INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA EL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS A EFECTO DE FACULTAR AL CONGRESO DE LA UNIÓN A EXPEDIR UNA LEY GENERAL EN MATERIA DE CIBERSEGURIDAD QUE DISTRIBUYA COMPETENCIAS ENTRE LA FEDERACIÓN Y LAS ENTIDADES FEDERATIVAS EN ESTA MATERIA.

El que suscribe, **Senador Alejandro Moreno Cárdenas**, integrante del Grupo Parlamentario del Partido Revolucionario Institucional, de la LXVI Legislatura del H. Congreso de la Unión y con fundamento en lo dispuesto en el artículo 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, así como por el artículo 8, numeral 1, fracción I del Reglamento del Senado de la República, someto a la consideración del Pleno, la siguiente Iniciativa con Proyecto de Decreto de acuerdo con la siguiente:

Exposición de Motivos

En el primer cuarto del siglo XXI, la tecnología ha transformado profundamente todos los aspectos de la vida social, económica, política y cultural, pero también ha generado retos significativos en materia de seguridad.

La ciberseguridad ha emergido como una prioridad estratégica para los gobiernos, las instituciones públicas, las empresas privadas y la sociedad en general. Los delitos y ataques cibernéticos han sido una amenaza creciente para la seguridad de los ciudadanos, gobiernos, asociaciones civiles, organizaciones sociales, instituciones de seguridad y las empresas a nivel global, según la Evaluación de la amenaza de la delincuencia organizada en Internet de Europol. Dichos fenómenos se consideran globales y sin fronteras, y la intensificación de la cooperación internacional para combatirla, ha sido una prioridad para los países de todo el mundo durante varios años.[1]

El ***Convenio del Consejo de Europa de 2001 sobre la Ciberdelincuencia,*** conocido como el *Convenio de Budapest,* fue uno de los primeros tratados internacionales sobre la ciberdelincuencia, y sobre la prevención de una serie de poderes y procedimientos para investigarlos, así como para desarrollar infraestructura y cooperación para establecer esquemas integrales y conceptuales de ciberseguridad.[2]

De hecho, el *Convenio de Budapest* fue abierto a los no miembros del Consejo de Europa y se han adherido a él, países de todas las regiones geográficas. Hasta la fecha, hay 66 Estados Parte y se ha invitado a otros catorce países a adherirse. Desafortunadamente México no se adhirió, y sin embargo, dicho convenio es la base

[1] https://www.europol.europa.eu/publications-events/main-reports/iocta-report
[2] https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

de la legislación contra la ciberdelincuencia en el 80% de los países del mundo. La adopción de un ***Segundo Protocolo Adicional al Convenio de Budapest*** por parte del Comité de Ministros del Consejo de Europa el 17 de noviembre de 2021 demostró la continua relevancia del Convenio como marco para la cooperación internacional en materia de ciberdelincuencia y del establecimiento de bases para la ciberseguridad.[3]

El auge de la tecnología de la información y el rápido desarrollo de nuevos sistemas de telecomunicaciones y redes informáticas, así como el uso y abuso de las tecnologías con fines delictivos, también han figurado en la agenda de las Naciones Unidas. El 21 de diciembre de 2010, la Asamblea General de las Naciones Unidas adoptó la Resolución 65/230 en la que se solicitaba a la Comisión de Prevención del Delito y Justicia Penal que estableciera un grupo intergubernamental de expertos de composición abierta, para que realizara un estudio exhaustivo del problema de la ciberdelincuencia [4]

De forma paralela, algunos Estados miembros de la Organización de las Naciones Unidas, fueron estableciendo esfuerzos para trabajar en conseguir de un tratado sobre ciberseguridad, en las deliberaciones de la *Tercera Comisión de la Asamblea General de las Naciones Unidas*. Por lo cual, la Asamblea General de las Naciones Unidas adoptó la *Resolución 73/187, de 17 de diciembre de 2018,* sobre "*La lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos*". [5]

Posteriormente, el 27 de diciembre de 2019, la Asamblea General de las Naciones Unidas adoptó una segunda Resolución, la 74/247, sobre el mismo tema, estableciendo un comité intergubernamental *ad hoc* de composición abierta de expertos, para elaborar una convención internacional amplia sobre la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos.[6]

