Constitución Política de los Estados Unidos Mexicanos, todas las personas tendrán los siguientes derechos digitales: I. Acceder a servicios de tecnologías de la información y comunicación de calidad, en un entorno de inclusión digital, neutralidad e igualdad en la red, así como libertad para utilizar el sistema y hardware que deseen, siempre y cuando sea lícito; II. A la no discriminación para el acceso e interacción en medios digitales;	En general, todo el capítulo I y el II de este Título Cuarto parecen innecesarios toda vez que son derechos previamente reconocidos en la Constitución y regulados en las normas en la materia, por lo que no habría lugar a incorporarlos en esta normativa, además de que, en algunos puntos invade facultades exclusivas del IFT y el INAI.

	III. A la libertad de expresión en medios digitales y derecho de acceso a la información; IV. A la protección de sus datos personales en el entorno digital, en términos de lo dispuesto en la Ley aplicable en la materia; V. A la libertad de conciencia y de religión en el entorno digital; VI. A la libertad de reunión y asociación en línea; VII. A la privacidad digital; VIII. A la protección de la personalidad virtual; IX. A contar con una identidad digital; X. A una vida digital libre;	

	XI. A la defensa de su integridad en medios digitales; XII. A la protección de sus datos digitales; XIII. A recibir educación, acceso al conocimiento, cultura y trabajo a través de Internet y otros medios digitales; XIV. A la reserva de la información que se brinde a la autoridad de aquellos datos sobre incidentes cibernéticos en los que hayan sido víctimas; XV. A la protección de los derechos de los teletrabajadores en términos de lo dispuesto en la Ley aplicable en la materia; XVI. A la protección de los derechos de los consumidores en Internet, en	

	términos de lo dispuesto en la Ley aplicable en la materia; XVII. A que la información recopilada por las empresas que brindan servicios tecnológicos no sea utilizada para fines distintos a los autorizados; XVIII. Al comercio electrónico legal a través del ciberespacio en términos de lo dispuesto en la Ley aplicable en la materia; y XIX. Las demás que le confieran esta Ley u otros ordenamientos aplicables. Artículo 45. Las obligaciones de los usuarios de servicios digitales son: I. Respetar los derechos de los demás usuarios;	

	II. Utilizar los servicios digitales con responsabilidad y sólo para fines lícitos; III. Utilizar la identidad digital sólo para fines lícitos; IV. Acceder a los servicios de tecnologías de información y comunicaciones, así como cualquier otro servicio digital de manera legal; y V. Cooperar con las autoridades competentes, ante cualquier investigación en materia de ciberseguridad.	
TÍTULO QUINTO DE LA PRESTACIÓN DE SERVICIOS, USO DE INFRAESTRUCTURA DIGITAL Y	Artículo 53. Los proveedores de servicios de infraestructura digital, plataformas de redes sociales, comunidades de videojuegos en línea, *streaming*, plataformas de entretenimiento en línea y telecomunicaciones que operen en territorio nacional están obligados a	Varias de las obligaciones que se imponen en los términos de este título a los prestadores de servicios de telecomunicaciones pueden considerarse excesivas y van más allá de lo dispuesto

TELECOMUNICACIONES	atender todo mandamiento por escrito, fundado y motivado de la autoridad competente en los términos que establezca la Constitución Política de los Estados Unidos Mexicanos y demás leyes. Para lo cual estarán sujetos a las siguientes obligaciones específicas: I. Contar cuando menos con una representación legal con presencia física en el territorio nacional; II. Contar con una unidad de cumplimiento para la atención y respuesta de incidentes de ciberseguridad; III. Registrarse ante la Agencia Nacional de Ciberseguridad; IV. Establecer medidas de autenticación y cifrado para el acceso a servicios donde se ingresen datos personales;	en la Ley que regula su actividad; es decir, la LFTR e incluso parecieran desconocer las obligaciones y marco legal para la colaboración con la justicia prevista en el Título Octavo de la LFTR.

