INICIATIVA CON PROYECTO DE DECRETO QUE REFORMA Y ADICIONA DIVERSAS DISPOSICIONES A LA LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES, EN MATERIA DE SEGURIDAD DE DATOS PERSONALES, PRESENTADA POR EL SENADOR JOSÉ ALBERTO GALARZA VILLASEÑOR DEL GRUPO PARLAMENTARIO DE MOVIMIENTO CIUDADANO.

El suscrito, José Alberto Galarza Villaseñor, Senador del Grupo Parlamentario de Movimiento Ciudadano, de la LXIV Legislatura del H. Congreso de la Unión, con fundamento en el artículo 71, fracción II de la Constitución Política de los Estados Unidos Mexicanos, y el artículo 8, fracción I del Reglamento del Senado de la República, someto a consideración la siguiente: **Iniciativa con Proyecto de Decreto que reforma y adiciona diversas disposiciones a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, en materia de seguridad de datos personales.**

EXPOSICIÓN DE MOTIVOS

I. De acuerdo con el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, los datos personales son cualquier información que refiera a una persona física que pueda ser identificada a través de los mismos, los cuales se pueden expresar en forma numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo, como: nombre, apellidos, CURP, estado civil, lugar y fecha de nacimiento, domicilio, número telefónico, correo electrónico, grado de estudios, sueldo, entre otros.

Es importante señalar que dentro de los datos personales hay una categoría que se denomina “datos personales sensibles”, que requieren especial protección, ya que refieren a información que pueda revelar aspectos íntimos de una persona o dar lugar a discriminación, como el estado de salud, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, origen racial o étnico y preferencia sexual, por mencionar algunos.

En este sentido, los dueños de los datos personales son las personas a las que corresponden o refieren estos datos, derivado de la importancia de esta información personal, en México la protección de los datos personales es un derecho que se encuentra reconocido a nivel constitucional por el párrafo segundo del artículo 16 de nuestra Carta Magna que prevé lo siguiente:

> *"**Toda persona tiene derecho a la protección de sus datos personales,** al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceros."*

Como medida legislativa para el fortalecimiento de dicho derecho, el 30 de abril de 2009 se publicó en el Diario Oficial de la Federación el decreto por el que se adiciona la fracción XXIX-O al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, que establece la facultad del Congreso de la Unión para legislar en materia de protección de datos personales en posesión de particulares.

En cumplimiento a esta obligación, el Congreso de la Unión aprobó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, misma que fue publicada el 5 de julio de 2010 en el Diario Oficial de la Federación, el objeto de esta ley es la de regular el tratamiento legítimo, controlado e informado de los datos personales que estén en manos de particulares, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas.

Ahora bien, en el ámbito internacional la Declaración Universal de los Derechos Humanos en su artículo 12 dispone que *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, domicilio o su correspondencia, ni ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".* Asimismo, el artículo 17 del Pacto Internacional sobre Derechos Civiles y Políticos establece en los mismos términos

dicha protección. En el mismo sentido, la Convención Americana de Derechos Humanos en los incisos 2 y 3 del artículo 11, refieren al derecho a la vida privada.

II. Un elemento clave de cualquier política en materia de seguridad de los datos personales es poder, en la medida de lo posible, prevenir una vulneración a la seguridad de los datos personales y, cuando a pesar de todo se produzca, reaccionar de forma rápida a estos eventos indeseados e inesperados, en especial, dada la evolución tecnológica en la que se ven envueltos los tratamientos de datos personales actualmente.