Mas recientemente, el 26 de mayo de 2021, la Asamblea General de las Naciones Unidas adoptó la resolución 75/282 que, decidió, entre otras cosas, que el *Comité ad hoc* convocara al menos seis sesiones, de 10 días cada una, que comenzaron en enero de 2022, y una sesión de clausura para presentar un proyecto de convención a la Asamblea General de las Naciones Unidas en su septuagésimo octavo período de sesiones en 2024. [7]

Tras tres años de intensas negociaciones en el seno del Comité Especial de la ONU para la Elaboración de una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, los Estados miembros de la Organización de las Naciones Unidas aprobaron por consenso, el 8 de agosto de 2024, el **texto de la Convención contra**

[3] https://www.consilium.europa.eu/es/press/press-releases/2022/04/05/access-to-e-evidence-council-authorises-member-states-to-sign-international-agreement/pdf/
[4] https://documents.un.org/doc/undoc/gen/n10/526/37/pdf/n1052637.pdf
[5] file:///C:/Users/aflor/Downloads/A_RES_73_187-ES%20(3).pdf
[6] https://documents.un.org/doc/undoc/gen/n19/440/32/pdf/n1944032.pdf
[7] https://documents.un.org/doc/undoc/gen/n21/133/55/pdf/n2113355.pdf

el Ciberdelito, el primer instrumento de alcance mundial jurídicamente vinculante en materia de ciberdelincuencia. [8]

El gobierno de México celebró la adopción de esta Convención, que considera puede sentar las bases para una cooperación internacional efectiva y proveer de herramientas para el combate a la ciberdelincuencia de manera colectiva y expedita. También, considera que "*contribuirá a cerrar brechas en nuestra legislación en la materia y a establecer estándares que permitan una armonización normativa a nivel internacional*".[9]

De acuerdo con algunos expertos, la ciberseguridad es un tema crucial para la protección y gestión de la información de cualquier organización pública, social o privada, por lo que es de suma importancia reconocer las categorías que existen para determinar las acciones en cada una de ellas.

La ciberseguridad es el conjunto de leyes, políticas, procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos, incluidos los de inteligencia artificial.[10]

La ciberseguridad contempla, al menos, cuatro rubros principales[11]:

- Confidencialidad: Solo usuarios autorizados pueden acceder a recursos, datos e información.
- Integridad: Solo los usuarios autorizados deben ser capaces de modificar los datos cuando sea requerido, sin afectar a terceros, ni derechos fundamentales.
- Disponibilidad: Los datos deben estar disponibles para los usuarios cuando sea necesario.
- Autenticación: Verificar que realmente se está en comunicación con quién se están comunicando.

La ciberseguridad se aplica tanto a la protección de elementos físicos para evitar amenazas e intromisiones, a la seguridad de hardware y software, así como de redes y del ciber espacio, por lo que se encarga de encontrar las vulnerabilidades existentes en los equipos desde su fabricación, hasta los dispositivos de entrada y salida que están conectados.[12]

Actualmente son las actividades encaminadas a la protección de datos en red, es decir, la función de proteger el uso, fiabilidad, integridad y seguridad de la

[8] https://www.unodc.org/lpomex/es/noticias/agosto-2024/estados-miembro-de-las-naciones-unidas-aprueban-borrador-para-una-convencion-contra-la-ciberdelincuencia.html
[9] https://www.gob.mx/sre/prensa/el-gobierno-de-mexico-celebra-la-adopcion-de-la-convencion-contra-el-ciberdelito-en-la-onu?idiom=es
[10] https://www.ift.org.mx/sites/default/files/contenidogeneral/usuarios-y-audiencias/glosariodeciberseguridadift.pdf
[11] https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_spanish.pdf

[12] Ibidem

red para evitar que la información sea modificada o robada, se han vuelto trascendentales y desde luego, la ciberseguridad vista de manera integral, se ha convertido en tema de seguridad nacional y mundial.