	V. Establecer en sus servicios medidas de seguridad tecnológica, que permitan salvaguardar la integridad, confidencialidad y disponibilidad de la información de los usuarios; VI. Notificar ante el CERT-MX y a la Agencia, cualquier incidente de ciberseguridad en la operación o prestación de su servicio que represente un riesgo relevante de conformidad con los lineamientos a los que hace referencia el artículo 38 de la presente Ley; VII. Dar aviso a los usuarios, respecto a incidentes cibernéticos que puedan tener impacto en la privacidad o protección de sus datos, o en la continuidad del servicio;	

	VIII. Privilegiar que la información de los usuarios se encuentre almacenada en territorio nacional; IX. En caso de que la información contenga datos que pudieran vulnerar la seguridad nacional, deberá almacenarse en territorio nacional; X. Informar a los usuarios de forma permanente, fácil, directa y gratuita, sobre los diferentes medios de carácter técnico que aumenten los niveles de seguridad de la información y permitan, entre otros, la protección frente a códigos maliciosos; XI. Informar sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para los menores de edad;	

	XII. Facilitarán información a los usuarios acerca de las posibles responsabilidades en que puedan incurrir por el uso indebido de sus servicios, en particular, para la comisión de delitos y vulneración de la legislación en materia de propiedad intelectual e industrial; XIII. Dar de baja direcciones IP, aplicaciones, dominios y sitios de internet dentro de las 72 horas posteriores a la notificación que le realicen la Agencia, la Fiscalía General de la República, CERT-MX y autoridades judiciales competentes para su inhabilitación XIV. Conservar la información sobre las IP y datos de registro; y XV. Establecer un acuerdo de corresponsabilidad y confidencialidad en el caso de	

	realizar actos de subcontratación o intermediación sobre el uso o distribución de bases de datos e información digital. Lo anterior, sin perjuicio en lo dispuesto por la Ley Federal de Telecomunicaciones y Radiodifusión y demás leyes en la materia. Artículo 54. De conformidad con el principio de cooperación internacional, los proveedores de servicios y plataformas constituidas en el extranjero que tengan y operen plataformas, sistemas de información, productos o servicios digitales a través de Internet o algún otro medio tecnológico que cuenten con usuarios registrados y activos en México, podrán ser requeridos mediante orden judicial, a colaborar con las autoridades mexicanas de procuración de justicia o encargadas de la seguridad pública y nacional, según	

	corresponda en términos de las disposiciones aplicables en la materia. Para efectos del párrafo anterior, los proveedores antes citados, deberán sujetarse a lo dispuesto en el Título Octavo "De la Colaboración con la Justicia", de la Ley Federal de Telecomunicaciones y Radiodifusión. Artículo 55. Los proveedores de servicios bancarios y financieros están obligados a establecer las medidas de Ciberseguridad necesarias para evitar fraudes electrónicos en las plataformas y los servicios que prestan. Artículo 56. Los proveedores que desarrollen, operen, comercialicen o pretendan comercializar la tecnología a que se refiere el artículo 3 fracción XXXV, dentro del territorio nacional, están obligados a inscribirse en el Registro Nacional de Proveedores de Tecnología	

	para Intervención de Comunicaciones y, a comercializar dicha tecnología únicamente con las autoridades con competencia legal. Artículo 57. El Centro Nacional de Inteligencia conformará el Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones, en términos de lo dispuesto en el Reglamento de la presente Ley. Artículo 58. La información contenida en el Registro Nacional de Proveedores de Tecnología para Intervención de Comunicaciones será tratada con el carácter de reservada por motivos de Seguridad Nacional, debido a que su revelación indebida podría actualizar o potenciar una amenaza que ponga en riesgo la integridad, permanencia y estabilidad del Estado mexicano.	

	Artículo 59. El uso de Tecnología para Intervención de Comunicaciones es exclusivo para las Instituciones de seguridad pública o nacional; las autoridades observarán en todo momento el respeto a las formalidades legales, y los derechos humanos, por lo que su venta queda prohibida para fines distintos a los establecidos.	
SECCIÓN TERCERA De la interceptación de datos	Artículo 69. Quien a través de cualquier medio o método, intercepte sin una orden judicial, cualquier tipo de datos informáticos, electrónicos telemáticos, incluidas las emisiones electromagnéticas y radiofrecuencias, originadas y/o provenientes desde otro sistema o equipo o realizadas dentro del mismo, se le impondrá de diez a veinte años de prisión y multa de diez mil a veinte mil unidades de medida de actualización. Artículo 70. A quien sin tener facultades legales para tal efecto adquiera o	Además de ser poco claros los tipos penales, lo cual haría impugnable su aplicación y sanción, se invaden las facultades del IFT.

