EL SENADO Y CÁMARA DE DIPUTADOS
DE LA NACIÓN ARGENTINA, REUNIDOS EN CONGRESO…
SANCIONAN CON FUERZA DE
LEY:

NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD. MODIFICACION DEL ARTICULO 9 DE LA LEY 25326 - PROTECCIÓN DE DATOS PERSONALES

ARTÍCULO 1 ° .- Sustitúyase el Artículo 9° de la Ley 25.326 por el siguiente:

1. El responsable del tratamiento de datos personales o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

En caso de que ocurra un incidente que viole la seguridad de los datos personales, el responsable del tratamiento deberá notificarlo sin dilación y de ser posible dentro de las setenta y dos (72) horas desde de que haya tomado conocimiento del mismo a la Autoridad de Control correspondiente y al titular de los datos, a menos que sea improbable que dicha violación de seguridad constituya un riesgo para los derechos de los titulares de datos.

De igual manera, el responsable del tratamiento deberá realizar la Denuncia Penal respectiva en la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), Juzgado Federal, Fiscalía o Dependencia Policial correspondiente.

Si la notificación a la autoridad de Control no tiene lugar en el plazo de setenta y dos (72) horas, podrá extenderse dicho plazo hasta diez (10) días siempre que se acrediten los motivos justificados de la dilación .

La notificación y denuncia contempladas en los párrafos anteriores deberán contener, al menos, la siguiente información: a) la naturaleza del incidente, b) la categoría de datos

personales comprometidos, c) identificación de titulares afectados, d) posibles consecuencias del incidente, e) medidas adoptadas para remediarlo y en su caso para mitigar los posibles efectos negativos, f) medidas correctivas aplicadas para evitar futuros incidentes, g) recomendaciones al titular de los datos acerca de las medidas que este pueda adoptar para
proteger sus intereses, h) Los medios a disposición del titular de los datos para obtener mayor información al respecto.

El responsable del tratamiento deberádocumentar todo incidente de la seguridad de los datos personales, identificando, de manera enunciativa pero no limitativa, la fecha en que ocurrió, el motivo, los hechos relacionados con él y sus efectos, y las medidas correctivas implementadas de forma inmediata y definitiva.

2. Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

ARTÍCULO 2°. - Comuníquese al Poder Ejecutivo.

Firmante: **Gabriela BESANA**

FUNDAMENTOS

Señor presidente:

Es de público conocimiento que en octubre del año pasado la base de datos del Registro Nacional de las Personas (RENAPER), que contiene datos privados de todos los habitantes del país, fue accedida y filtrados los datos en foros de seguridad informática, redes sociales y puestos a la venta on line.

Estos hechos de extrema gravedad, nos obligan a repensar en la necesidad no sólo de reforzar los mecanismos de seguridad informática en el tratamiento de los datos personales, sino también en la notificación inmediata de estos incidentes para mitigar el daño que pueden producir.

Según informó el Renaper se detectó el ingreso de un usuario del SISA (Sistema Integrado de Información Sanitaria Argentino) quien luego publicó en la red social Twitter, fotos y los datos que figuran en el DNI (Documento Nacional de Identidad) de al menos 44 funcionarios y personajes públicos.

Este incidente podría afectar a los 45 millones de habitantes de la nación, ya que se filtró no sólo el número de documento, sino también la foto, nombre, apellido, fecha de nacimiento, dirección, número de trámite de DNI. Esto, ataca no sólo su privacidad sino que a su vez, los deja indefensos ante robos de identidad ya que el número de trámite de DNI se exige para trámites sensibles dentro de los que se incluye trámites a distancia en ANSES, app CUIDAR y el otorgamiento de créditos on line.

Podemos recordar otros incidentes similares, como aquellos ocurridos en AFIP donde funcionarios y empleados del propio organismo robaron información sensible como , los datos del último blanqueo de capitales. También, el incidente en donde se vendieron datos sobrepotenciales clientes a través de una empresa llamada Reporte On Line y que fuera denunciado por el organismo en febrero de 2018. Por su parte, en agosto de 2019 el ataque a los servidores de la Policía Federal –"La Gorra Leaks"– puso en jaque a toda la administración nacional.

También se filtraron datos de la Dirección Nacional de Migraciones entre los que figuran datos personales de 25.723 ciudadanos argentinos, como el archivo que tiene el nombre "Repatriados.csv" y que reúne nombre, apellido, fecha de nacimiento, teléfonos particulares o números de celulares, direcciones, procedencia y puerto de ingreso al país de quienes volvieron en plena pandemia entre abril y mayo de 2020.

Todos estos casos, son ejemplos de datos sensibles de las personas en poder del Estado que se filtraron supuestamente por los propios empleados, lo que requiere que no solamente se obligue siempre a informar estos incidentes a los titulares de los datos sino también a

informar qué medidas se toman para mitigar los daños y para evitar hechos similares en el futuro.

Esto incidentes no sólo ocurren en organismos públicos sino también en empresas privadas, por cuanto quienes tratan datos personales a escala son los principales objetivos de ataques por parte de los delincuentes, quienes vulneran la seguridad de los datos, comprometiendo información confidencial en busca de obtener beneficios, en la mayoría económicos, con su venta.