En México, el aumento de los ciberataques, la vulneración de datos personales, el espionaje digital y el uso indebido de las tecnologías han puesto en evidencia la necesidad urgente de contar con un marco normativo sólido que permita proteger a las personas e instituciones frente a estos riesgos.

Sin embargo, el debate legislativo en torno a la ciberseguridad ha generado confusión debido a las diversas propuestas que se han presentado en el Congreso de la Unión.

Mientras algunas iniciativas proponen una ley de alcance federal, otras sugieren la creación de una ley general que establezca un marco de competencias compartidas entre la Federación y los estados.

Este panorama plantea interrogantes sobre el alcance jurisdiccional de las normativas y, más importante aún, sobre los límites constitucionales del Congreso de la Unión para legislar en esta materia.

El crecimiento exponencial de las tecnologías digitales y la hiperconectividad han incrementado la exposición de las personas, las empresas y las instituciones a riesgos cibernéticos.

En México, estos riesgos incluyen:

- Ciberataques a instituciones públicas y privadas: En los últimos años, varias instituciones gubernamentales, bancos y empresas han sido blanco de ataques cibernéticos que han comprometido la información sensible y paralizado servicios críticos.

- Robo de datos personales: El aumento de las brechas de seguridad ha puesto en peligro la privacidad de millones de ciudadanos, exponiéndolos a fraudes y suplantaciones de identidad.

- Desinformación y manipulación digital: Las redes sociales y otras plataformas tecnológicas han sido utilizadas para difundir información falsa, influir en procesos electorales y desestabilizar a las instituciones democráticas.

- Cibercrimen organizado: Los grupos delictivos han adoptado tecnologías avanzadas para perpetrar actividades ilícitas, desde el tráfico de drogas hasta el lavado de dinero, utilizando plataformas digitales.

Ante esta realidad, es evidente que México necesita una estrategia integral de ciberseguridad respaldada por un marco normativo robusto que aborde tanto la

prevención como la respuesta a los riesgos cibernéticos. No obstante, la elaboración de dicho marco enfrenta retos conceptuales y jurídicos derivados de la distribución de competencias en nuestro sistema federal.

En el Congreso de la Unión se han presentado diversas iniciativas que buscan regular la ciberseguridad. Sin embargo, estas propuestas reflejan enfoques divergentes respecto al alcance jurisdiccional de la normativa:

A) Ley Federal: Algunas iniciativas proponen que la ciberseguridad sea regulada exclusivamente por la Federación a través de una ley federal. Este enfoque implicaría que las disposiciones normativas aplicaran únicamente a las autoridades e instituciones federales, dejando fuera a los estados y municipios.

B) Ley General: Otras iniciativas sugieren la creación de una ley general que distribuya competencias entre los tres niveles de gobierno (Federación, estados y municipios). Este enfoque permitiría establecer un marco normativo uniforme en todo el país, asegurando que los gobiernos locales también participen en la implementación de políticas de ciberseguridad.

Ambos enfoques tienen implicaciones importantes pues mientras que una ley federal podría ser más sencilla de implementar desde el punto de vista legislativo, carecería de la capacidad de coordinar esfuerzos entre los diferentes niveles de gobierno. Por otro lado, una ley general permitiría un enfoque más integral, pero su viabilidad constitucional es cuestionable con el texto actual de nuestra Carta Magna.

La distribución de competencias legislativas entre la Federación y los estados en México ha sido un tema fundamental en el diseño del sistema federal establecido por la Constitución de 1917.

Este marco normativo organiza la división de poderes y competencias entre los órdenes de gobierno, asegurando que cada uno ejerza sus facultades dentro de un esquema de autonomía, pero también de coordinación. Los artículos 73 y 124 de la Constitución Política de los Estados Unidos Mexicanos son pilares fundamentales en esta arquitectura.

El artículo 73 establece las atribuciones legislativas del Congreso de la Unión, delimitando las materias sobre las cuales puede expedir leyes de aplicación general.

Entre sus fracciones, se detallan competencias específicas como comercio exterior, crédito, deuda pública, educación, salud y otras que tienen un impacto nacional o internacional. Esta centralización de competencias se justifica bajo el principio de unidad nacional, que busca garantizar uniformidad en materias clave para el desarrollo del país.