	arriende Tecnología para Intervención de Comunicaciones, se le impondrán de diez a veinte años de prisión y multa de diez mil a veinte mil unidades de medida de actualización. Artículo 71. A quien sin estar registrado para tal efecto comercialice Tecnología para Intervención de Comunicaciones en territorio nacional, se le impondrán de diez a veinte años de prisión y multa de diez mil a veinte mil unidades de medida de actualización	

IV. RECOMENDACIÓN

Por lo anteriormente expuesto, este Consejo Consultivo recomienda que el Instituto participe de forma proactiva buscando que la redacción final de la norma que se desarrolle en pro de la ciberseguridad:

(i) no invada competencias que le corresponden en exclusiva y como garante de los derechos de los usuarios en términos del artículo 6 Constitucional Apartado B, fracción V; y los artículos 7 y 145 fracción III de la Ley Federal de Telecomunicaciones y Radiodifusión;

(ii) considere la participación del Instituto en el ámbito de su competencia para contribuir a la ciberseguridad en el país con sus capacidades regulatorias, humanas y técnicas, así como para coadyuvar y promover la ciberseguridad en el país;

(iii) promueva la coordinación de las autoridades a nivel nacional e internacional;

(iv) no duplique las obligaciones en materia de colaboración con la justicia que prevé la Ley Federal de Telecomunicaciones y Radiodifusión en su Título Octavo, y

(v) considere la importancia de tener presente el desarrollo tecnológico y la innovación por una parte para garantizar que sus disposiciones sean generales y abstractas y por otra para que las medidas que se adopten no sean excesivas y generen obstáculos a la innovación.

Lilia Eurídice Palma Salas

Presidenta del VII Consejo Consultivo

Mtra. Rebeca Escobar Briones

Secretaria del Consejo Consultivo

La Recomendación fue aprobada por el VII Consejo Consultivo del Instituto Federal de Telecomunicaciones por unanimidad de votos de los consejeros: Alejandro Ildefonso Castañeda Sabido, Sara Gabriela Castellanos Pascacio, Ernesto M. Flores-Roux, Mario Germán Fromow Rangel, Gerardo Francisco González Abarca, Misha Leonel Granados Fernández[21], Erik Huesca Morales, Salma Leticia Jalife Villalón, Luis Miguel Martínez Cervantes, Lucía Ojeda Cárdenas, Eurídice Palma Salas y Cynthia Gabriela Solís Arredondo. Lo anterior, en la I Sesión Extraordinaria celebrada el 21 de septiembre de 2023, mediante Acuerdo CC/VII/IFT/210923/28, en términos del artículo 17 último párrafo de las Reglas de Operación del Consejo Consultivo del Instituto Federal de Telecomunicaciones.

La Recomendación fue desarrollada por la consejera Cynthia Gabriela Solís Arredondo, con la contribución de los consejeros Sara Gabriela Castellanos Pascacio, Eurídice Palma Salas y Luis Miguel Martínez Cervantes.

[21] El consejero Misha Leonel Granados Fernández emitió su voto favorable vía correo electrónico el 4 de octubre de 2023.

ANEXO

Se resaltan los elementos que pueden significar un riesgo sustancial para los derechos humanos en relación con las limitaciones, restricciones o medidas de control que se tendrían que implementar a las telecomunicaciones.

INICIATIVA	CONTENIDO	FECHA
INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD La suscrita Juanita Guerra Mena Diputada Federal integrante del Grupo Parlamentario de MORENA en la LXV Legislatura	LEY GENERAL DE CIBERSEGURIDAD TÍTULO PRIMERO DISPOSICIONES GENERALES Capítulo Único Disposiciones Generales Artículo 4. Para garantizar la protección de los derechos humanos de los cibernautas, las autoridades deberán atender los siguientes principios: … … V. La vigilancia e intervención de comunicaciones privadas deben estar fundadas en la legislación aplicable, atendiendo a los principios de necesidad y proporcionalidad, utilizando mecanismos de control, transparencia y rendición de cuentas; VI. Deberán promover el mejoramiento y adopción del cifrado como medida para mitigar riesgos y fortalecer la Ciberseguridad;	03-10-22

