INICIATIVA QUE ADICIONA EL ARTÍCULO 5°. DE LA LEY DE SEGURIDAD NACIONAL, A CARGO DEL DIPUTADO JAIME MARTÍNEZ LÓPEZ, DEL GRUPO PARLAMENTARIO DE MORENA.

El que suscribe, Jaime Martínez López, diputado federal de la LXV Legislatura e integrante del Grupo Parlamentario de Morena, con fundamento en los artículos 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos y, en ejercicio de la facultad conferida en los artículos 6, numeral 1, fracción I, 77, numeral 1, y 78 del Reglamento de la Cámara de Diputados, presenta iniciativa con proyecto de decreto por el que se adiciona la fracción XIII al artículo 5, de la Ley de Seguridad Nacional, en materia de amenazas a sistemas informáticos que vulneren la democracia y las capacidades del Estado, al tenor de la siguiente

Exposición de Motivos

Un Estado democrático y de derecho debe tener su origen y desarrollo en la voluntad y la participación ciudadana, pero, además, que todos los habitantes estén sometidos al imperio de la Ley, así como en los principios y valores determinados por las condiciones históricas de la población, pero siempre en busca de las mejores condiciones de vida.

Respecto a la vida democrática nacional, México es una República representativa, democrática, laica y federal; es “democrático, considerando a la democracia no solamente como una estructura jurídica y un régimen político, sino como un sistema de vida fundado en el constante mejoramiento económico, social y cultural del pueblo” (artículo 3 constitucional).

En el contexto antes referido, los procesos electorales en las democracias en general, tienden al aprovechamiento de las tecnologías de información y comunicaciones siendo por tanto fundamental abordar las amenazas cibernéticas que atenten contra la democracia, hechos que han sido recurrentes como lo refiere la Organización de Estados Americanos (OEA).

“Recientemente, se han presentado presuntos incidentes de piratería en elecciones latinoamericanas, desde desfigurar sitios web de campañas, entrar en las bases de datos de otros partidos para realizar espionaje y usar software malicioso. moderna, un proceso electoral puede volverse vulnerable a medida que las instituciones adoptan nuevas tecnologías” (OEA, página 10).

Por otro lado, en cada expresión social, el Estado debe incorporar principios para legitimarse y ser reconocido por la sociedad. De esta manera, no se puede pensar en decisiones ajenas a la voz o la visión de la ciudadanía y de sus diversos representantes, pues ello derivaría en actitudes arbitrarias de los servidores públicos y lesivos de los derechos fundamentales tutelados por nuestra Carta Magna.

Al respecto, es necesario precisar que un Estado constitucional y democrático se funda en las libertades, individuales y colectivas, concibiendo al Estado bajo los principios de libertad,

orden y justicia social, en un marco de seguridad para el desarrollo, tomando en cuenta a la seguridad como la esencia y el deber ser del Estado.

En esta tesitura, resulta fundamental la legislación que norma la seguridad nacional, cuyo objetivo es garantizar la defensa de la Nación y por supuesto del Estado mismo como organización política democrática, cimentada en los derechos fundamentales del gobernado.

Ahora bien, ¿qué se entiende por seguridad nacional?

Al respecto, el Glosario de Términos Unificados en Seguridad Nacional elaborado por el Colegio de Defensa Nacional y el Centro de Estudios Superiores Navales, la define en los términos siguientes:

> "Condición necesaria que proporciona el Estado para garantizar la prevalencia de su integridad territorial, independencia, soberanía, estado de derecho, su estabilidad política, social y económica y la consecución de sus Objetivos Nacionales". (Codenal - Semar, 2018, página 23)

Es de destacarse que la definición del glosario citado considera la seguridad nacional como una "condición" para garantizar la prevalencia de su integridad territorial, independencia, soberanía, estado de derecho, su estabilidad, **con base en el supuesto de riesgos o amenazas que vulneren gravemente la existencia del Estado.**

Adolfo Aguilar Zinser señala que para México la noción de seguridad se refiere "en esencia a la protección y ejercicio de la soberanía nacional, entendida ésta como un atributo político-jurídico que abarca el territorio, a una zona económica marítima exclusiva y a determinados recursos naturales".[1]

De los conceptos vertidos con antelación, resulta claro que los conceptos de Seguridad Nacional pueden modificarse de acuerdo con las necesidades de la realidad social conforme al marco jurídico actual; basta señalar como ejemplo que a partir del crecimiento del ilícito de carácter internacional del narcotráfico y de los delitos ligados al mismo, la seguridad nacional ha tenido profundas transformaciones.