Es importante destacar que la inclusión de una materia en el artículo 73 no implica únicamente la atribución para legislar, sino que también delimita el alcance de las

acciones estatales en dichas áreas. En este sentido, cuando el Congreso ejerce sus facultades exclusivas, las entidades federativas quedan impedidas de intervenir en esas materias, a menos que la legislación federal disponga lo contrario.

Este principio asegura que el poder legislativo federal no invada el ámbito de competencia local, respetando la soberanía de las entidades federativas.

El artículo 124 **de la Constitución de la República** consagra el principio de facultades residuales. Según este precepto, las facultades que no estén expresamente concedidas por esta Constitución a los funcionarios federales, se entienden reservadas a los estados.

Este principio determina que todas las atribuciones que no estén expresamente conferidas a la Federación se entienden reservadas a los estados. En términos prácticos, este esquema dota a las entidades federativas de un margen amplio de acción en todas aquellas áreas que no han sido objeto de regulación federal.

Dichas facultades residuales son un reflejo del pacto federal, en el cual los estados, como entidades soberanas, conservan competencias propias mientras no las hayan cedido expresamente a la Federación.

Este principio, sin embargo, puede entrar en tensión cuando se requiere armonizar intereses federales y estatales, especialmente en áreas donde las competencias no están claramente delimitadas.

La ley general es un mecanismo diseñado para resolver las posibles tensiones derivadas de la concurrencia de competencias entre la Federación y los estados. Sustentada en el artículo 73 constitucional, una ley general permite al Congreso de la Unión establecer un marco normativo que distribuye de manera precisa las competencias entre diversos niveles de gobierno.

En este contexto, las leyes generales desempeñan un papel esencial en nuestro diseño constitucional. De acuerdo con el artículo 73, el Congreso de la Unión tiene la facultad de emitir leyes generales que establezcan bases de coordinación entre los ámbitos federal y estatal. Estas leyes distribuyen competencias entre ambos niveles de gobierno, asegurando que cada uno actúe dentro de su ámbito y que las regulaciones sean consistentes a nivel nacional.

En tal sentido, se considera de acuerdo con la interpretación de la Tesis: P. IX/2007 de la Suprema Corte de la Justicia de la Nación, que, las leyes generales son aquellas que pueden incidir válidamente en todos los órdenes jurídicos parciales que integran al Estado Mexicano. Es decir, que las leyes generales corresponden a aquellas respecto a las cuales el Constituyente o el Poder Revisor de la Constitución, ha renunciado expresamente a su potestad distribuidora de atribuciones entre las entidades políticas que integran el

Estado Mexicano. Por lo que el origen de estas normas (que están en cláusulas constitucionales), obligan al Congreso de la Unión, a dictarlas y éstas deben ser aplicadas por todas las autoridades, tanto federales, locales, como municipales, lo que representa un principio de supremacía, así como una extensión de derechos, facultando al Estado con parámetros mínimos para su cumplimiento. [13]

Un ejemplo paradigmático de una ley general es la Ley General de Educación. Este instrumento establece principios, objetivos y criterios comunes para todo el país, pero también reconoce la facultad de los estados para regular aspectos específicos de acuerdo con sus necesidades locales, siempre que se ajusten a los lineamientos nacionales.

La inclusión en el artículo 73 de la facultad del Congreso para expedir leyes generales conlleva implicaciones importantes para el pacto federal. En esencia, esta facultad significa que los estados ceden una parte de su soberanía regulatoria en favor de un esquema de coordinación nacional.

Esto es particularmente relevante cuando se trata de reformas constitucionales, ya que la aprobación de los estados es necesaria para legitimar la transferencia de competencias a la Federación.

Esto se debe a que, en su naturaleza, estas leyes implican una redistribución de competencias que originalmente recaerían en los estados. En otras palabras, una ley general redefine el esquema de facultades residuales al asignar al Congreso federal la facultad de regular materias y distribuir competencias que, de otra forma, los estados habrían podido ejercer.

En este contexto, el papel de los estados no desaparece, sino que se transforma.

