INICIATIVA QUE REFORMA Y ADICIONA DIVERSAS DISPOSICIONES DE LA LEY DE SEGURIDAD NACIONAL, EN MATERIA DE CIBERSEGURIDAD, A CARGO DEL DIPUTADO MARCO ANTONIO PÉREZ GARIBAY, DEL GRUPO PARLAMENTARIO DE MORENA.

Quien suscribe, diputado Marco Antonio Pérez Garibay, con fundamento en lo dispuesto en los artículos 71, fracción II, y 72 de la Constitución Política de los Estados Unidos Mexicanos; y 6, numeral 1, fracción I, y 6, numeral 1, fracción I, 77 y 78 del Reglamento de la Cámara de Diputados, somete a consideración de esta soberanía la iniciativa con proyecto de decreto por el que se reforman y adicionan diversas disposiciones de la Ley de Seguridad Nacional, en materia de ciberseguridad, al tenor de la siguiente

Exposición de Motivos

El origen fundante del Estado es el de la protección de la seguridad de las personas, éste se materializa en la posibilidad verdadera de ejercer con plenitud nuestros derechos y en el alcance plural de una vida digna. Es el Estado, entonces, el encargado de institucionalizar (orgánica y jurídicamente) los esfuerzos que desde el gobierno vengan para cumplir con su fin último.

En este sentido, el texto constitucional, en el artículo 21, contempla a la seguridad nacional como una condición indispensable para el bienestar popular, definiéndola como la responsabilidad estatal de salvaguardar la integridad y los derechos de las personas, así como de preservar las libertades, el orden y la paz públicos.

Así, a través del cumplimiento de las responsabilidades constitucionales en la materia que el artículo 69 de la Carta Magna le da al Gobierno de México, se creó la Estrategia Nacional de Seguridad Pública. Esta Estrategia Nacional marca la pauta de acción de todas las instancias gubernamentales en aras de tener como prioridad del Estado Mexicano a la Seguridad Nacional.

La presente iniciativa, entonces, tiene como punto de partida la búsqueda irrestricta de la Seguridad Nacional en todas las dimensiones de la vida pública del país. Acción impensable sin considerar la dimensión tecnológica, virtual y digital de esta última, y por tanto su objetivo fundamental es la consideración e inclusión de la ciberseguridad nacional como un elemento indispensable para la garantía de la seguridad en todo el territorio nacional mexicano.

Es importante destacar que la ciberseguridad nacional adquiere relevancia, debido a la creciente tendencia del uso de datos sensibles e información confidencial en plataformas y medios digitales. Esta información, de correr riesgo o de caer en manos de adversarios del Gobierno de México, puede ser un instrumento para poner en riesgo la seguridad e integridad de las instituciones del Estado y de toda la población. Es por ello que, para poder garantizar la seguridad nacional, en materia de ciberseguridad, el primer paso es contemplar en su legislación los conceptos que nos protegen en el apartado digital para estar oportunamente preparados; conceptos como ciberseguridad nacional, jaqueo e información digital sensible.

En este orden de ideas es válido señalar que nuestro país, de acuerdo con la cuarta edición del Índice Global de Ciberseguridad de la Unión Internacional de Comunicaciones (que es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación), tiene una puntuación de 37.66 puntos sobre 100 en su capacidad de asegurar la ciberseguridad para el gobierno y sus habitantes, posicionándolo en el lugar 84 de 160 a nivel mundial. Tan es así que, en los últimos tiempos, el gobierno mexicano ha sido sujeto de múltiples ataques y jaqueo que ponen en riesgo información digital sensible que, a su vez, podría representar un riesgo en la ciberseguridad nacional en caso de que se use peligrosamente.

Sabemos que dependencias gubernamentales han sido víctimas de 'ransomware' o secuestro de datos. Tal es el caso de la filtración de información digital sensible de Pemex en 2019,[1] de la Comisión Nacional de Seguros y Fianzas en el 2020[2] e, incluso, de la Sedena (Secretaría de la Defensa Nacional) en el 2022,[3] siendo éste el ciberataque más grave y de mayor impacto en la historia reciente de México.

Sabemos que **parte importante del funcionamiento óptimo de la infraestructura crítica del Estado, depende directamente de la ciberseguridad.** Es responsabilidad del Gobierno de México garantizar la seguridad nacional a partir de la defensa del ciberespacio. Con base en todo lo anterior, podemos afirmar que la intención principal de la presente reforma es la de crear certeza jurídica en la legislación en materia de seguridad nacional, respecto a los ataques que se han suscitado en tiempos recientes, poniendo siempre por delante el interés público y del Estado mexicano.