	X. Las políticas de Ciberseguridad deben sustentarse en la disponibilidad continua de la conectividad, y XI. La regulación de la vigilancia y monitoreo de la red y de la investigación y persecución de los ciberdelitos, se hará con absoluto respeto a los derechos humanos y garantías individuales. Artículo 5. Para los efectos de la presente Ley, se entiende por: … VII. Ciberespacio.- Es un entorno digital global constituido por redes informáticas y de telecomunicaciones, en el que se comunican e interactúan las personas y permite el ejercicio de sus derechos y libertades como lo hacen en el mundo físico; XIX. Hiperconectividad.- Conexión a los sistemas de información a través de diferentes dispositivos; XX. Internet.- Conjunto de redes de telecomunicaciones que a través de la red pública de telecomunicaciones ofertan servicios y comunicaciones digitales;	

	XXVII. TIC.- Tecnologías de Información y Comunicaciones, que comprende los equipos de cómputo, programas de computación, servicios y dispositivos de impresión que sean utilizados para almacenar, procesar, convertir, proteger, transferir y recuperar información, datos, voz, imágenes y video; XXVIII. Virtual.- Todo lo que tiene lugar en los medios digitales,… TÍTULO SEGUNDO DE LOS ÁMBITOS DE COMPETENCIA EN CIBERSEGURIDAD Capítulo I Distribución de competencias Artículo 7. Las autoridades en materia de Ciberseguridad son: V. Las demás que con ese carácter determinen la presente Ley y otras disposiciones legales aplicables. Artículo 10. Son auxiliares en materia de Ciberseguridad, cuando sean requeridos por algunas de las autoridades en el cumplimiento de sus atribuciones, los siguientes:	

	V. Las demás que dispongan los ordenamientos legales aplicables, cuando su colaboración resulte necesaria para el cumplimiento de los fines de esta Ley. Sección Primera De la Dirección General de Investigación Cibernética y Operaciones Tecnológicas Artículo 16. Son atribuciones de la Dirección General de Investigación Cibernética y Operaciones Tecnológicas, en materia de Ciberseguridad: II. Monitorear la red pública de Internet con el fin de prevenir conductas delictivas; III. Coordinar y autorizar los métodos de análisis y monitoreo en medios electrónicos u otras plataformas tecnológicas que pudieran ser utilizadas para cometer un hecho probablemente constitutivo de delito; X. Solicitar la baja de información, sitios o páginas electrónicas que representen un riesgo, amenaza o peligro para la seguridad ciudadana, conforme a las disposiciones aplicables;	

	XXIII. Desarrollar mecanismos para la instalación de equipo tecnológico para vigilancias en puntos fijos y móviles;	
INICIATIVA DE LA SENADORA JESÚS LUCÍA TRASVIÑA WALDENRATH, CON PROYECTO DE DECRETO POR EL QUE SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD Y SE DEROGAN DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL	LEY GENERAL DE CIBERSEGURIDAD LIBRO PRIMERO TÍTULO PRIMERO CAPÍTULO I Disposiciones Preliminares Artículo 1.- La presente Ley es reglamentaria de los artículos 6 y 21 de la Constitución Política de los Estados Unidos Mexicanos en materia de Ciberseguridad y tiene por objeto regular la integración, organización y funcionamiento de la Comisión Nacional de Ciberseguridad y de la Agencia Nacional de Ciberseguridad, así como establecer la distribución de competencias y las bases de coordinación entre la Federación, las Entidades Federativas y los Municipios, en esta materia. XXI. Delitos cibernéticos o ciberdelitos: Acciones delictivas que utilizan como medio o como fin a las tecnologías de la información y comunicación y que se encuentran tipificados en algún código penal u otro ordenamiento nacional. XXII. Dispositivo: Aparato, artificio, mecanismo, artefacto, órgano, periférico, gadget, producto,	23 de marzo de 2021

	elemento de un sistema o componente electrónico. Dispositivo de Acceso: Es toda tarjeta, placa, código, número, u otros medios o formas de acceso, a un sistema o parte de éste, que puedan ser usados independientemente o en conjunto con otros dispositivos, para lograr acceso a un sistema de información o a cualquiera de sus componentes. XXIV. Dominio: Espacio de aplicabilidad intangible que define el campo de acción del ciberdelito. XXV. Nombre de dominio: Es un nombre fácil de recordar asociado a una dirección física de internet. XXVI. Emisiones Electromagnéticas: Combinación de campos eléctricos y magnéticos oscilantes, que no necesitan un canal o medio para su propagación de un lugar a otro. XXVII. Entorno Digital: Conjunto de canales, plataformas y herramientas que disponen cualquier individuo, marcas o negocios para tener presencia en Internet. Internet: Conjunto de redes de telecomunicaciones que a través de la red pública de telecomunicaciones ofertan servicios y comunicaciones digitales	