Al aprobar una reforma constitucional que faculta al Congreso para expedir una ley general, los estados no solo reconocen la necesidad de una regulación nacional en determinadas materias, sino que también asumen un compromiso de colaboración para implementar las disposiciones de dicha ley en sus respectivos territorios.

Por ejemplo, cuando el artículo 73 se reforma para incluir la facultad del Congreso de expedir una ley general en materia de derechos humanos, esto significa que los estados pierden parte de su facultad para legislar en ese ámbito. Esta pérdida se ve compensada por la posibilidad de contar con un marco normativo uniforme y coherente que garantice derechos fundamentales a nivel nacional.

---

[13] Espinoza Valdez, Odracir Ricardo. LEYES GENERALES EN MÉXICO, en BIOLEX Revista Jurídica del Departamento de Derecho UNISON URC Academia de Derecho Administrativo Tercera Época Año 9. No 17 Julio –Diciembre de 2017.

Este proceso también tiene un componente político relevante: al tratarse de una reforma constitucional, se requiere la aprobación de al menos dos terceras partes de las legislaturas estatales.

Este requisito asegura que los estados participen en la decisión de ceder competencias al ámbito federal.

El desafío principal en el diseño y aplicación de leyes generales es lograr un equilibrio entre la necesidad de uniformidad nacional y el respeto a la autonomía estatal. Este equilibrio se puede alcanzar mediante una participación activa de los estados en el proceso legislativo a través de consultas y negociaciones, se puede garantizar que las leyes generales reflejen las necesidades y prioridades de las entidades federativas y un diseño claro de competencias ya que las leyes generales deben definir con precisión las responsabilidades de cada orden de gobierno, minimizando ambigüedades y conflictos de competencia, a través de mecanismos de coordinación intergubernamental eficientes.

El sistema federal mexicano, sustentado en los artículos 73 y 124 de la Constitución, refleja un equilibrio dinámico entre centralización y autonomía. Las facultades residuales aseguran que los estados mantengan un grado significativo de soberanía, mientras que las leyes generales permiten una coordinación efectiva en materias de interés común.

La facultad del Congreso de la Unión para expedir leyes generales es un ejemplo claro de cómo el federalismo puede evolucionar para enfrentar los retos de un país complejo y diverso como México.

Este mecanismo permite conciliar las necesidades de uniformidad y autonomía, garantizando que el sistema federal siga siendo una herramienta eficaz para el desarrollo y bienestar del país.

Justificación de la propuesta

El principal obstáculo para la emisión de una ley general en materia de ciberseguridad radica en las disposiciones de la Constitución mexicana.

Si bien el artículo 73 otorga al Congreso de la Unión facultades para legislar en materias como comunicaciones, tecnologías de la información y seguridad nacional, no contempla explícitamente la posibilidad de emitir una ley general en ciberseguridad que distribuya competencias entre los niveles de gobierno.

Actualmente el marco normativo en materia de ciberseguridad en el orden federal descansa esencialmente en lo que dispone el artículo 73 constitucional, el cual establece que el Congreso de la Unión está facultado para expedir leyes en materia de tecnologías de la información, banda ancha e internet y seguridad nacional, entre las cuales quedaría inserta una legislación en materia de ciberseguridad.

Dicho artículo señala en dos fracciones, facultades expresas del Congreso para legislar en materia de sistemas informáticos:

> *XVII. Para dictar leyes sobre vías generales de comunicación, tecnologías de la información y la comunicación, radiodifusión, telecomunicaciones, incluida la banda ancha e Internet, postas y correos, y sobre el uso y aprovechamiento de las aguas de jurisdicción federal.*
>
> *XXIX-M. Para expedir leyes en materia de seguridad nacional, estableciendo los requisitos y límites a las investigaciones correspondientes.*

En el caso de la fracción XVII es claro que el Congreso puede abordar todo aquello que quede incluido en las definiciones de tecnologías de información, banda ancha e internet, lo cual es consustancial a los medios considerados como cibernéticos y su seguridad.