En el marco constitucional, el artículo 89 fracción VI de nuestra Carta Magna, otorga al presidente de la República a "Preservar la seguridad nacional, en los términos de la ley respectiva"

Por su parte, la Ley de Seguridad Nacional refiere en su artículo 3, a la seguridad nacional como "las acciones destinadas de manera inmediata y directa a mantener la integridad, estabilidad y permanencia del Estado mexicano [...]".

En tanto, el artículo 5 dice que son amenazas a la seguridad nacional:

- Actos tendentes a consumar espionaje, sabotaje, terrorismo, rebelión, traición a la patria, genocidio, en contra de los Estados Unidos Mexicanos dentro del territorio nacional;

- Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano;

- Actos que impidan a las autoridades actuar contra la delincuencia organizada;

- Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos;

- Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada;

- Actos en contra de la seguridad de la aviación;

- Actos que atenten en contra del personal diplomático;

- Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva;

- Actos ilícitos en contra de la navegación marítima;

- Todo acto de financiamiento de acciones y organizaciones terroristas;

- Actos tendentes a obstaculizar o bloquear actividades de inteligencia o contrainteligencia;

- Actos tendentes a destruir o inhabilitar la infraestructura de carácter estratégico o indispensable para la provisión de bienes o servicios públicos.

De un análisis a las hipótesis contenidas en la Ley de Seguridad Nacional, se observa que no se encuentran como amenazas a la seguridad nacional, los actos tendentes a acceder, conocer, obtener, copiar o utilizar información, modificar, destruir, ocasionar pérdida de información contenida en sistemas informáticos **que vulneren la democracia y las capacidades del Estado.**

No obstante que las instituciones del Estado cuentan con sistemas de ciberseguridad para protegerse de los ataques cibernéticos, es un hecho que existen intrusiones recurrentes a dichos sistemas, lo que puede constituir en afectaciones a la seguridad nacional.

Para contextualizar lo anterior es importante definir a la ciberseguridad: "**el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de información de la organización y los usuarios en el ciberentorno"** (Guardia Nacional, 2021, página 41).

Así, la seguridad nacional de los estados modernos depende en gran medida de su capacidad para protegerse contra los ataques cibernéticos. Esto se debe a que muchos de

los sistemas críticos de un país, como los sistemas de energía, transporte, comunicaciones y defensa que dependen de la tecnología informática y están interconectados.

Un ataque a uno de estos sistemas puede tener graves consecuencias para la seguridad y la economía del país, lo que lo hace vulnerable a las amenazas cibernéticas.

Por tal razón, es necesario incluir **como amenaza a la seguridad nacional los actos que emplean el ciberespacio para atacar la información contenida en sistemas o equipos de informática del Estado, los cuales se encuentran protegidos por medidas y técnicas de ciberseguridad, con la finalidad de generar las condiciones para identificar riesgos, la probabilidad de ocurrencia y disminuir la vulnerabilidad del Estado.**

Al efecto, considero que los gobiernos deben desarrollar políticas claras y coherentes en materia de ciberseguridad y trabajar en estrecha colaboración con el sector privado y otros países para garantizar la protección efectiva de los sistemas críticos y los datos confidenciales.