	XLIV. Proveedor de Servicios de Internet: Es la empresa que proporciona una conexión de acceso a Internet a sus clientes (ISP), que incluye tránsito y registro de nombres de dominio. XLV. Proveedor de contenidos en Internet: Persona física o moral que brinda servicios, aplicaciones, almacenamiento, infraestructura y soporte técnico de diversos productos basados en Internet, entre otros, bajo las políticas de privacidad y condiciones que él mismo establece. XLVI. Radiofrecuencia: También denominado espectro de radiofrecuencia, es la distribución energética del conjunto de las ondas electromagnéticas, es decir, la radiación electromagnética que emite una antena de radiocomunicación. XLVIII. Red Pública de Internet: Es un tipo de red que puede usar cualquier persona y no como las redes que están configuradas con clave de acceso personal. XLIX. Red Social: Comunidad virtual que permite la interacción entre personas u organizaciones que se conectan a partir de intereses o valores comunes, basados en la estructura de conocido ha conocido.	

	LX. Sistema de Telecomunicaciones: Conjunto de dispositivos relacionados, conectados o no, cuyo fin es la transmisión, emisión, almacenamiento, procesamiento y recepción de señales, señales electromagnéticas, signos, escritos, imágenes fijas o en movimiento, video, voz, sonidos, datos o informaciones de cualquier naturaleza, por medio óptico, celular, radioeléctrico, electromagnético o cualquiera otra plataforma útil a tales fines. Este concepto incluye servicios de telefonía fija y móvil, servicios de valor agregado, televisión por cable, servicios espaciales, servicios satelitales y otros. LXIII. Sistema Telemático: Sistema que combina los sistemas de telecomunicaciones e informáticos como método para transmitir la información. LXIV. Tecnologías de la Información y Comunicación: Conjunto de herramientas, sistemas, programas, recursos, procedimientos que sirven para el almacenamiento y facilitar la emisión, acceso y tratamiento de la información mediante códigos variados que pueden corresponder a textos, imágenes, videos, sonidos, entre otros.	

	LXIX. Wi Fi: Es una red de dispositivos inalámbricos interconectados entre sí y generalmente conectados a Internet a través de un punto de acceso inalámbrico. Se trata de una red LAN que no utiliza un cable físico para el envío de la información. Tecnología de interconexión de dispositivos electrónicos de forma inalámbrica, que funciona en base al estándar 802.11, que regula las transmisiones inalámbricas. Capítulo IV De los delitos a la propiedad intelectual Artículo 39.- Cuando las conductas descritas en la Ley Federal de Derechos de Autor y en la Ley de Propiedad Industrial, vigentes al momento de los hechos, se cometan a través del empleo de sistemas electrónicos, informáticos, telemáticos o de telecomunicaciones, o en cualquiera de sus componentes, se sancionará con prisión de seis a doce años y con multa de dos mil a diez mil unidades de medida de actualización (UMA), sin perjuicio de las sanciones penales que sea procedente aplicar conforme a otras leyes, en apego al principio penal de especificidad que sobre conductas ilegales corresponde a esta Ley. Capítulo V De los delitos contra la Nación	

	Artículo 40.- Serán considerados también delitos contra la Nación, los actos que se realicen a través de un sistema informático, electrónico, telemático o de telecomunicaciones, que atenten contra los intereses fundamentales y de Seguridad de la Nación, tales como los siguientes: Capítulo VII Disposiciones comunes a los delitos en materia de las tecnologías de la Información y comunicación, que afectan redes de sistemas informáticos, electrónicos o telemáticos. Artículo 52.- Las Policías, la Guardia Nacional y el Ministerio Público, en apego a lo establecido en el Código Nacional de Procedimientos Penales, podrán solicitar sin intervención de la autoridad judicial: I. La cooperación con empresas proveedoras de servicios de Internet, y de servicios en la Red Pública de Internet nacionales e internacionales, para neutralizar sitios, páginas electrónicas y perfiles de redes sociales, siempre y cuando no se afecte la libertad de expresión, en los siguientes casos: a) Inciten al terrorismo realicen la apología del odio nacional, racial, sexual o religioso;	

