



LEGISLATIVO

Inician los diálogos para delinear la normatividad en el Congreso

# LEY FEDERAL DE CIBERSEGURIDAD: ¿DEFENDER O VIGILAR LA LIBERTAD?

R. Esaú Sánchez  
resau.sanchez@gmail.com

En abril de 2023 se presentó la primera iniciativa para regular las interacciones digitales, pero la propuesta llama la atención de usuarios por las acciones y delitos que incluye.

**E**n las comisiones de Seguridad Ciudadana, y de Ciencia, Tecnología e Innovación de la Cámara de Diputados se aprobó la metodología para dictaminar la iniciativa para expedir la Ley Federal de Ciberseguridad. El suceso comienza a llamar la atención de especialistas e internautas debido a las implicaciones sociales que tiene la propuesta, pues se aproxima al problema como un tema de seguridad nacional.

De hecho, los diputados acordaron reunirse con las secretarías de Defensa Nacional (Sedena), de Marina (Semar) y de Hacienda y Crédito Público (SHCP) para analizar y mejorar la iniciativa de ley.

La intervención y opinión de los usuarios de internet y de los empresarios, quienes suelen ser los más vulnerados, quedaron relegadas a un segundo plano.

El “descongelamiento” de la iniciativa, que llevaba en las bóvedas legislativas desde abril de 2023, coincide con los señalamientos por parte del Poder Ejecutivo a presuntas campañas de desprestigio en redes sociales.

Según el gobierno federal se promueven falsas noticias como “un mecanismo de manipulación; no son personas de carne, hueso y un pedazo de pescado. ¿Cómo opera eso y cuánto cuesta? Estamos hablando de millones de pesos por una campaña así; y esa es una amenaza hacia adelante”.





Descongelan iniciativa.

Entre otras cosas, la Ley Federal de Ciberseguridad faculta a la Sedena y a la Semar para monitorear y ejecutar “operaciones militares” en internet, aunque no se especifica qué tipo de actividades cuentan como militares, ni define si tendrán que ser autorizadas por jueces o autoridades, ni desarrolla un procedimiento para la protección de datos personales.

Además, el artículo 78 de la ley estipula que se castigaría a quienes diseñen o describan contenido que incite al odio, a la burla o a la desinformación. Al no haber un parámetro claro de lo que estos conceptos significan, es posible que los videos o imágenes con un sentido humorístico, como los memes, se tipifiquen como delitos.

## Sanciones

Para el diputado Javier López Casarín, del PVEM y quien presentó la iniciativa de ley, la ciberdelincuencia representa una industria multimillonaria a nivel mundial, por lo que el Estado requiere de herramientas para poder actuar y defender los intereses y derechos de instituciones y particulares.

Entre otras cosas, la iniciativa también propone la creación de una Agencia Nacional de Ciberseguridad que dependa enteramente del Poder Ejecutivo y se encargue de generar estrategias y políticas públicas, al mismo tiempo que concentra la información sobre incidentes, ataques y delitos, de modo que haya indicadores para saber si dicha seguridad aumenta o empeora día con día.

Cabe señalar que la ley definiría a los delitos cibernéticos o ciberdelitos como las acciones u omisiones delictivas que, haciendo uso de las Tecnologías de la Información y Comunicación (TIC), se encuentran tipificadas en algún código penal.

De hecho, el documento establece que el Poder Judicial de la Federación cuente con jueces especializados en esta materia y detalla algunos de los actos que considera como delitos.

Entre ellos están el acceso o robo de información que provoque la pérdida de confidencialidad e integridad en sistemas o medios informáticos, mismo que se castigará con entre cinco y 20 años de prisión; las interceptaciones sin órdenes judiciales de

cualquier tipo de comunicación electrónica, que serán castigadas con entre diez y 20 años de prisión; la producción y comercialización de programas y equipos informáticos para uso ilícito; la apropiación de bienes o derechos patrimoniales que se realice a través de fraudes o engaños en medios informáticos; las extorsiones digitales o telefónicas; y la promoción e incitación a menores para participar en actividades lascivas o sexuales.

Volviendo a las actividades que incitan al odio, a la burla o a la desinformación, la ley sí aclara que “no serán motivo de sanción aquellas expresiones que se realicen en apego a la libertad de expresión”.

