INICIATIVA QUE REFORMA, ADICIONA Y DEROGA DIVERSAS DISPOSICIONES DE LAS LEYES DE SEGURIDAD NACIONAL; GENERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS; Y ORGÁNICA DE LA ADMINISTRACIÓN PÚBLICA FEDERAL, Y DEL CÓDIGO PENAL FEDERAL, EN MATERIA DE PROTECCIÓN DE BASES DE DATOS POBLACIONALES ESTRATÉGICAS DEL ESTADO, A CARGO DEL DIPUTADO FELIPE MIGUEL DELGADO CARRILLO, DEL GRUPO PARLAMENTARIO DEL PVEM

El que suscribe, diputado Felipe Miguel Delgado Carrillo, integrante del Grupo Parlamentario del Partido Verde Ecologista de México, de la LXVI Legislatura de la Cámara de Diputados del Honorable Congreso de la Unión, con fundamento en lo dispuesto en los artículos 71, fracción II, y 72 de la Constitución Política de los Estados Unidos Mexicanos, así como en los artículos 6, numeral 1, fracción I, 77 y 78 del Reglamento de la Cámara de Diputados, somete a consideración de esta soberanía la presente iniciativa con proyecto de decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley de Seguridad Nacional, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de la Ley Orgánica de la Administración Pública Federal y del Código Penal Federal, en materia de protección de bases de datos poblacionales estratégicas del Estado, al tenor de la siguiente

Exposición de Motivos

En la era digital, la información poblacional se ha convertido en un activo estratégico del Estado mexicano. Las bases de datos que concentran datos personales de millones de personas –registros de identidad, padrones electorales, expedientes de seguridad social, entre otros– son hoy tan relevantes para el funcionamiento nacional como las instalaciones físicas de energía, comunicaciones o transporte. Su protección eficaz resulta esencial para garantizar la continuidad del Estado, la confianza ciudadana en las instituciones y el pleno ejercicio de derechos fundamentales.

No obstante, en los años recientes México ha enfrentado incidentes alarmantes de ciberataques, filtraciones masivas y venta ilegal de datos personales sustraídos de sistemas gubernamentales. Tales hechos han puesto de relieve graves vulnerabilidades en la custodia de la información poblacional, comprometiendo derechos constitucionales, la seguridad nacional y la gobernabilidad democrática.

En este contexto, la presente iniciativa propone declarar a las bases de datos poblacionales estratégicas en poder del Estado como componentes de seguridad nacional e infraestructura crítica. Esta declaratoria permitirá reconocer jurídicamente su relevancia estratégica, establecer medidas reforzadas de protección y ciberseguridad, tipificar conductas delictivas específicas en torno a ellas y articular mecanismos institucionales acordes con los más altos estándares internacionales.

A continuación se exponen las razones que motivan la propuesta, justificando su necesidad, su encuadramiento constitucional y su consonancia con las mejores prácticas comparadas, en particular los modelos de protección de datos críticos desarrollados en Corea del Sur y Estonia.

Bases de datos poblacionales como infraestructura crítica del Estado

La Ley de Seguridad Nacional encomienda al Consejo de Seguridad Nacional la identificación e inventario de la infraestructura estratégica del país, entendida como aquellas instalaciones, sistemas y recursos cuya afectación pondría en peligro la integridad, estabilidad y permanencia del Estado mexicano. Tradicionalmente, este concepto se ha asociado a sectores como el energético, las comunicaciones, el sistema financiero o las instalaciones militares.

Sin embargo, la definición operativa de instalación estratégica es más amplia: comprende "los espacios, inmuebles, construcciones, equipos y demás bienes" indispensables para el funcionamiento de las actividades estratégicas definidas en la Constitución, así como aquellos que aseguran la continuidad del Estado. Importa subrayar que una instalación estratégica no se agota en edificaciones o infraestructura física; incluye también sistemas informáticos, software, redes de comunicación y personal especializado. En otras palabras, los sistemas de información gubernamentales pueden constituir infraestructura estratégica cuando resultan imprescindibles para la operación del país.

Bajo esa lógica, las bases de datos poblacionales –por ejemplo, el Registro Nacional de Población (Renapo) que administra la CURP, el padrón electoral del Instituto Nacional Electoral, las bases de derechohabientes del IMSS y del ISSSTE, entre otras– califican como infraestructura crítica. En ellas se concentran datos personales (nombre, fecha de nacimiento, domicilio, identificadores únicos, datos biométricos, historial de servicios) de prácticamente toda la población. Son la columna vertebral informativa para la prestación de servicios públicos esenciales: identificación de las personas, seguridad social, salud pública, planeación económica, política fiscal, seguridad pública y programas sociales, entre otros.