	b) Que constituya incitación a la discriminación, la hostilidad o la violencia; c) La instigación directa y pública a cometer genocidio y pornografía infantil; d) Suplantación de identidad para fraude, y robo de datos personales; e) Dañe la imagen pública y la reputación de una persona o Institución; II. La preservación de la información, a los proveedores de servicios y contenidos en Internet, nacionales e internacionales. III. En los hechos relacionados con el presente Título, y de conformidad con las políticas de privacidad de los proveedores de servicios y contenidos en Internet y cualquier otra entidad que contenga en su infraestructura indicios de hechos delictivos que pongan en riesgo las libertades, derechos humanos y otras garantías, la información correspondiente por los mecanismos establecidos por dichas personas físicas o morales. En los casos de que los indicios se refieran a datos de contenido o datos personales deberá de solicitarse por control judicial y en caso de que se encuentren fuera del país también se deberá	

	recurrir a los Tratados de Asistencia Jurídica Mutua o de Carta Rogatoria, según corresponda en términos de las disposiciones de Derecho Internacional. De igual forma se podrá solicitar la colaboración de los proveedores de servicios de Internet en términos de lo dispuesto en la Ley Federal de Telecomunicaciones y Radiodifusión y sus Lineamientos de Colaboración en Materia de Seguridad y Justicia. Así mismo, dichas peticiones podrán ser realizadas por las policías, la Guardia Nacional y el Ministerio Público en casos de urgencia, de conformidad a lo establecido en el Código Nacional de Procedimientos Penales. Solicitar a una persona física o moral preservar y mantener la integridad de un sistema de información o de cualquiera de sus componentes, por un período de hasta noventa (90) días, pudiendo esta orden ser renovada por períodos sucesivos. Artículo 53.- El Ministerio Público atendiendo a la urgencia del caso particular y con la debida diligencia, puede autorizar la actuación de	

	agentes encubiertos a efectos de realizar las investigaciones de los delitos previstos en la presente Ley y de todo delito que se cometa en el ciberespacio o mediante tecnologías de la información y comunicación, de conformidad con lo establecido en los ordenamientos jurídicos aplicables.	
Senadora Alejandra Lagunes Soto Ruiz INICIATIVA CON PROYECTO DE DECRETO PARA REFORMAR Y ADICIONAR DIVERSAS DISPOSICIONES DEL CÓDIGO PENAL FEDERAL EN MATERIA DE CIBERSEGURIDAD	Artículo 168 Bis.- Se impondrán de seis meses a dos años de prisión y de trescientos a tres mil días multa, a quien sin derecho: I. Descifre o decodifique señales de telecomunicaciones distintas a las de satélite portadoras de programas, o II. Transmita la propiedad, uso o goce de aparatos, instrumentos o información que permitan descifrar o decodificar señales de telecomunicaciones distintas a las de satélite portadoras de programas. III. Produzca, transmita la propiedad, obtenga para su utilización o usufructo, importación, difusión u otra forma de puesta a disposición de: a) Dispositivos, incluidos programas informáticos diseñados o adoptados principalmente para la intervención de comunicaciones privadas, geolocalización o la interceptación de datos de navegación en internet sin consentimiento;	Abril 2019

	b) Contraseñas, códigos de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático. IV. Produzca, transmita la propiedad, obtenga para su utilización o usufructo, importación, difusión u otra forma de puesta a disposición de dispositivos, programas de computación especializados en señales, redes y aplicativos de cualquier aparato portátil o casero que atenten contra la privacidad. V. Posea alguno de los elementos contemplados en la fracción anterior, con la intención de ser utilizados para cometer ilícitos relacionados con la violación de confidencialidad, integridad, privacidad y disponibilidad de la información y sistemas informáticos. Artículo 177.- A quien intervenga comunicaciones privadas o los datos de tráfico de las telecomunicaciones realizadas por cualquier vía telefónica, medios digitales o cualquier medio de comunicación de orden público, sin mandato de autoridad judicial competente, se le aplicarán sanciones de seis a doce años de prisión y de trescientos a seiscientos días multa. La pena prevista en este artículo se duplicará para el caso de servidores públicos que en	