En el rubro internacional, el Consejo de Seguridad de la ONU exhorta a los Estados Miembros a "establecer o reforzar las alianzas nacionales, regionales e internacionales con las partes interesadas, tanto públicas como privadas, según proceda, para intercambiar información y experiencias a fin de prevenir, proteger, mitigar e investigar los daños causados por atentados terroristas contra instalaciones de infraestructura vital, así como para responder a ellos y recuperarse de ellos, en particular mediante actividades conjuntas de capacitación, y la utilización o el establecimiento de redes de alerta de emergencia o de comunicación pertinentes".[2]

El Convenio de Budapest sobre Ciberdelincuencia, adoptado en 2001, es un tratado internacional que tiene como objetivo combatir el ciberdelito y promover la cooperación internacional en materia de ciberseguridad. El convenio establece la obligación para los Estados parte de adoptar medidas legislativas y técnicas para prevenir y combatir el ciberdelito, así como para proteger los sistemas y datos informáticos contra los ataques.

Además, el Convenio de Budapest, mejor conocido como Convenio sobre Ciberdelincuencia, que surge de la preocupación por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes.

El citado Convenio, obliga a los Estados parte a criminalizar una serie de delitos informáticos, incluyendo la interferencia ilegal en sistemas informáticos, la interceptación ilegal de datos y el acceso no autorizado a sistemas informáticos. Por otro parte, se establecen medidas para garantizar la privacidad de los datos y la protección de las víctimas de ciberdelitos. Los Estados parte también se comprometen a promover la cooperación internacional en la investigación y enjuiciamiento de delitos cibernéticos.

El Convenio de Budapest ha sido ratificado por más de 60 países, incluyendo a los Estados Unidos, la Unión Europea, Canadá y Australia, lo que demuestra la importancia que se le da a la regulación de la ciberseguridad a nivel internacional.

Por otra lado, en el contexto regional, de acuerdo con la Organización de los Estados Americanos (OEA) en la nueva modalidad del gobierno digital "la aplicación de las Tecnologías de la Información y la Comunicación en el funcionamiento del sector público, [... tiene por ...] objetivo incrementar la eficiencia, la transparencia y la participación ciudadana",[3] que va tomando fuerza por la "confianza" que el ciudadano deposita en las autoridades para llevar a cabo sus trámites convencionales, a través de plataformas digitales.

En consecuencia, si los ciudadanos perciben que el gobierno no puede proteger la información, pierden confianza en la capacidad del gobierno para garantizar la disponibilidad, integridad y disponibilidad de los datos digitales.

La recomendaciones internacionales y regionales, así como el convenio de Budapest han servido como base para la cooperación internacional en la lucha contra el ciberdelito y han impulsado la adopción de leyes y políticas en todo el mundo para prevenir y combatir los delitos informáticos.

El Programa Nacional de Seguridad Pública 2022-2024 que deriva del Plan Nacional de Desarrollo, considera "la mejora en las condiciones de ciberseguridad para la prevención de incidentes que afecten la infraestructura crítica del país y la erradicación de manera prioritaria de las expresiones de corrupción con el fin de garantizar la paz y preservar la seguridad nacional" (PNSP, página 38).

El programa antes indicado, contempla la estrategia prioritaria de "fortalecer los mecanismos de investigación para prevenir las conductas delictivas en los sitios web", con las siguientes acciones:

- Implementar mecanismos de detección de ataques en ciberseguridad a la infraestructura tecnológica que permita asegurar y resguardar la información contenida en las plataformas tecnológicas.

- Establecer acuerdos con organismos nacionales e internacionales públicos y privados que permitan generar medidas para la prevención, investigación y persecución del delito en materia de ciberseguridad.

- Diseñar e implementar mecanismos para dar respuesta a los incidentes de ciberseguridad, así como al seguimiento de las acciones propuestas para su mitigación y prevención.

Por lo anterior es evidente que, las amenazas a través del ciberespacio deben ser de especial consideración ya que pueden causar afectaciones a los campos del poder (político, social, militar, económico y tecnológico), por ejemplo: manipulación mediática a través de medios digitales para desestabilizar gobiernos (campo político); ciberataques por parte de la

delincuencia organizada (campo social); difundir a través de las tecnologías de información y comunicaciones, información sensible que genere incertidumbre financiera (campo económico); sustraer de equipos informáticos información de inteligencia que perjudique de las operaciones de las fuerzas armadas (campo militar); y robo de tecnologías (campo tecnológico).