Su interrupción, destrucción, alteración masiva o uso indebido tendría un impacto profundamente disruptivo en la sociedad y en la gobernanza. Así, una pérdida de integridad en el Renapo afectaría la expedición de documentos de identidad en todo el territorio; una caída o manipulación maliciosa de la base del IMSS podría paralizar la atención médica y el pago de pensiones a nivel nacional; una filtración del padrón electoral vulneraría principios democráticos y socavaría la confianza en los procesos electorales. Escenarios de esa naturaleza comprometen directamente la seguridad nacional, entendida como la preservación del orden constitucional, las instituciones y la población frente a amenazas internas o externas.

El derecho comparado confirma que la información gubernamental esencial es tratada como componente crítico del Estado. En Estonia, país pionero en gobierno digital, la legislación define la infraestructura de información crítica como los sistemas de información y comunicación cuya continuidad, confiabilidad y seguridad son esenciales para el funcionamiento adecuado del país, integrándolos explícitamente en la infraestructura crítica nacional. De manera semejante, en Corea del Sur la normativa en la materia incluye los sistemas electrónicos vinculados con la administración pública y la seguridad nacional dentro de las infraestructuras de información a proteger con prioridad. En ambos casos se

reconoce que la información poblacional e institucional es un activo estratégico que debe resguardarse al más alto nivel.

Siguiendo esta tendencia, México debe dar el paso normativo de reconocer explícitamente sus bases de datos poblacionales estratégicas como infraestructura crítica y objeto de seguridad nacional. Esta declaratoria proporcionará el marco legal para destinar recursos, capacidades y protocolos excepcionales de protección, del mismo modo que se hace con instalaciones estratégicas físicas como puertos, aeropuertos, refinerías o redes eléctricas.

Riesgos actuales: ciberataques, filtraciones masivas y venta ilegal de datos

Diversos incidentes recientes han puesto de manifiesto que nuestras bases de datos poblacionales están expuestas a amenazas reales e inminentes. Cada uno de ellos subraya la urgencia de reforzar su protección:

Ciberataques y filtraciones en el sector salud y seguridad social. Tan solo en el año 2025, el Instituto Mexicano del Seguro Social enfrentó múltiples ataques cibernéticos de gran envergadura dirigidos a sus bases de datos, con robo masivo de información de millones de afiliados. En uno de los episodios más graves, se sustrajeron decenas de millones de registros de derechohabientes –incluyendo nombres, CURP, número de seguridad social y datos sensibles de salud–, comprometiendo información de casi la mitad de la población del país. Posteriormente se hizo público que un grupo de atacantes ofreció en mercados clandestinos de la web oscura los datos personales de alrededor de 20 millones de pensionados del IMSS por una suma irrisoria, confirmándose la veracidad de las muestras difundidas.

Aunque la institución negó haber sufrido un “hackeo” tradicional y atribuyó el incidente a una posible filtración interna por uso indebido de credenciales legítimas, lo cierto es que se habría tratado de un acto de traición o colusión desde el interior, igualmente grave que un ataque externo. Más allá de la vulneración a la privacidad, estos hechos exponen a los adultos mayores a delitos subsecuentes: extorsiones, fraudes de identidad, robos patrimoniales y otros ilícitos, al encontrarse sus datos personales a disposición de grupos criminales.

Vulneración de otras entidades y venta clandestina de datos. Los ciberdelincuentes no se han limitado al IMSS. Investigaciones recientes han documentado el compromiso de decenas de millones de registros personales custodiados por instituciones como el Infonavit, los cuales habrían sido ofrecidos ilegalmente en foros clandestinos. Asimismo, se detectó un ataque masivo que extrajo centenares de gigabytes de información de diversas dependencias federales –incluyendo de nueva cuenta datos del sector salud– sin que fuera posible contener o revertir el robo en tiempo real.

A nivel estatal, también se han acreditado intrusiones a sistemas de seguridad pública, como centros de comando (C5) y fiscalías, en las que se habrían exfiltrado bases de datos relacionadas con videovigilancia, investigaciones o reportes ciudadanos. Estos casos

evidencian un patrón sistemático de ataques persistentes y coordinados contra bases de datos gubernamentales en distintos niveles de gobierno.