De acuerdo con lo dispuesto por el artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, *"Todo responsable que lleve a cabo tratamiento de datos personales deberá establecer y mantener medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado".*

En esta tesitura, el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, establece en el artículo 2, lo siguiente:

> *"V. Medidas de seguridad administrativas: Conjunto de acciones y mecanismos para establecer la gestión, soporte y revisión de la seguridad de la información a nivel organizacional, la identificación y clasificación de la información, así como la concienciación, formación y capacitación del personal, en materia de protección de datos personales;*
>
> *VI. Medidas de seguridad físicas: Conjunto de acciones y mecanismos, ya sea que empleen o no la tecnología, destinados para:*
>
> *a) Prevenir el acceso no autorizado, el daño o interferencia a las instalaciones físicas, áreas críticas de la organización, equipo e información;*

b) Proteger los equipos móviles, portátiles o de fácil remoción, situados dentro o fuera de las instalaciones;

c) Proveer a los equipos que contienen o almacenan datos personales de un mantenimiento que asegure su disponibilidad, funcionalidad e integridad, y

d) Garantizar la eliminación de datos de forma segura;

VII. Medidas de seguridad técnicas: Conjunto de actividades, controles o mecanismos con resultado medible, que se valen de la tecnología para asegurar que:

a) El acceso a las bases de datos lógicas o a la información en formato lógico sea por usuarios identificados y autorizados;

b) El acceso referido en el inciso anterior sea únicamente para que el usuario lleve a cabo las actividades que requiere con motivo de sus funciones;

c) Se incluyan acciones para la adquisición¸ operación, desarrollo y mantenimiento de sistemas seguros, y

d) Se lleve a cabo la gestión de comunicaciones y operaciones de los recursos informáticos que se utilicen en el tratamiento de datos personales;

Asimismo, el Capítulo III de dicho reglamento define de manera general los factores que los responsables y encargados deberán tomar en cuenta para el tratamiento de datos personales con el propósito de determinar las medidas de seguridad a implementar para la protección de los mismos, así como las acciones que deberán llevar a cabo los responsables y encargados para la implementación de las medidas de seguridad.

No obstante que la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su reglamento establecen las medidas de protección de los datos personales y su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la

autodeterminación informativa de las personas, es importante mencionar que existen riesgos de vulneración de las medidas de seguridad, en este contexto el artículo 63 de su reglamento, determina los supuestos de vulneración de los datos personales, a saber:

- Pérdida o destrucción no autorizada;
- Robo, extravío o copia no autorizada;
- Uso, acceso o tratamiento no autorizado, o
- Daño, alteración o modificación no autorizada.

Ahora bien, cuando los datos personales sean objeto de alguno de los supuestos arriba señalados, el responsable tiene la obligación de notificar al titular lo sucedido, de acuerdo con lo establecido por el artículo 20 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y 64 de su reglamento, para que el titular pueda tomar medidas para la protección de sus derechos morales y patrimoniales, sin considerar alguna notificación al respecto al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. A diferencia del caso del sector público, donde los sujetos obligados tiene el deber de notificar las vulneraciones a las medidas de seguridad a dicho Instituto o al organismo garante de la entidad federativa que corresponda, conforme a lo dispuesto por los artículos 40 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados y 66, 67, 68 y 69 de los Lineamientos Generales de Protección de Datos Personales para el Sector Público.

III. En el ámbito internacional, existen normas como el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de directa aplicación en toda Europa, relativo a la protección de las personas físicas respecto al tratamiento de datos personales y a la libre circulación de estos datos, que estableció en el artículo 85, la obligación específica a todos los responsables del tratamiento para que de ser posible, a más tardar 72 horas, notifiquen las violaciones de la seguridad de los datos personales a la autoridad de control nacional competente y, en determinados casos, como lo señala el artículo 86, se comunique a las personas cuyos datos personales se hayan visto afectados por la violación.

Para mayor claridad, de lo anterior se transcriben textualmente los artículos antes referidos:

> 85. *Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida.*
>
> 86. *El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las*

autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continuas o similares.

