OPINIÓN

# Análisis a la iniciativa de Ley Federal de Ciberseguridad

**Por Ernesto Ángeles** · 4 de mayo de 2023 · 10 min de lectura




Al día de hoy es más que común escuchar, casi a diario, información sobre nuevos productos, beneficios o soluciones que el sistema digital y sus tecnologías brindan y brindarán a la humanidad en el futuro; sin embargo, a la hora de analizar los riesgos, amenazas y peligros que genera este sistema tecnológico, la situación cambia drásticamente, al punto que se tilda de "represor" a cualquier instancia que intente aportar un poco de orden a este sistema y sus prácticas inseguras, depredadoras, colonialistas y abusivas.

Tal aversión a la regulación no sólo se deviene de la publicidad y la romantización de la tecnología, sino que en el ordenamiento del sistema tecnológico confluyen una serie de intereses y poderes de carácter económico, financiero, político, social y militar (nacionales y extranjeros) que intentan dar forma a la manera en la cual los elementos del sistema digital interactúan y operan en territorio nacional, así como la relación del país con el sistema tecnológico internacional; además, este sistema opera a través de dos dimensiones: la dimensión estructural y la dimensión funcional, lo que impone aún más complejidad a cualquier intento de ordenamiento o regulación.

México, desde hace varios años, ha intentado ejercer un esfuerzo político y legislativo con el fin de promulgar legislación en materia de "ciberseguridad", con resultados variados y poco interoperativos; en donde no sólo los intereses y capitales inmiscuidos han ejercido un rol de contención, sino que también la preparación e intereses de las personas y administraciones encargadas de legislar o asesorar ha jugado un rol importante en la manera en la cual el Estado Mexicano se relaciona con el sistema tecnológico digital, mejor conocido como ciberespacio.

Y tal como habría de esperarse, el cambio de estructuras políticas y sociales que significó el arribo de la 4T vino acompañado de un cambio en la manera en cual el Estado Mexicano se relaciona con el ciberespacio. Es así como hace un par de semanas, ante el Comité contra Drogas y Delincuencia de la Organización de Naciones Unidas (ONU), el presidente de la Comisión de Ciencia de la Cámara de Diputados, Javier López Casarín (de Partido Verde), presentó un proyecto de iniciativa de Ley Federal de Ciberseguridad, el cual implicó un proceso consultivo de más de 15 meses, con la participación de más de 300 especialistas de la academia, gobierno e iniciativa privada.

Y así como se mencionó en un principio, no faltaron aquellos grupos de la sociedad civil (financiada por EUA) en salir a denunciar la "represión" y "militarización" que implica tal iniciativa[1], así como señalar otras deficiencias. En contraposición, tampoco faltaron aquellas voces que presentan la iniciativa como una panacea por tratarse de un proyecto consultivo con múltiples partes interesadas.

En lo personal, considero que el proyecto representa un gran avance en materia de ciberseguridad y un fuerte paso para la construcción de elementos de cibersoberanía; sin embargo, la iniciativa presenta diversos vacíos y la necesidad de complementar, contextualizar y profundizar las propuestas; ya que, de lo contrario, algunos puntos terminarían siendo poco más que buenos deseos, tal como lo expondré a continuación.

Para comenzar, la iniciativa parte de una comprensión de "riesgos" y "peligros" bastante diversos y amplios, lo que implica que engloba aspectos como la defensa de la seguridad nacional, la seguridad pública, el cibercrimen, el ciber terrorismo, el ciber espionaje y otras fuentes de peligros, todo lo anterior sin una taxonomía específica o definida. Lo mismo sucede con los ejes rectores, los cuales abarcan áreas tan diversas como la economía, la cultura o la salud, lo que, en el mejor de los casos, se deberían de publicar leyes, normas o manuales profundizando en cada área.

