



Especialistas y organismos que defienden los derechos digitales consideran que la iniciativa de la Ley Federal de Ciberseguridad, presentada el mes pasado por el diputado Javier López Casarín, es ambigua, da muchas facultades a los órganos militares y podría vulnerar los derechos de las personas, por lo que es necesario modificar esos puntos o, de ser posible, desecharla.

Los organismos Red en Defensa de los Derechos Digitales (R3D), Article19 México y Centroamérica, SocialTIC, Cultivando Género AC y Luchadoras MX emitieron un comunicado sobre los problemas que presenta la nueva propuesta y que demuestran que existe un "profundo desconocimiento" de las nociones básicas de derechos humanos en el entorno digital, así como del funcionamiento de las tecnologías y la economía digital.

SOBRE LA NUEVA INICIATIVA

- Fue presentada a la Cámara de Diputados por Javier López Casarín, miembro del Partido Verde Ecologista de México y presidente de la Comisión de Ciencia, Tecnología e Innovación de la Cámara baja
- Desde octubre del año pasado se estaban revisando las 19 iniciativas de ley de ciberseguridad presentadas en el Congreso durante los últimos años
- Consta de 92 artículos divididos en ocho títulos y con ocho artículos transitorios
- Propone la creación de una Agencia Nacional de Ciberseguridad que tendrá varias atribuciones, así como la creación de un Registro Nacional de Incidentes de Ciberseguridad

19
INICIATIVAS
de posibles leyes de ciberseguridad se han presentado al Congreso

VEN GRANDES RIESGOS

NO CONVENCE INICIATIVA DE LEY FEDERAL DE CIBERSEGURIDAD

ANALISTAS Y EXPERTOS dudan de operaciones militares en el ciberespacio por parte de la Sedena y la Marina

POR AURA HERNÁNDEZ
aura.hernandez@gimm.com.mx

Entre las principales preocupaciones destaca que esta iniciativa de Ley Federal de Ciberseguridad, que posiblemente se analizará en el próximo periodo de sesiones de la Cámara de Diputados, faculta a la Secretaría de la Defensa Nacional y a la Secretaría de Marina a monitorear y llevar a cabo operaciones militares en el ciberespacio, sin definir con precisión el tipo de actividades que podrían llevar a cabo las fuerzas armadas, bajo qué procedimientos y con qué salvaguardas.

Para Luis Fernando García, director de R3D en México, dichas operaciones en el ciberespacio están "tan vagamente" definidas que podrían



PERIÓDICO	PAGINA	FECHA	SECCIÓN
EXCELSIOR	7D	03/05/2023	LEGISLATIVO

entrar desde espionaje a civiles hasta ataques informáticos a otro país.

El organismo a su cargo teme que esto signifique que las fuerzas armadas profundicen las tareas de vigilancia, espionaje e intervención de comunicaciones privadas de la población.

No hay que olvidar que recientemente se reveló que los militares de esta administración siguen utilizando el software Pegasus contra defensores de derechos humanos y periodistas.

“Hay muchas más cosas peligrosas, absurdas y hasta ridículas en la iniciativa de #LeyDeCiberseguridad”, aseguró García en su cuenta de Twitter.

92 ARTÍCULOS
tiene la actual propuesta de ley que se discutirá

2 INSTANCIAS
tendrían facultades de monitoreo de seguridad: Sedena y la Marina

Esto porque la iniciativa podría facultar a una nueva Agencia Nacional de Ciberseguridad, a la Guardia Nacional, a la Fiscalía General de la República y a autoridades judiciales a dar de baja direcciones IP, dominios y sitios de internet de manera discrecional.

Red en Defensa de los Derechos Digitales (R3D), Article19 México y Centroamérica, SocialTIC, Cultivando Género AC y Luchadoras MX consideran dicha medida como inconstitucional porque constituye una censura que está prohibida tanto por la Constitución como por tratados internacionales

en materia de derechos humanos.

En este sentido, también se teme que haya invasiones a la privacidad de las personas porque da facultades a la nueva agencia para fortalecer actividades de inteligencia. También impone obligaciones a los particulares para que entreguen cualquier información que le sea requerida por las autoridades, por ejemplo, pedirá datos sobre incidentes cibernéticos.

Pablo Corona, director global de ventas en NYCE, comentó en un blog personal que pedir a los particulares la información sobre sus incidentes, sin que estos afecten infraestructuras críticas, es excesivo y difícil de implementar.

Otro punto es que la iniciativa utiliza términos amplios, vagos e imprecisos.