Para el caso de la fracción XXIX-M, se remite a la Ley de Seguridad Nacional, que en su artículo 3 define a esta como:

> *"... las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado Mexicano, que conlleven a:*
>
> *I. La protección de la nación mexicana frente a las amenazas y riesgos que enfrente nuestro país"*

Adicionalmente, el artículo 5 de la misma Ley establece que:

> *Artículo 5.- Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:*
>
> *I. Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;*
>
> *XI. Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia;*
>
> *XII. Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos,*

De ello resulta que la ciberseguridad puede encuadrarse fácilmente en los supuestos específicos previstos por la Ley de Seguridad Nacional, para ser considerada una amenaza o riesgo a la misma, pues ni la constitución ni la ley especifican todas aquellas conductas que pudieran afectar la seguridad nacional de

forma que pueda determinarse si el legislador está específicamente facultado para abordar todas y cada una de ellas.

Vayan como ejemplos el *sabotaje* o el *terrorismo*, conductas sobre las que la Constitución no faculta al Congreso para legislar de forma expresa, pero que se han abordado en diversas leyes, como la antes referida de Seguridad Nacional o el Código Penal Federal, debido a que forman parte de un sistema de conductas delictivas contrario a los derechos y libertades tutelados por la constitución.

Mas allá de lo anterior y ante el ejemplo de los hackeos de que ha sido objeto el Estado mexicano en instituciones estratégicas tales como la Secretaria de la Defensa Nacional, la Comisión Nacional del Agua, PEMEX, la Secretaría de Economía, y otros casos conocidos, la ciberseguridad encuadra perfectamente no solo en la definición del artículo 3 de la Ley de Seguridad Nacional, sino en las tres fracciones citadas del artículo 5 de dicha norma.

En este contexto, el Congreso de la Unión ya ha expedido en el pasado reciente diversas normas relativas a la tipificación de delitos y seguridad informáticos.

Es el caso de la adición en 1999, en el Código Penal Federal del *Título Noveno,* denominado *Revelación de secretos y acceso ilícito a sistemas y equipos de informática*, el cual se subdivide en un *Capítulo I* cuyo título es *Revelación de secretos* y un *Capítulo II*, denominado *Acceso ilícito a sistemas y equipos de informática*, el cual tipifica los delitos relativos a la transgresión de sistemas de seguridad informática.

A modo de ejemplo baste señalar que en este Capítulo II se establece lo siguiente, respecto a conductas delictivas relativas a la seguridad de sistemas informáticos, es decir, a ciberseguridad:

> *Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.*
>
> *Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.*
>
> *Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa*

Es el caso igualmente, de la reforma publicada en el DOF el 9 de marzo de 2018, conocida como Ley FINTECH, es decir, el *Decreto por el que se expide la Ley para Regular las Instituciones de Tecnología Financiera y se reforman y adicionan diversas disposiciones de la Ley de Instituciones de Crédito, de la Ley del Mercado de Valores, de la Ley General de Organizaciones y Actividades Auxiliares del Crédito, de la Ley para la Transparencia y Ordenamiento de los Servicios Financieros, de la Ley para Regular las Sociedades de Información Crediticia, de la Ley de Protección y Defensa al Usuario de Servicios Financieros, de la Ley para Regular las Agrupaciones Financieras, de la Ley de la Comisión Nacional Bancaria y de Valores y, de la Ley Federal para la Prevención e Identificación de Operaciones con Recursos de Procedencia Ilícita.*

En dicha reforma, la Ley para Regular las Instituciones de Tecnología Financiera establece distintas previsiones relativas a la preservación de la seguridad informática y sanciones relativas a su transgresión.

A modo de ejemplo baste señalar que su artículo 39 establece que:

> *Artículo 39.- Las solicitudes para obtener las autorizaciones de la CNBV previstas en el presente Capítulo deberán acompañarse de lo siguiente:*
>
> *VI. Las medidas y políticas en materia de control de riesgos operativos, así como de seguridad de la información, incluyendo las políticas de confidencialidad, con la evidencia de que cuentan con un soporte tecnológico seguro, confiable y preciso para sus Clientes y con los estándares mínimos de seguridad que aseguren la confidencialidad, disponibilidad e integridad de la información y prevención de fraudes y ataques cibernéticos, de conformidad con lo establecido en las disposiciones de carácter general aplicables;*

Igualmente, dicha norma incluye capítulos relativos a Operaciones con Activos Virtuales y Modelos Novedosos, cuya operación depende de autorizaciones que otorgue la Comisión Nacional Bancaria y de Valores una vez que se han acreditado diversos requisitos en materia de seguridad informática de la información financiera, es decir, ciberseguridad.