Otra de las cosas que llama mi atención de las primeras páginas es que considero que una Ley en materia de ciberseguridad tendría que partir y fundamentar fuertemente qué entiende por el prefijo "ciber" y los aspectos a "asegurar", cosa que no es el caso, ya que no sólo no cuenta con una taxonomía clara de riesgos, amenazas y peligros, sino que el concepto de ciberespacio que presentan es laxo, inexacto y no abarca todo el sistema, ya que su atención se centra únicamente en cómo funciona el ciberespacio; así como el fuerte énfasis en únicamente la capacidad de comunicación e información, como si las infraestructuras de procesamiento y almacenamiento fueran meros complementos y no materia de consideraciones más profundas, tal como sucede con el caso del almacenamiento de datos o los riesgos derivados de la inestabilidad en la cadena internacional de producción y suministros de semiconductores.

El capítulo II contempla la creación de la Agencia Nacional de Ciberseguridad, la cual sería encargada de coordinar el desarrollo, implementación, evaluación, actualización y mejora continua de la Estrategia Nacional de Ciberseguridad; sin embargo, dicha agencia tiene un rango de competencias tan extensas y tan diversas, que se esperaría que en su marco organizacional partieran de una taxonomía de amenazas y riesgos más detallada y sectorial. Este es uno de los puntos que más preocupó a grupos como Artículo 19, ya que entre las atribuciones de la Agencia Nacional de Ciberseguridad se tiene contemplado el solicitar la baja "de direcciones IP, aplicaciones, dominios y sitios de internet a través de los cuales se realicen conductas ilícitas", lo que abre la pregunta ¿Qué se entiende por conducta ilícita? Sin mencionar que "la baja" significaría el bloqueo de acceso en muchos casos, ya que tales servicios no se encuentran siquiera alojados en servidores en México.

Entre los objetivos de la estrategia se encuentran materias tan amplias y diversas, que hasta se contempla el "Desarrollo de una industria de la ciberseguridad", aún cuando el concepto sea vago

En el capítulo IV se crea el Registro Nacional de Incidentes de Ciberseguridad, en donde "Incidente" se considera a aquellos "eventos que representan algún ataque, delito cibernético o evento que haya provocado una interrupción o degradación importante o relevante a la operación dentro de la infraestructura tecnológica de un organismo

público o privado", lo que es bastante vago, amplio y discrecional, ya que de facto equipara atacantes de naturaleza tan distinta como los criminales, terroristas, Estados hostiles u otros actores maliciosos.

Lo que se considera amenazas a la seguridad nacional resulta también vago, por citar un ejemplo: en el artículo 20 sección I se considera como una amenaza aquello que "Comprometa la operación y capacidades de las instancias de seguridad nacional", lo que podría incluir la escasez de componentes derivados de la dependencia extranjera, un ciberataque, el robo de información o un ataque a infraestructuras.

En el capítulo III artículo 28, la ley habla de la ciberdefensa y, aunque el tema es distinto a la ciberseguridad, se agradece la contemplación legal de esta área tan pendiente en el compendio de leyes nacionales; sin embargo, el artículo repite diversas inexactitudes, tal como el caso de la polémica sección I, en donde se faculta a la SEDENA y a la Secretaría de Marina "Monitorear el ciberespacio para prevenir, identificar y neutralizar ciberamenazas y ciberataques;", algo que a todas luces es imposible por su extensión, lo que daría pie a interpretaciones que carecerán de un sentido sectorial; ya ni se diga que se faculta el monitorear un espacio el cual no se toman la molestia de definir extensa y analíticamente.

La sección VI del artículo 28 es bastante peculiar, ya que faculta la realización de "operaciones militares y navales en el ciberespacio", lo que evidencia la imposibilidad de la creación de un mando común en el ciberespacio y le da facultades cibernéticas a dos áreas de las fuerzas armadas, como si existiera un ciberespacio naval y uno terrestre, salvo si se hablara sólo de infraestructuras, aunque dudo que este sea el caso.