Filtraciones históricas del padrón electoral y registros de identidad. No es la primera vez que México enfrenta filtraciones masivas de datos poblacionales estratégicos. En 2016, una copia prácticamente completa del padrón electoral del Instituto Nacional Electoral –con información personal de más de 90 millones de votantes– fue encontrada expuesta públicamente en un servidor de almacenamiento en el extranjero, sin contraseña ni cifrado. La base contenía nombres, domicilios, fechas de nacimiento y otros datos confidenciales.

Más preocupante aún fue el hecho de que el propio Instituto no reportó intrusiones externas en sus sistemas, lo cual sugiere que la filtración pudo realizarse desde dentro, por actores con acceso legítimo que extrajeron indebidamente la información. De forma similar, se han documentado intentos de intrusión al Registro Nacional de Población, cuya base central –que genera y administra la CURP– resulta especialmente atractiva para grupos criminales por su valor para suplantaciones de identidad y fraudes. Expertos han advertido que iniciativas recientes, como la creación de una CURP con fotografía y datos biométricos como nueva identificación oficial, incrementan el atractivo del Renapo para los mercados ilícitos y podrían motivar intentos redoblados de ataque contra esa plataforma.

Estos ejemplos demuestran que las bases de datos poblacionales de México ya son objetivo directo de ciberataques y filtraciones, tanto por parte de hackers motivados por lucro como, potencialmente, por grupos de delincuencia organizada e incluso actores extranjeros que buscan explotar nuestra información con fines ilícitos o de desestabilización. La venta ilegal de datos personales en mercados negros se ha convertido en una actividad lucrativa que erosiona la privacidad ciudadana y alimenta otras conductas delictivas. La oferta de millones de registros por montos reducidos evidencia la sobreabundancia de datos robados en circulación, haciendo fácil y barata la obtención de información personal de prácticamente cualquier individuo.

Se trata, en suma, de una amenaza multidimensional: a la seguridad de las personas, a la economía (por fraudes financieros y transaccionales), a la seguridad pública (por extorsiones y violencia asociada) y a la seguridad del Estado, en la medida en que se mina la confianza en las instituciones custodias de datos y se abre la puerta a actos de sabotaje o espionaje masivo.

Los riesgos actuales no son hipotéticos, sino palpables y documentados. Si no se actúa legislativamente, México continuará expuesto a pérdidas irremediables de información sensible, con costos incalculables para la sociedad y el gobierno. Blindar jurídicamente estas bases de datos como infraestructura crítica es una necesidad impostergable para elevar su prioridad de protección.

Por lo expuesto, fundado y motivado, someto a consideración de esta soberanía el siguiente proyecto de

Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley de Seguridad Nacional, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de la Ley Orgánica de la Administración Pública Federal y del Código Penal Federal, en materia de protección de bases de datos poblacionales estratégicas del Estado

Artículo Primero. Se reforman las fracciones XII y XIII y se adiciona una fracción XIV al artículo 5; se adiciona un artículo 6 Bis a la Ley de Seguridad Nacional, para quedar como sigue:

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. Cualquier acto dirigido a destruir, alterar, extraer, copiar, acceder o inutilizar, sin autorización, la información contenida en bases de datos poblacionales estratégicas bajo resguardo del Estado, así como los actos tendentes a facilitar, encubrir o aprovechar dichas conductas. En general, se considerará amenaza a la seguridad nacional todo atentado cibernético, intrusión, divulgación no autorizada o sabotaje que vulnere la integridad, confidencialidad o disponibilidad de las bases de datos poblacionales estratégicas del país.

Artículo 6 Bis.- Las bases de datos poblacionales estratégicas en poder del Estado Mexicano se consideran parte de la infraestructura crítica nacional, por ser indispensables para la seguridad nacional y el interés público. Se entiende por bases de datos poblacionales estratégicas aquellas administradas por autoridades públicas que contienen datos personales de una proporción significativa de la población o datos de identidad de los habitantes, cuya alteración, destrucción, divulgación o uso ilícito podría:

I. Comprometer la seguridad nacional, la seguridad interior o la seguridad pública;

II. Afectar la continuidad de servicios esenciales del Estado o la garantía de derechos fundamentales de la población a gran escala, o

III. Lesionar la gobernabilidad democrática, la integridad de procesos electorales, la estabilidad económica o la confianza ciudadana en las instituciones, mediante el uso indebido de dicha información.