A modo de ejemplo, de varios que hay a lo largo de dicha norma, existen varias secciones relativas al control de los llamados mecanismos novedosos.

En la *Sección Cuarta* denominada *Delitos para la Protección del Patrimonio de las ITF y de las Sociedades Autorizadas para operar con Modelos Novedosos*, los cuales se refieren a la violación se sistemas informáticos, de la forma siguiente:

> *Artículo 130.- Se sancionará con prisión de tres a nueve años y multa de 5,000 a 150,000 UMA, a quien valiéndose de cualquier medio físico, documental, electrónico, óptico, magnético, sonoro, audiovisual, informático o de cualquier*

otra clase de tecnología, suplante la identidad, representación o personalidad de cualquiera de las Autoridades Financieras o de alguna de sus unidades administrativas o áreas o de un servidor público, de las ITF o sociedades autorizadas para operar con Modelos Novedosos o de alguno de sus directivos, consejeros, empleados, funcionarios, dependientes o representantes legales.

Artículo 133.- Al que sin autorización obtenga, extraiga o desvíe recursos, fondos de pago electrónicos o activos virtuales por medio de los sistemas o equipos de informática de las ITF o de las sociedades o Entidades Financieras u otros sujetos supervisados por alguna Comisión Supervisora o por el Banco de México, autorizados para operar con Modelos Novedosos, se le impondrán las siguientes sanciones (...)

De todo ello resulta que el Congreso de la Unión ya ha abordado el tema de la ciberseguridad de diversas formas en distintas normas con base en su facultad constitucional originaria para poder legislar en la materia en el orden federal.

Lo que no puede hacer el Congreso de la Unión ya que no está facultado para ello expresamente, es expedir una Ley General en la materia, ya que estas distribuyen competencias e implican que el Poder Legislativo Federal interviene en la soberanía estatal para regular ciertos aspectos que de otra forma se entienden reservados para su jurisdicción, conforme lo establece el artículo 127 constitucional.

En este sentido es indispensable que el artículo 73 constitucional incluya alguna referencia expresa para que el Congreso pueda emitir una Ley general, idéntica a la que ya incluye en los siguientes casos que nos sirven de ejemplo:

XXIX-T. Para expedir la ley general que establezca la organización y administración homogénea de los archivos de la Federación, de las entidades federativas, de los Municipios y de las demarcaciones territoriales de la Ciudad de México, y determine las bases de organización y funcionamiento del Sistema Nacional de Archivos.

XXIX-U. Para expedir las leyes generales que distribuyan competencias entre la Federación y las entidades federativas en materias de partidos políticos; organismos electorales, y procesos electorales, conforme a las bases previstas en esta Constitución.

XXIX-V. Para expedir la ley general que distribuya competencias entre los órdenes de gobierno para establecer las responsabilidades administrativas de los servidores públicos, sus obligaciones, las sanciones aplicables por los actos u omisiones en que éstos incurran y las que correspondan a los particulares vinculados con faltas administrativas graves que al efecto prevea, así como los procedimientos para su aplicación.

En el caso de la ciberseguridad, la Constitución no contiene una disposición similar.

Esto significa que, aunque el Congreso puede legislar en esta materia a nivel federal, carece de la facultad para emitir una ley general que coordine esfuerzos con los estados y municipios.

Este vacío normativo plantea un desafío significativo para la regulación de la ciberseguridad, ya que la naturaleza transversal y global de los riesgos cibernéticos exige una coordinación estrecha entre todos los niveles de gobierno.

Para superar las limitaciones actuales, sería necesario promover una reforma constitucional que otorgue al Congreso de la Unión la facultad de expedir una ley general en materia de ciberseguridad. Dicha reforma podría incluir los siguientes elementos:

1. Incorporación de la ciberseguridad como materia de interés nacional: Establecer que la ciberseguridad es una materia de competencia concurrente, similar a la educación o la salud, justificando su relevancia en el contexto actual.