Sobre el particular, el entonces Grupo de Trabajo del Artículo 29 de la Unión Europea señaló que este nuevo requisito de notificación tiene como ventaja que, a la hora de notificar a la autoridad de control, los responsables del tratamiento pueden obtener asesoramiento sobre la necesidad de informar a las personas afectadas; asimismo, la comunicación de una violación a las personas permite que el responsable proporcione información sobre los riesgos que se presentan como resultado de la violación y las medidas que dichas personas pueden adoptar para protegerse de sus posibles consecuencias. Por consiguiente, la notificación de las violaciones de la seguridad debe considerarse como una herramienta que mejora el cumplimiento respecto de la protección de los datos personales.

Por otra parte, el 25 de agosto de 2017, el Embajador Santiago Oñate, titular de la representación de México ante el Consejo de Europa, entregó al Secretariado del Consejo de Europa la solicitud del Estado mexicano para adherirse al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y a su Protocolo Adicional relativo a las autoridades de control y a los flujos transfronterizos de datos personales. La solicitud estaba acompañada de una serie de documentos que confirmaban la compatibilidad de la legislación mexicana en materia de protección de datos personales con el contenido del Convenio 108 y de su Protocolo Adicional.

Posteriormente, el 16 de octubre, el Comité Consultivo de dicho Convenio aprobó por unanimidad la Opinión sobre la adhesión de México al instrumento internacional y concluyó que la legislación mexicana de protección de datos personales cumplía de manera general con los principios del Convenio 108 y de su Protocolo Adicional. En ese sentido, opinó que a la solicitud correspondiente se le debía dar una respuesta favorable.

Si bien, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento cumple con los establecido con el artículo 7 del Convenio 108, es necesario señalar que, en dicha opinión se comentó que la Ley Federal y en consecuencia su reglamento no establecen la notificación de violación de datos personales ante la autoridad de control.

Respecto al Protocolo que moderniza el Convenio para la protección de las personas en materia de procesamiento automático de datos personales, conocido como Convenio 108+, el cual persigue hacer frente a los retos derivados de la utilización de las nuevas tecnologías de la información y la comunicación, como parte de sus puntos de innovación, en su artículo 7 relativo a la seguridad de las datos, adicionó un párrafo segundo para establecer la obligación para el responsable de notificar a las autoridades de control, aquellas vulneraciones de datos que puedan interferir gravemente con los derechos y las libertades fundamentales de los titulares de datos.

Es importante mencionar, que el 19 de junio de 2018 que dicho instrumento de adhesión fue firmado por el entonces titular del Ejecutivo Federal y posteriormente aprobado por la Cámara de Senadores, el 26 de abril de 2018, según el decreto publicado en el Diario Oficial de la Federación el 12 de junio de 2018.

Bajo este precedente, el 28 de septiembre de 2018, se publicó en el Diario Oficial de la Federación el *"DECRETO Promulgatorio del Protocolo Adicional al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, a las Autoridades de Control y a los Flujos Transfronterizos de Datos, hecho en Estrasburgo, Francia, el ocho de noviembre de dos mil uno"* entrando en vigor al día siguiente de su publicación.

A partir de lo anterior, indispensable considerar la homologación de este Convenio con la legislación nacional, para que la notificación de vulneraciones sea un requisito establecido para el sector privado en lo correspondiente informar al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, como autoridad garante de la protección de datos personales.

IV. En tal virtud, para lograr una efectiva protección de datos, más allá del andamiaje jurídico vigente, resulta necesario incorporar una serie de disposiciones que coadyuven a garantizar la privacidad y seguridad de los datos personales por parte de los responsables respecto de su tratamiento.

En el caso de las vulneraciones de datos personales, es imprescindible que el responsable del tratamiento de la información, en un plazo no mayor a 72 horas, notifique al titular, así como al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, con el propósito de que la persona afectada pueda minimizar lo antes posible el impacto de las vulneraciones tomando las medidas necesarias como: cambio de contraseñas, de número de cuenta, cancelación de tarjetas de crédito o débito, entre otros, para evitar daños, reales o significativos en su patrimonio, seguridad, libertad o vida.