	ejercicio de sus funciones o aprovechando el cargo, ordene, permita, autorice o realice las conductas señaladas en este artículo, además de la privación del cargo o inhabilitación para ocupar otro hasta por cinco años. Artículo 211 Bis 7.- A quien intercepte, por cualquier medio o método, información o datos informáticos en transmisiones dirigidas a un sistema o equipo informático físico o digital, originadas desde otro sistema o equipo o realizadas dentro del mismo, incluidas las emisiones electromagnéticas y radiofrecuencias provenientes de un sistema o equipo informático que transporten dicha información o datos informáticos, se le impondrá de seis meses a cuatro años de prisión y de cien a seiscientos días multa.	
Miguel Ángel Mancera Espinosa INICIATIVA CON AVAL DEL GRUPO PARLAMENTARIO QUE CONTIENE PROYECTO DE DECRETO POR EL QUE SE MODIFICA LA	Artículo 22 Bis. El Centro Nacional de Ciberseguridad tendrá, entre otras, las siguientes atribuciones: V. Coordinarse con el Instituto Federal de Telecomunicaciones para determinar la política en la materia de Ciberseguridad.	1 de septiembre 2020

DENOMINACIÓN DEL CAPÍTULO II, DEL TÍTULO NOVENO, DEL LIBRO SEGUNDO Y SE REFORMA EL ARTÍCULO 211 BIS 1 Y SE DEROGAN DIVERSOS ARTÍCULOS DEL CÓDIGO PENAL FEDERAL; SE REFORMAN Y ADICIONAN DIVERSOS ARTÍCULOS DE LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA; SE ADICIONA UNA FRACCIÓN XIV AL ARTÍCULO 5° DE LA LEY DE SEGURIDAD NACIONAL; Y SE EXPIDE LA LEY GENERAL DE CIBERSEGURIDAD	TERCERO.- Se adiciona una fracción XIV al artículo 5° de la Ley de Seguridad Nacional para quedar como sigue: Artículo 5.- ... I a la XIII. ... XIV. Actos tendentes a amenazar, afectar, inhabilitar o destruir la infraestructura activa o pasiva de telecomunicaciones que sean indispensable para la provisión de bienes o servicios públicos o para el adecuado funcionamiento de las instituciones del Estado. Artículo 3.- La presente ley tiene por objeto: I. Establecer los tipos penales en la materia e integrar la forma y los términos en que las autoridades de las entidades federativas y los municipios colaborarán con la Federación en dicha tarea, con el fin de garantizar el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de telecomunicaciones, incluido el de banda ancha e internet en forma segura;	

	Artículo 8.- El Centro Nacional se coordinará con el Instituto Federal de Telecomunicaciones, para determinar la política en la materia de Ciberseguridad. TÍTULO V DE LAS AMENAZAS A LA CIBERSEGURIDAD Y LA SEGURIDAD DE LA INFORMACIÓN EN LA RED Artículo 25.- El Centro Nacional deberá publicar e informar al Secretario Ejecutivo del Sistema Nacional de Seguridad Pública de manera continua un reporte de amenazas a la ciberseguridad para la población en general y generar un informe anual sobre el estado que guarda la ciberseguridad, con el fin de que las personas conozcan los mayores riesgos a los que están expuestos por el uso de sistemas de telecomunicación, información y comunicación. Artículo 26.- El Centro Nacional deberá informar a las autoridades de las ciberamenazas que enfrentan en el desempeño de sus funciones, así como establecer los lineamientos de capacitación de las y los servidores públicos en la materia. Artículo 27.- Los operadores de red deberán de implementar sistemas de protección para garantizar la confidencialidad de la información de las personas usuarias.	

	Artículo 28.- Los operadores de red adoptarán las acciones necesarias para garantizar al máximo la seguridad de la información personal que recopilan y para evitar que la información personal se divulgue, destruya o se pierda. Artículo 29.- Todas las personas y empresas serán responsables del uso de sus sitios web y por ningún motivo deberán establecer sitios de internet o grupos de comunicación para realizar actividades ilícitas, difundir o perpetrar fraudes, impartir métodos criminales, elaborar o comercializar artículos prohibidos o controlados, u otras actividades ilegales. 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.	
Cristóbal Arias Solís INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMAN LOS ARTÍCULOS 6 Y 73 DE	DECRETO POR EL QUE SE REFORMAN LOS ARTÍCULOS 6 Y 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS ÚNICO. Se reforma el artículo 6, tercer párrafo, y fracciones I y II del Apartado B; y se adiciona la fracción XXIII Ter al artículo 73 de la Constitución	04 de noviembre de 2022

LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS EN MATERIA DE SEGURIDAD CIBERNÉTICA	Política de los Estados Unidos Mexicanos, para quedar como sigue: Artículo 6. ... El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá ´ condiciones de competencia efectiva en la prestación de dichos servicios. La Ley establecerá los mecanismos de cooperación y coordinación institucional para prevenir y combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos, así como garantizar la protección, seguridad y desarrollo del ecosistema digital y la prevención de riesgos o amenazas en el entorno digital o ciberespacio. A) ... B. En materia de radiodifusión y telecomunicaciones: I. El Estado garantizará a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital universal con metas anuales y sexenales, de alfabetización digital y el establecimiento de la Estrategia Nacional Digital y de Ciberseguridad	

	con perspectiva de derechos humanos y enfoque basado en prevención y gestión de riesgos, así como de eficiencia en los procesos digitales, combate a la corrupción, seguridad en la información y soberanía tecnológica. II. Las telecomunicaciones son servicios públicos de interés general, por lo que el Estado garantizará que sean prestados en condiciones de competencia, calidad, pluralidad, cobertura universal, interconexión, convergencia, continuidad, acceso libre, seguridad y sin riesgos o amenazas e injerencias arbitrarias. III. a VI. ... Artículo 73. ... I. a XXIII BIS. ... XXIII Ter. Para expedir leyes que, con respeto a los derechos humanos, establezcan los principios y las bases sobre las cuales la Federación, las entidades federativas y los Municipios en el ámbito de sus respectivas competencias coordinarán sus acciones para prevenir y combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos, de conformidad con lo establecido en el artículo 6 de esta Constitución. XXIV a XXXI. ...	

INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMA LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA EN MA TERIA DE SEGURIDAD CIBERNÉTICA	DECRETO POR EL QUE SE REFORMA LA LEY GENERAL DEL SISTEMA NACIONAL DE SEGURIDAD PÚBLICA ÚNICO. Se reforma el artículo 17 de la Ley General del Sistema Nacional de Seguridad Pública y, se adiciona el artículo 20 Bis a dicho ordenamiento, para quedar como sigue: Artículo 17. El Secretariado Ejecutivo es el órgano operativo del Sistema y gozará de autonomía técnica, de gestión y presupuestal. Contara´ con los Centros Nacionales de Información, de Prevención del Delito y Participación Ciudadana, de Seguridad Cibernética, así como de Certificación y Acreditación. El Titular del Ejecutivo Federal expedirá el Reglamento del Secretariado, que establecerá las atribuciones y articulación de estos Centros. Artículo 20 Bis. El Centro Nacional de Seguridad Cibernética tendrá, como principales atribuciones: l. Proponer al Consejo Nacional lineamientos y políticas transversales de prevención del Cibercrimen, con perspectiva de derechos humanos y enfoque basado en gestión de riesgos, a fin de preservar un entorno digital seguro y	

	resiliente, cuyas acciones tendrán el carácter de permanentes y estratégicas; 11. Promover el uso adecuado de las Tecnologías de la Información y Comunicaciones, a través de una cultura de información y concientización sobre el uso adecuado de las herramientas tecnológicas que se encuentran al alcance de la ciudadanía y los riesgos en el uso de la red de Internet; en general, promover una cultura del autocuidado, civismo y alfabetización digitales. III. Emitir opiniones y recomendaciones, dar seguimiento y evaluar los programas implementados por las Instituciones de Seguridad Pública, en los tres órdenes de gobierno para: a) Prevenir el cibercrimen y los delitos en el espacio digital. b) Promover el uso adecuado de las Tecnologías de la Información y Comunicaciones.	

FIRMADO POR: LILIA EURIDICE PALMA SALAS
FECHA FIRMA: 2023/10/17 6:26 PM
AC: AUTORIDAD CERTIFICADORA
ID: 73011
HASH:
AB44E86C0E6B647B7DA1316B6DB4915F45B76A8BA92255
CDE24C0267A4F0AD74

FIRMADO POR: REBECA ESCOBAR BRIONES
FECHA FIRMA: 2023/10/17 7:09 PM
AC: AUTORIDAD CERTIFICADORA
ID: 73011
HASH:
AB44E86C0E6B647B7DA1316B6DB4915F45B76A8BA92255
CDE24C0267A4F0AD74