Sin embargo, para que determinada amenaza sea materia de seguridad nacional debe ser un "acto generado por el poder de otro Estado, o por actores no estatales, que puede vulnerar de modo particularmente grave las aspiraciones, intereses y objetivos nacionales del Estado mexicano".[4]

Es importante señalar, que los actos tendentes al acceso ilícito a sistemas y equipos de informática deben ser tratados con la seriedad que merecen y se tomen las medidas para prevenirlos y combatirlos. Esto incluye, la promulgación de leyes y políticas adecuadas para proteger la seguridad de los sistemas de información, y la cooperación entre los sectores público y privado.

Puntualizando, dichos actos pueden ser utilizados por gobiernos extranjeros u otros actores no estatales para llevar a cabo actividades de espionaje, sabotaje o guerra cibernética.

De ahí que existan las operaciones de guerra cibernética, que pueden incluir la interrupción de la infraestructura crítica, el sabotaje de sistemas informáticos, la interrupción de servicios de comunicación y otras actividades económicas y sociales diversas con graves consecuencias para la seguridad Nacional.

Es innegable que las amenazas a la integridad, estabilidad y permanencia del Estado, generalmente provienen del exterior, por lo tanto, es fundamental tomar previsiones en el ámbito jurídico ante los eventos que ocurren en el contexto mundial.

Los ciberataques se han convertido en un arma estratégica, por ejemplo: en el conflicto Rusia y Ucrania. Según la BBC News, se han realizado "ataques cibernéticos a varios sitios web de los departamentos gubernamentales y bancarios de este país [...Ucrania...], que en ocasiones han llevado al colapso total de su sistema [...] acusaron al Kremlin de estar detrás de la ofensiva —que afectó a los sitios web del Parlamento, del Servicio de Seguridad y del ministerio de Relaciones Exteriores de Ucrania, entre otros— y dijeron que los piratas informáticos 'ya no intentan ocultar su identidad'".[5]

Otro ejemplo: de acuerdo con las fuentes consultadas por el diario Excelsior, del 22 de mayo de 2018, 'bots' de Twitter influyeron en los sufragios afectando la democracia de la Unión Europea y de los Estados Unidos.

"Los 'bots' de Twitter han influido en el resultado de las elecciones presidenciales de Estados Unidos y en la votación del Brexit, de 2016, en un 3.23 y un 1.76 por ciento en los resultados que dieron la victoria a Donald Trump y a la marcha de la Unión Europea, respectivamente, según recoge un estudio económico de la Oficina Nacional de Investigación Económica (National Bureau of Economic Research /NBER), de Estados Unidos.

Las cuentas automatizadas desempeñaron un papel importante en dos de las votaciones más destacadas de 2016: las elecciones presidenciales de Estados Unidos y la salida o permanencia de Reino Unido de la Unión Europea, como concluye un estudio conjunto de las universidades de California en Berkeley (Estados Unidos) y Swansea (Reino Unido).[6]

En el contexto nacional, de acuerdo con fuentes de información del diario El Economista:[7]

- En informes divulgados a través de la plataforma de transparencia, Petróleos Mexicanos, la Presidencia de la República y la Secretaría de Educación Pública son las dependencias con mayor número de ciberataques, pues hasta el 2021 las instituciones registraron más 128 millones, 78 millones y 3 millones de ataques respectivamente.

- Por otro lado, también figura el Instituto Nacional Electoral con 2 millones 968 mil 244 ataques; la Suprema Corte de Justicia de la Nación con 312 mil 716; Banxico con 17 mil 669; la Secretaría de Salud con 14 mil 742; la Secretaría de Marina con 4 mil 608; el ejército con mil 107; y, Economía con 15 ataques a sus sistemas en la primera mitad del 2021.

- México se ha convertido en objetivo atractivo para los cibercriminales, ha padecido el 66 por ciento de los ciberataques ocurridos en América Latina en el periodo 2021 – 2022, lo que provocó pérdidas de entre 3000 y 5000 millones de dólares por año de acuerdo con la Asociación de Bancos México y la American Chamber.