Obligar al responsable a notificar las vulneraciones al Instituto es brindarle la oportunidad al titular de la información la posibilidad de adoptar conjuntamente con este Órgano garante las medidas oportunas para proteger a las personas de peligros reales y latentes.

Sin duda, con la presente iniciativa estaremos promoviendo una mayor rendición de cuentas en el sector privado y fortaleciendo la gestión de vulneraciones de datos personales, mejorando las condiciones para la defensa y protección de los derechos a la privacidad y datos personales de las personas, y estaremos acorde con los más altos estándares internacionales en la materia.

Por último, la presente iniciativa con proyecto de decreto se elaboró a partir del diálogo, propuestas y trabajo realizado entre la Presidenta, Consejeros y un equipo de trabajo de la Secretaría de Protección de Datos Personales del Instituto Nacional de Acceso a la Información, con el suscrito, ya que una de las principales actividades que he realizado como Senador, es escuchar a los organismos constitucionalmente autónomos y retomar su experiencia construida por medio del trabajo que realizan día con día, con el objetivo de fortalecer la legislación que les da su razón de ser.

Por lo anteriormente expuesto, se somete a la consideración el siguiente:

DECRETO

ÚNICO. Se reforma el artículo 20 y, se adiciona un párrafo segundo y tercero, al artículo 20, un artículo 20 Bis y 20 Ter, a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, para quedar como sigue:

Artículo 20.- El responsable deberá informar sin dilación alguna al titular y al Instituto, en un plazo no mayor de setenta y dos horas, las vulneraciones que afecten de forma significativa los derechos patrimoniales o morales de los titulares, **en cuanto se confirme que ocurrió la vulneración y que el responsable haya empezado a tomar las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, a fin de que los titulares afectados** puedan tomar las medidas correspondientes para la defensa de sus derechos.

El Instituto y el titular podrán coadyuvar con el responsable para mitigar o eliminar, el impacto o magnitud de la afectación, siempre y cuando a consideración del Instituto esto resulte posible en función al tipo de vulneración.

Existirá una afectación significativa, cuando con independencia del impacto o la magnitud de la vulneración o del daño que se hubiere producido, la esfera de derechos del titular en cuanto al patrimonio, la seguridad, la libertad o la vida puedan quedar comprometidos de no iniciar acciones correctivas o reparadoras.

Artículo 20 Bis.- Se entenderá que se afectan los derechos patrimoniales del titular cuando la vulneración esté relaciona, con lo siguiente:

I. Bienes muebles e inmuebles;
II. Información fiscal;
III. Historial crediticio;
IV. Ingresos o egresos;
V. Cuentas bancarias;
VI. Seguros, afores o fianzas;

VII. **Servicios contratados;**
VIII. **Cantidades o porcentajes relacionados con la situación económica del titular, o**
IX. **Cualquier otra que pudiera afectar sus derechos patrimoniales.**

Artículo 20 Ter.- Se entenderá que se afectan los derechos morales del titular cuando la vulneración esté relaciona, con lo siguiente:

I. **Sentimientos o afectos;**
II. **Creencias;**
III. **Honor, reputación o decoro;**
IV. **Vida privada;**
V. **Configuración y aspecto físicos;**
VI. **Consideración que de sí mismo tienen los demás;**
VII. **Cuando se menoscabe ilegítimamente la libertad;**
VIII. **Cuando se menoscabe la integridad física o psíquica, o**
IX. **Cualquier otra que pudiera afectar sus derechos morales.**

PRIMERO. El Presente Decreto entrará en vigor al día siguiente de su publicación.

SEGUNDO. Dentro de un plazo de noventa días a partir de la entrada en vigor de este Decreto, el Ejecutivo Federal publicará las modificaciones reglamentarias que correspondan.

A T E N T A M E N T E,

Sen. José Alberto Galarza Villaseñor

Grupo Parlamentario de Movimiento Ciudadano

Senado de la República

LXIV Legislatura

Abril de 2021