Esta propuesta busca: agregar los conceptos de 'ciberseguridad nacional', 'jaqueo' e 'información digital sensible' a la legislación en materia de seguridad nacional; la consideración de las amenazas dentro del ciberespacio a la seguridad nacional; dotar de facultades al Centro de Investigación y Seguridad Nacional para preservar la ciberseguridad; y, proteger la información sensible que pudiera poner en riesgo la ciberseguridad nacional.

Cuadro comparativo

Por lo anteriormente expuesto someto a consideración de esta soberanía el siguiente

Decreto por el que se reforman y adicionan diversas disposiciones de la Ley de Seguridad Nacional, en materia de ciberseguridad

Único. Se reforman las fracciones XII y XIII, adicionándose una fracción XIV al artículo 5; se reforman las fracciones V y VI, adicionándose las fracciones VII, VIII y IX al artículo 6; se reforma la fracción IX del artículo 19; y se reforman las fracciones I y II, adicionándose una fracción III al artículo 51 de la Ley de Seguridad Nacional.

Para quedar como sigue:

Ley de Seguridad Nacional

Artículo 5. Para los efectos de la presente Ley, son amenazas a la Seguridad Nacional:

I. a **XI** …

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

XIII. [Actos ilícitos en contra del fisco federal a los que hace referencia el artículo 167 del Código Nacional de Procedimientos Penales]**, y**

XIV. Actos de jaqueo en contra del Estado mexicano, que pongan en riesgo información digital sensible de interés público y que atenten contra la ciberseguridad nacional.

Artículo 6. Para los efectos de la presente Ley, se entiende por:

I. a **IV** …

V. Información gubernamental confidencial: Los datos personales otorgados a una instancia por servidores públicos, así como los datos personales proporcionados al Estado Mexicano para determinar o prevenir una amenaza a la Seguridad Nacional**;**

VI. Agentes Extranjeros: Funcionarios extranjeros que en sus países de origen ejercen funciones policiales, de inspección o de supervisión de las leyes y otras disposiciones de carácter reglamentario o aquéllas de carácter técnico especializado**;**

VII. Ciberseguridad nacional: El conjunto de elementos, medidas, técnicas y equipos destinados a controlar la seguridad informática de la nación, la cual tiene como fin la protección a los sistemas digitales importantes y a la información confidencial ante los ataques digitales;

VIII. Información digital sensible: Información en medios digitales que contiene datos privados o confidenciales: nombres, fechas, ubicaciones, datos financieros o de seguridad, o cualquier otra información que, cuya publicidad, pudiese atentar contra la ciberseguridad nacional, y

IX. Jaqueo: Ataque cibernético que tiene como objetivo acceder ilegalmente a sistemas informáticos y manipularlos.

Artículo 19. Son atribuciones del Centro:

I. a **VIII** …

IX. Operar la tecnología de comunicaciones especializadas, **para resguardar entre otros actos en contra del Estado mexicano, la ciberseguridad nacional y evitar actos de jaqueo,** en cumplimiento de las atribuciones que tiene encomendadas o en apoyo de las instancias de gobierno que le solicite el Consejo;

X. a **XI** …

Artículo 51. Además de la información que satisfaga los criterios establecidos en la legislación general aplicable, es información reservada por motivos de Seguridad Nacional:

I. Aquella cuya aplicación implique la revelación de normas, procedimientos, métodos, fuentes, especificaciones técnicas, tecnología o equipo útiles a la generación de inteligencia para la Seguridad Nacional, sin importar la naturaleza o el origen de los documentos que la consignen**;**

II. Aquella cuya revelación pueda ser utilizada para actualizar o potenciar una amenaza**, o**

III. Aquella que pueda poner en riesgo la ciberseguridad nacional.

Transitorios

Primero. Publíquese el presente Decreto en el Diario Oficial de la Federación.

Segundo. El presente Decreto entrará en vigor al día siguiente de su publicación.

Tercero. Se derogan todas aquellas disposiciones que se opongan al presente decreto.

Notas

1 Comunicado No. 48 del 11 de noviembre del 2019 de Petróleos Mexicanos.

2 Comunicado oficial realizado el 28 de noviembre del 2020 a través de sus redes sociales institucionales.

3 Comunicado de prensa 161 de la Secretaría de Defensa Nacional del 4 de octubre del 2022.

Palacio Legislativo de San Lázaro, a 21 de febrero del 2023

Diputado Marco Antonio Pérez Garibay (rúbrica)