Asimismo, en el Programa Sectorial de Seguridad y Protección Ciudadana 2020-2024, indica que en los 6 años previos se neutralizaron alrededor de 26 mil sitios web con actividades ilícitas.

Con base en lo anteriormente expuesto y tomando en cuenta que el ciberespacio manifiesta un crecimiento constante que integra a más del 50 por ciento de la población mundial, con muy diversos riesgos y amenazas tanto a la sociedad como el Estado, resulta de suma importancia que los actos tendentes a afectar gravemente la información contenida en sistemas informáticos que vulneren la democracia y las capacidades del Estado sean considerados como amenazas a la seguridad nacional.

Por tal razón, considero de particular importancia adicionar una fracción XIII al artículo 5 de la Ley de Seguridad Nacional con la finalidad de establecer como amenazas a la seguridad nacional **los actos tendentes a acceder, conocer, obtener, difundir, copiar o utilizar información, modificar, destruir, ocasionar pérdida de información contenida en sistemas informáticos que vulneren la democracia y las capacidades del Estado.**

Para ilustrar lo anterior, se presenta el siguiente cuadro comparativo:

LEY DE SEGURIDAD NACIONAL	
TEXTO VIGENTE	ADICIÓN PROPUESTA
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; II. Actos de interferencia extranjera en los asuntos nacionales que puedan implicar una afectación al Estado Mexicano; III. Actos que impidan a las autoridades actuar contra la delincuencia organizada; IV. Actos tendentes a quebrantar la unidad de las partes integrantes de la Federación, señaladas en el artículo 43 de la Constitución Política de los Estados Unidos Mexicanos; V. Actos tendentes a obstaculizar o bloquear operaciones militares o navales contra la delincuencia organizada; VI. Actos en contra de la seguridad de la aviación; VII. Actos que atenten en contra del personal diplomático; VIII. Todo acto tendente a consumar el tráfico ilegal de materiales nucleares, de armas químicas, biológicas y convencionales de destrucción masiva; IX. Actos ilícitos en contra de la navegación marítima; X. Todo acto de financiamiento de acciones y organizaciones terroristas; 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, y	**Artículo 5.-** Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional. I a XII... **XIII. Actos tendentes a acceder, conocer, obtener, difundir, copiar o utilizar información, modificar, destruir, ocasionar pérdida de información contenida en sistemas informáticos que vulneren la democracia y las capacidades del Estado.**

Por lo anteriormente expuesto y con fundamento en el artículo 71, fracción II, de la Constitución Política de los Estados Unidos Mexicanos, someto a consideración de este honorable pleno la siguiente iniciativa con proyecto de

Decreto por el que se adiciona una fracción XIII al artículo 5o. de la Ley de Seguridad Nacional

Único. Se adiciona una fracción XIII al artículo 5° de la Ley de Seguridad Nacional, para quedar como sigue:

Artículo 5....

I al XII...

XIII. Actos tendentes a acceder, conocer, obtener, difundir, copiar o utilizar información, modificar, destruir, ocasionar pérdida de información contenida en sistemas informáticos que vulneren la democracia y las capacidades del Estado.

Transitorio

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

Notas

1 Aguilar Zinser, Adolfo, "La seguridad mexicana vista por Estados Unidos. Los dos mitos"

2 https://www.un.org/counterterrorism/es/cybersecurity

3 https://www.gob.mx/blog/articulos/que-es-el-gobierno-electronico

4 https://www.gob.mx/cms/uploads/attachment/file/535129/Amenazas_Riesgos.pdf

5 https://www.bbc.com/mundo/noticias-internacional-60508957

6 https://www.excelsior.com.mx/hacker/bots-si-influyeron-en-el-brexit-y-las-elecciones-presidenciales-de-eu-estudio/1240473

7 https://www.eleconomista.com.mx/tecnologia/El-66-de-los-ataques-ciberneticos-de-America-Latina-ocurren-en-Mexico-20230217-0048.html

Dado en el Palacio Legislativo de San Lázaro, a 11 de abril de 2023.

Diputado Jaime Martínez López (rúbrica)