Artículo Segundo. Se adiciona un Capítulo III, denominado “De las Bases de Datos Críticas del Estado”, que contiene los artículos 76 Bis, 76 Ter, 76 Quáter y 76 Quintus, al Título Sexto de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, para quedar como sigue:

Capítulo III
De las Bases de Datos Críticas del Estado

Artículo 76 Bis. Para efectos de esta ley, se considera Base de Datos Crítica del Estado aquella base de datos en posesión de sujetos obligados que, por su naturaleza estratégica o por el volumen o sensibilidad de los datos personales que contiene, resulte indispensable para la continuidad de funciones esenciales del Estado o cuya afectación pudiera comprometer la seguridad nacional, la seguridad pública o causar un daño grave a un amplio conjunto de personas.

En todo caso, tendrán carácter de bases de datos críticas del Estado, entre otras, las bases de datos poblacionales estratégicas determinadas conforme a la Ley de Seguridad Nacional y aquellas que sean calificadas como infraestructura de información crítica mediante lineamientos del Sistema Nacional de Transparencia y del Consejo de Seguridad Nacional.

Artículo 76 Ter. Los responsables de bases de datos críticas del Estado deberán implementar medidas de seguridad reforzadas de nivel alto, superiores a las establecidas con carácter general, a fin de garantizar la integridad, disponibilidad, confidencialidad, autenticidad y resiliencia de la información. Entre dichas medidas, que serán proporcionales a la criticidad de la base de datos, se incluirán al menos:

I. Controles de acceso estrictos y monitoreo continuo, con mecanismos de autenticación robusta y registro permanente de cualquier acceso, consulta, modificación o transferencia de datos;

II. Cifrado criptográfico de los datos personales sensibles o de identificación en reposo y en tránsito, así como medidas de seudonimización o disociación cuando aplique, para minimizar riesgos en caso de filtración;

III. Planes periódicos de evaluación de vulnerabilidades y pruebas de penetración en los sistemas informáticos que soportan la base de datos, para detectar y subsanar oportunamente posibles brechas de seguridad;

IV. Protocolos de respuesta a incidentes de seguridad orientados a contener, mitigar y notificar cualquier vulneración de la seguridad de los datos personales. En caso de detectarse acceso no autorizado o pérdida/alteración de información en una base de datos crítica, el responsable deberá notificar de inmediato al órgano garante competente en materia de protección de datos personales y al Consejo de Seguridad Nacional, para la coordinación de acciones de contención y las investigaciones conducentes, y

V. Auditorías de seguridad y cumplimiento normativo al menos una vez al año a cargo del órgano interno de control o unidad equivalente, con participación, en su caso, de la autoridad garante en materia de datos personales, para verificar la eficacia de las medidas implementadas y formular recomendaciones. Los resultados de estas auditorías serán documentados y, tratándose de bases de datos poblacionales estratégicas, podrán ser clasificados como información reservada por seguridad nacional, conforme a la Ley General de Transparencia, siempre que su publicidad ponga en riesgo la protección de los datos o la seguridad de los sistemas.

Artículo 76 Quáter. Las instituciones responsables de bases de datos críticas del Estado deberán designar, en el ámbito de su Comité de Transparencia u órgano colegiado equivalente, a un Enlace de Seguridad de la Información encargado de supervisar el debido cumplimiento de las medidas de protección reforzadas. Este Enlace de Seguridad deberá ser un servidor público de nivel directivo con conocimientos especializados en seguridad de la información y protección de datos personales, cuyas funciones incluirán:

I. Coordinar la elaboración e implementación del Documento de Seguridad específico para la base de datos crítica, detallando políticas, procedimientos y controles particulares;

II. Fungir como punto de contacto institucional con la Agencia de Transformación Digital y Telecomunicaciones, con el Consejo de Seguridad Nacional y con el órgano garante de transparencia, para la atención de recomendaciones, lineamientos técnicos y eventuales incidentes relacionados con la base de datos crítica, y

III. Promover la capacitación continua del personal que maneja la base de datos crítica, en temas de seguridad de la información, ciberseguridad y manejo ético de los datos, estableciendo controles de confianza cuando la naturaleza de la información lo amerite.

Artículo 76 Quintus. El régimen de transparencia y acceso a la información aplicable a las bases de datos críticas del Estado deberá observar un equilibrio entre la máxima publicidad y la salvaguarda de la seguridad nacional y la privacidad. En ese sentido:

I. La existencia, finalidad y marco normativo de cada base de datos crítica del Estado serán públicos. Los sujetos obligados deberán publicar en sus sitios electrónicos y en la Plataforma Nacional de Transparencia descripciones generales de dichas bases de datos, incluyendo su denominación, propósito, categoría de información que contienen y medidas básicas de protección implementadas, siempre que dicha información general no comprometa la seguridad de la base de datos.