## Fechas clave

- **19-20 de febrero** Reunión con miembros de la Sedena, Semar, SHCP, Guardia Nacional y Centro Nacional de Inteligencia para dialogar sobre la Ley Federal de Ciberseguridad.
- **20-21 de febrero** Circulación del dictamen.
- **28 de febrero** Discusión y votación del dictamen en comisiones unidas de Seguridad Ciudadana y de Ciencia, Tecnología e Innovación.

Aunque el problema persiste, pues no especifica cuáles son los parámetros bajo los cuales se puede establecer que un contenido digital incita o no al odio nacional, racial, sexual o religioso, ni cuándo constituye o no un acto de desinformación o manipulación individual o colectiva.

Quienes incurran en este delito podrían ser castigados con hasta seis años de prisión y una multa de hasta mil Unidades de Medida y Actualización (UMA).

Otro artículo que resulta poco claro es el 83, con el que se castigan “las conductas descritas en la Ley Federal de Derechos de Autor y en la Ley de Propiedad Industrial”, siempre y cuando se realicen a través de sistemas electrónicos.



### Freno opositor

En la Cámara de Diputados las bancadas de los partidos de oposición lograron frenar temporalmente la iniciativa de Morena con la que a partir de cuatro votos de los once ministros de la Suprema Corte de Justicia de la Nación (SCJN) se declaraba constitucionalidad en alguna reforma impugnada. Ignacio Mier, coordinador de Morena en San Lázaro, aclaró que la llamada “ley antiamparo” se incluirá a debate junto con la iniciativa para reducir la jornada laboral de 48 a 40 horas, por lo que tendrá que esperar a que se realicen los foros nacionales del 19 de febrero al 15 de abril y extender así su análisis.

El apartado no especifica qué conductas se considerarán como infracciones, por lo que *stricto sensu* el registro de una marca o la publicación de una obra registrada en medios digitales podrían ser delitos castigados con hasta doce años de prisión y diez mil UMA.

### Afectados

Al considerar los cibercrimes como un problema de seguridad nacional, la iniciativa de ley tiene un enfoque de vigilancia y militar.

Por ello, diputados de oposición como el panista Román Cifuentes Negrete ven necesaria la participación del sector privado, pues “muchos de los ataques cibernéticos vulneran espacios de comunicación de este sector”.

En estricto sentido, los usuarios “de a pie” son los más afectados y quienes más sufren amenazas de ciberataques, ya sea por el robo de datos o por las amenazas de perder parte de su patrimonio.

De hecho, según el estudio *Ciberseguridad en México 2023*, realizado por la Asociación de Internet MX (AIMX), 73% de los encuestados considera como principal motivo de preocupación los ataques relacionados a los bancos y el sector financiero.

Asimismo, 66% “teme por la suplantación de identidad, que además de ser de índole financiera, también puede afectar la esfera de lo privado”.

Para Pablo Corona, presidente de AIMX, “es fundamental conocer los hábitos de los usuarios mexicanos de internet para poder mejorar su experiencia y establecer los mecanismos de protección para las empresas”.

En la misma investigación se resalta que aun cuando 58% de los internautas no se ha expuesto ni ha sido víctima de algún fraude, virus o robo de datos, al menos 33% sí ha recibido noticias falsas, posicionándose de hecho como el principal incidente en internet.

A principios de este año el World Economic Forum (WEF) presentó su lista de riesgos globales para 2024. En primer lugar, obviamente, está la crisis climática; pero en segundo y en tercer lugar se encuentran la desinformación y la polarización política, respectivamente.

Y considerando el gran número de países que tienen elecciones este año, el foro considera que para 2026 la desinformación será el riesgo más grande a nivel mundial.

“Dado que no se requiere un particular conjunto de habilidades, las interfaces fáciles de usar y los modelos de Inteligencia Artificial (IA) a gran escala han desembocado en una explosión de información falsificada y en contenido ‘sintético’, desde sofisticada clonación de voz, hasta websites falsos”, alerta el documento.

El WEF advierte que estas nuevas tecnologías, que avanzan cada vez más rápido, pronto provocarán la creación de nuevos delitos, como manipulación en bolsas de valores y hasta creación de contenido para adultos falso y no consensuado.

Finalmente, el organismo internacional adelanta que, en términos electorales, la desinformación podría “desestabilizar severamente la realidad y la percepción de legitimidad de un nuevo gobierno electo”. Y, como se mencionaba previamente, son los ciudadanos y bancos los que más vulnerables están ante la delincuencia cibernética.

Se espera que la iniciativa para expedir la Ley Federal de Ciberseguridad sea debatida y votada en comisiones el próximo 28 de febrero. **M**



Seguridad para los usuarios.