2. Distribución de competencias: Definir con claridad las responsabilidades de la Federación, los estados y los municipios en la protección de los sistemas cibernéticos y la respuesta a incidentes de seguridad.

3. Mecanismos de coordinación: Crear instancias de colaboración intergubernamental para el diseño e implementación de políticas públicas en ciberseguridad.

4. Principios rectores: Incluir principios como la protección de los derechos humanos, la proporcionalidad en las medidas de vigilancia y la promoción de la innovación tecnológica.

Esta reforma permitiría al Congreso de la Unión emitir una ley general que responda de manera integral a los desafíos de la ciberseguridad, garantizando la participación de todos los niveles de gobierno y fortaleciendo la capacidad de respuesta frente a los riesgos cibernéticos.

Honorable Asamblea

La ciberseguridad representa uno de los mayores retos para México en el siglo XXI, ya que los riesgos asociados al uso de las tecnologías digitales afectan tanto a las personas como a las instituciones públicas y privadas. Aunque el Congreso de la Unión ha reconocido la importancia de legislar en esta materia, las iniciativas presentadas hasta ahora reflejan una falta de claridad respecto al alcance jurisdiccional de las normativas propuestas.

La confusión entre la posibilidad de emitir una ley federal o una ley general pone de manifiesto las limitaciones del marco constitucional vigente. Mientras que una ley federal podría ser insuficiente para abordar los riesgos cibernéticos de manera integral, una ley general no puede ser emitida sin una reforma constitucional que otorgue al Congreso de la Unión las facultades necesarias para distribuir competencias en esta materia.

En este contexto, es fundamental que los legisladores impulsemos un debate serio y profundo sobre la necesidad de reformar la Constitución para facultar al Congreso de la Unión a expedir una ley general en ciberseguridad.

Solo así será posible construir un marco normativo que permita a México enfrentar los desafíos del entorno digital con eficacia, coordinación y respeto a los derechos fundamentales.

En el Partido Revolucionario Institucional luchamos por la promoción de las buenas prácticas en la arena digital, entendiendo la tecnología como una herramienta útil de comunicación; para que las actuales y las nuevas generaciones tengan acceso a la tecnología de una manera ética, responsable, útil y segura.[14]

Nos pronunciamos además, por la protección de la información personal para garantizar la privacidad y seguridad de los datos; el desarrollo y uso de la inteligencia artificial de manera ética y responsable, con un enfoque regulatorio que, asegure la transparencia, la protección de datos y la responsabilidad social en su uso. El PRI condena las malas prácticas como el acoso cibernético, la violencia digital y el fraude electrónico. Nos pronunciamos en contra del uso de la inteligencia artificial con fines de desprestigio y de usurpación de identidad.[15]

Por todo lo expuesto y fundamentado, someto a consideración de esta asamblea la siguiente iniciativa con proyecto de:

PROYECTO DE DECRETO POR EL QUE SE ADICIONA EL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS A EFECTO DE FACULTAR AL CONGRESO DE LA UNIÓN A EXPEDIR UNA LEY GENERAL EN MATERIA DE CIBESERSEGURIDAD QUE DISTRIBUYA COMPETENCIAS ENTRE LA FEDERACIÓN Y LAS ENTIDADES FEDERATIVAS EN ESTA MATERIA.

[14] Partido Revolucionario Institucional. Declaración de Principios, pagina 19 disponible en https://pri.org.mx/ElPartidoDeMexico/Documentos/2024/DeclaraciondePrincipios.pdf

[15] Partido Revolucionario Institucional. Declaración de Principios, pagina 20 disponible en https://pri.org.mx/ElPartidoDeMexico/Documentos/2024/DeclaraciondePrincipios.pdf

ARTÍCULO ÚNICO. Se adiciona una fracción XXXIII al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos para quedar como sigue:

Artículo 73. El Congreso tiene facultad:

I a XXXII.- ...

XXXIII.- Para expedir la ley general que distribuya competencias entre los órdenes de gobierno en materia de ciberseguridad.

TRANSITORIO

ÚNICO. El presente decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Senado de la República, a 12 de enero de 2025

Sen. Alejandro Moreno Cárdenas