II. Se considerará información reservada por motivos de seguridad nacional aquella que detalle la arquitectura de seguridad, los controles específicos, claves de cifrado, configuraciones técnicas o vulnerabilidades identificadas de la base de datos crítica, cuya divulgación pudiera facilitar riesgos o ataques. Asimismo, podrá reservarse la

información cuyo acceso irrestricto pueda ser utilizado para fines que pongan en peligro la seguridad de las personas (por ejemplo, listados completos de población con datos personales). Estas reservas se harán conforme a los criterios y procedimientos de la Ley General de Transparencia y Acceso a la Información Pública, sujetas a prueba de daño y ponderación caso por caso.

III. La información de carácter personal contenida en bases de datos críticas del Estado se regirá por lo dispuesto en la presente Ley y demás normas de protección de datos personales. En cualquier solicitud de acceso a datos personales contenida en dichas bases, el sujeto obligado deberá extremar precauciones para verificar la identidad y legitimidad del solicitante, aplicando controles adicionales si es necesario, en virtud de la criticidad de los datos solicitados.

IV. En caso de que alguna base de datos crítica contenga información no personal de interés público (por ejemplo, estadísticas agregadas, indicadores no confidenciales), se procurará ponerla a disposición en formatos de datos abiertos, con periodicidad y nivel de agregación que no comprometan la seguridad ni revelen datos protegidos. La publicación proactiva de información derivada de bases de datos críticas deberá ser aprobada por el Comité de Transparencia respectivo, siguiendo la asesoría del Enlace de Seguridad de la Información y atendiendo a las recomendaciones del órgano garante.

Artículo Tercero. Se adiciona una nueva fracción VI al artículo 42 Ter de la Ley Orgánica de la Administración Pública Federal, recorriéndose la actual en el orden subsecuente, para quedar como sigue:

Artículo 42 Ter.- A la Agencia de Transformación Digital y Telecomunicaciones le corresponde el despacho de los siguientes asuntos:

I. a V. ...

VI. **Coordinar, con las dependencias y entidades de la administración pública federal que sean responsables de bases de datos críticas del Estado, las acciones orientadas a la protección, estandarización e interoperabilidad de dichas bases de datos. En ejercicio de esta atribución, la Agencia deberá emitir lineamientos y criterios técnicos para asegurar un nivel homogéneo y óptimo de seguridad informática en la administración de las bases de datos críticas, fomentando la adopción de mejores prácticas en ciberseguridad, respaldo de información, recuperación ante desastres y continuidad operativa. Asimismo, la Agencia impulsará la interoperabilidad regulada entre bases de datos críticas y otros sistemas gubernamentales, con el fin de aprovechar sinergias tecnológicas y evitar duplicidades, todo ello sin comprometer la confidencialidad de los datos ni vulnerar las disposiciones de protección de datos personales. La Agencia actuará en estrecha coordinación técnica con las dependencias titulares de cada base de datos crítica, brindándoles asesoría y apoyo en materia de innovación tecnológica y protocolos de seguridad, y coadyuvará con las**

autoridades competentes en seguridad nacional y protección de datos para garantizar el cumplimiento integral de los lineamientos de este ámbito.

VII. Definir los protocolos de seguridad de la información y comunicaciones de la administración pública federal;

...

...

...

Artículo Cuarto. Se adiciona un Capítulo III, denominado "Delitos en Materia de Bases de Datos Críticas del Estado", que contiene los artículos 211 Bis 8, 211 Bis 9, 211 Bis 10, 211 Bis 11 y 211 Bis 12, al Título Noveno del Libro Segundo del Código Penal Federal, para quedar como sigue:

Capítulo III
Delitos en Materia de Bases de Datos Críticas del Estado

Artículo 211 Bis 8. Comete el delito de acceso ilícito a una base de datos crítica del Estado quien, sin autorización y mediante cualquier medio, acceda a una base de datos crítica del Estado, u obtenga, copie, extraiga, interfiera o altere total o parcialmente los datos personales contenidos en la misma, o los sistemas o equipos que la soportan.

I. Si el agente modifica, daña, borra, destruye o inutiliza información contenida en la base de datos crítica, o provoca la interrupción de su funcionamiento, se le impondrán de cinco a quince años de prisión y multa de quinientos a mil quinientos días.