En el capítulo V la propuesta de ley se centra en las infraestructuras críticas, en donde la ley fija la responsabilidad del cuidado de las infraestructuras a su operador, ya sea público o privado; además, señala la necesidad de integrar un Catálogo Nacional de Infraestructuras (cosa que considero lleva décadas pendiente y sólo aumentará su necesidad conforme otras áreas del funcionamiento del Estado se digitalicen). Esta sección también identifica las obligaciones de los operadores y administradores de infraestructuras; sin embargo, no establece criterios de auditoría, evaluación o cualquier acción que permita saber el cumplimiento o no de la norma, así como sus niveles de implementación.

Por otra parte, aunque la ley habla de la protección de datos personales (de manera más que somera), el documento nunca menciona al INAI, ni tampoco señala criterios más profundos en las responsabilidades de la protección de datos personales por terceras instancias; además, se dota de reservas a información asociada a la ciberseguridad, aún cuando su definición queda bastante abierta a la interpretación.

En lo que respecta a la prestación de servicios, uso de infraestructura digital y telecomunicaciones, la ley contempla que 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 deben tener una representación física en territorio nacional y registrarse ante la Agencia Nacional de Ciberseguridad, lo que debería venir acompañado de identificadores y métricas, ya que tal definición podría aplicar a buena parte de actores que prestan servicios en internet y cuyo rastro no puede ser identificado de antemano a menos que tenga un número considerable de usuarios nacionales. A su vez, la sección VIII habla de la necesidad de privilegiar que la información de los usuarios se encuentre en territorio nacional, algo que aplaudo enormemente, pero que se antepone al T-MEC, en donde se imponen salvaguardas para que no se obligue a empresas estadounidenses a almacenar datos de mexicanos en territorio nacional.

También esta ley dota a la Agencia, la Fiscalía General de la República, CERT-MX y autoridades judiciales competentes el solicitar la baja de direcciones IP, aplicaciones, dominios y sitios de internet, algo que sin duda es bastante extenso, riesgoso y discrecional; por lo que se deberían contar con criterios claros, específicos y fundamentados para avalar tales decisiones; sin mencionar que el bloqueo sería sobre el acceso (y no la baja), especialmente a aquellos servicios que no se encuentren alojados en territorio nacional.

El título sexto de la propuesta trata sobre la cultura y educación en ciberseguridad; sin embargo, es llamativo que entre las facultades centralizadoras de esta propuesta no se contemple un proyecto homologado y holístico de educación, sino que se deja la responsabilidad a los poderes de la unión, instituciones públicas y privadas, lo que evidentemente tendrá como resultado una cultura de la ciberseguridad bastante improvisada.

Por último, en lo que corresponde a los delitos cibernéticos, resulta interesante que el documento no menciona la influencia de la Convención de Budapest ni la armonización del marco de la propuesta con dicha convención; sin embargo, a efectos prácticos, esta propuesta de ley acerca más al país a ser un pleno adherente a tal Convención, cosa que aplaudo.

En conclusión, considero que la propuesta de ley es un paso enorme en materia de leyes cibernéticas; sin embargo, me parece que el objetivo de la ley es tan amplio y ambicioso que se pierde en la generalidad, lo que puede dar paso a omisiones o discrecionalidad; además, el documento carece de una taxonomía, identificadores y métricas, lo que aunado a las responsabilidades individuales que promueve el documento, podría dar pie a un marco de ciberseguridad heterogéneo, disparejo, desigual y sin armonía en absoluto, con la posibilidad de la conformación de instituciones muy poderosas, discrecionales e interpretativas por los administradores en turno. Además, la ley crea una serie de puestos que abarcarán una fuerte demanda de expertos, aunque nunca se menciona una estrategia de captación de talento en un mercado fuertemente competitivo y los requisitos de especialistas de punta

[1]https://articulo19.org/iniciativa-de-ley-de-ciberseguridad-amenaza-los-derechos-humanos-y-promueve-la-militarizacion/

Publicado en Punto de Referencia. Dirección original: https://puntodereferencia.mx/opinion/analisis-a-la-iniciativa-de-ley-federal-de-ciberseguridad
Descargado el 21 de noviembre de 2026.