II. Si el agente accede, conoce, descarga o copia información de la base de datos crítica sin causar daños o alteraciones a los sistemas, se le impondrán de tres a diez años de prisión y multa de trescientos a ochocientos días.

Artículo 211 Bis 9. Comete el delito de comercialización indebida de datos personales de una base de datos crítica del Estado quien, sin estar autorizado para ello, transfiera, venda, ceda, distribuya o divulgue a un tercero datos personales que formen parte de una base de datos crítica del Estado, con ánimo de lucro o beneficio propio o de un tercero, o con el objetivo de causar un perjuicio. A quien incurra en esta conducta se le impondrán de cuatro a doce años de prisión y de cuatrocientos a mil días multa.

Artículo 211 Bis 10. Comete el delito de manejo ilícito de datos en bases de datos críticas del Estado por parte de personal autorizado aquel servidor público, funcionario, empleado o contratista que, estando autorizado para acceder o administrar una base de datos crítica del Estado en razón de su empleo o función, incumpla deliberadamente sus deberes de custodia o exceda los permisos otorgados con cualquiera de las

finalidades siguientes: obtener, usar, sustraer, divulgar, alterar, falsificar o suprimir datos personales contenidos en la base de datos, fuera de los casos permitidos por la ley y sin consentimiento de la autoridad competente o de los titulares de los datos cuando se requiera.

I. Si la persona autorizada alterare, falsificare, destruyere, dañare o suprimiere datos de la base de datos crítica, o provocare la interrupción no autorizada de su operación, se le impondrán de tres a ocho años de prisión y de trescientos a novecientos días multa.

II. Si la persona autorizada obtiene, copia, extrae, divulga o transmite a terceros información contenida en la base de datos crítica, sin estar facultada para ello y al margen de los fines institucionales, se le impondrán de dos a seis años de prisión y de doscientos a seiscientos días multa.

Además de las sanciones anteriores, al responsable de este delito que ostente la calidad de servidor público se le impondrá la destitución del cargo y la inhabilitación para ocupar cualquier empleo, cargo o comisión en el servicio público por un plazo de cinco a diez años, según la gravedad de la conducta. En todos los casos del presente artículo, se entenderá que el autor actuó deliberadamente cuando conocía las restricciones legales sobre el uso de la información y aun así actuó en contravención de éstas con intención de beneficio propio o ajeno, o para causar daño o ventaja indebida.

Artículo 211 Bis 11. Comete el delito de omisión o negligencia grave en el manejo de bases de datos críticas del Estado el servidor público o encargado que, por falta de cuidado, inobservancia de sus deberes, incumplimiento de protocolos de seguridad o negligencia inexcusable, permita u origine con su conducta que personas no autorizadas accedan, obtengan, extraigan, alteren o difundan total o parcialmente los datos personales contenidos en una base de datos crítica del Estado, siempre que dicha conducta genere un riesgo efectivo o un daño a la seguridad de la información o a los derechos de los titulares de los datos.

A quien incurra en esta conducta se le impondrán de dos a siete años de prisión y de doscientos a quinientos días multa. Tratándose de un servidor público, se le impondrá además la destitución e inhabilitación para cargo público hasta por cinco años.

Artículo 211 Bis 12. Agravantes especiales. Las penas previstas en este Capítulo se aumentarán hasta en una mitad cuando concurra cualquiera de las siguientes circunstancias en la comisión de los delitos:

I. Cuando la información personal obtenida, revelada o utilizada indebidamente sea empleada con fines de lucro, ventaja económica o beneficio político para el autor del delito o terceros, o bien fuere difundida masivamente.

II. Cuando la conducta ilícita cause un perjuicio grave a la seguridad nacional, a la seguridad pública o a la defensa del Estado, ya sea porque los datos obtenidos se

utilicen para cometer otros delitos de alto impacto (espionaje, terrorismo, extorsión masiva, etc.) o porque comprometan operaciones, planes o personal relacionado con la seguridad nacional.

III. Cuando el delito fuere cometido por un servidor público perteneciente a alguna institución de seguridad nacional, seguridad pública, procuración de justicia o fuerzas armadas, aprovechando los conocimientos, accesos o facilidades propios de su cargo.

Transitorio

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

Dado en el Palacio Legislativo de San Lázaro, sede de la Comisión Permanente del Congreso de la Unión, a 21 de enero de 2026.

Diputado Felipe Miguel Delgado Carrillo (rúbrica)