El escándalo más conocido a nivel internacional por la venta de datos de redes sociales sucedió entre 2016 y 2018 donde a Facebook se le acusó de haber compartido de manera inapropiada los datos de millones de sus usuarios con la consultora política británica, Cambridge Analytica, generando reclamos acerca del posible uso de esos datos para influenciar los resultados de las elecciones presidenciales de 2016 en EE. UU. y del referendo del brexit en Reino Unido, llevado a cabo ese mismo año.

También puede recordarse la filtración de más de 500 millones de números telefónicos en Telegram ocurrida en 2020 o a nivel nacional el ataque al sistema informático de la empresa Cencosud en noviembre de 2020 donde , producto de este incidente de seguridad ocasionado por un malware y phishing se filtraron datos personales y de tarjetas de créditos de los clientes.

A ello se agrega que, con motivo del aislamiento social dictado por la pandemia de coronavirus, se produjo un acelerado avance hacia la digitalización y procesos remotos en casi todos los ámbitos, principalmente comercio y laboral, proceso que requiere estar acompañado de estrategia adecuadas de ciberseguridad.

A tal fin es que consideramos fundamental que en caso de producirse estos incidentes de seguridad de datos personales los mismos deban ser notificados inmediatamente, no sólo para tener conocimiento del tratamiento no autorizado de datos sino también a fin de que se puedan tomar las medidas que fueren necesarias para minimizar y mitigar el daño que estos incidentes pueden producir a sus titulares, como por ejemplo la filtración de datos de tarjetas de crédito o de filtración de claves.

Con la reforma propuesta, buscamos fortalecer y brindar a nuestro país un régimen legal adecuado que respete los derechos y garantías establecidos por nuestra Constitución Nacional y que, paralelamente, se adapte a las nuevas tecnologías y cambios regulatorios ocurridos en el derecho comparado durante los últimos años.

La evolución de la tecnología en los últimos veinte (20) años, si bien ha producido

beneficios innegables, ha impactado de forma negativa en la protección de los datos personales con el surgimiento de nuevas modalidades delictivas y vulneraciones a la

privacidad y confidencialidad.

Es importante resaltar que existe un nuevo contexto internacional en la materia que se encuentra en constante evolución y adaptación, tal es el caso de las nuevas regulaciones en Europa con la reciente aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo que ha entrado en vigencia en mayo de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

La República Argentina desde el año 2003 es considerada por la Unión Europea como un país con legislación adecuada para la protección de los datos personales (Comisión de las Comunidades Europeas - Decisión de la Comisión C (2003)1731 de fecha 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina).

Sin embargo, advertimos que el estatus de país adecuado está siendo actualmente evaluado por la Comisión Europea a la luz de la entrada en vigencia del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, motivo por el cual se propone la presente reforma con la finalidad de mantener los estándares internacionales, lo cual traerá consigo nuevas posibilidades de innovación, protección e inversión en nuestro país.

Somos conscientes de la necesidad de una modificación integral de la ley de Protección de Datos personales a fin de actualizar la normativa de protección de datos personales conforme los estándares internacionales vigentes y las nuevas tecnologías, sin embargo, este proceso llevará tiempo y en el ínterin siguen produciéndose este tipo de incidentes que vulneran los derechos del honor e intimidad de los titulares de esos datos y los pone en riesgo.

Es por ello que el presente proyecto propone incluir en forma urgente en la legislación actual, sancionada hace más de veinte años, esto es la ley 25.326 de Protección de Datos personales, la obligación del responsable del tratamiento de denunciar estos incidentes tanto a las autoridades como a los titulares de datos afectados, concretamente incorporándose en el artículo 9° de la referida ley, actualizando y adecuando de esta forma dicha norma a los avances tecnológicos producidos y a la legislación internacional existente.

Esta obligación de notificación ya se encuentra receptada por las legislaciones más modernas como la Europea, Australia, Canadá, México, Nueva Zelanda y Estados Unidos, entre otras.

Al respecto el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos contempla esta obligación de notificar la

ocurrencia de un incidente de seguridad en su art. 33 donde se establece: *"Notificación de una violación de la seguridad de los datos personales a la autoridad de control.*
1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificara, a la autoridad de control competente de conformidad con el articulo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificara, sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.
3. La notificación contemplada en el apartado 1 deberá, como mínimo: a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitara, de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentara, cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo."

Por su parte el Comité Europeo de Protección de Datos publicó su versión final de la Guía 1/2021 sobre notificación de incidentes de seguridad, en la cual través de 18 casos que sirven como ejemplos ilustrativos, determina cuándo notificar un incidente de seguridad a la autoridad de aplicación y/o a los titulares de los datos afectados por este. Además, recomienda una serie de medidas que adoptar en caso de sufrir algún incidente de seguridad de iguales o similares características a la de los casos presentados como ejemplo.

En nuestro país, encontramos tipificadas algunas conductas relacionadas al

tratamiento de datos personales en el Código Penal como acceder de cualquier forma a un banco de datos personales a sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos; proporcionar o revelar ilegítimamente a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar; insertar o hacer insertar ilegítimamente datos en un archivo de datos personales; acceder por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informativo de acceso restringido, y se pena con prisión a quienes cometan estos delitos agravándose la pena cuando el acceso fuere en perjuicio de un sistema o dato informático de un organismo estatal o de un proveedor de servicios públicos o de servicios financieros (arts. 153 bis y 157 bis).

Asimismo, los responsables por el tratamiento de datos personales objeto de la actividad delictiva también pueden tener consecuencias bajo el régimen de protección de datos personales, por cuanto en el artículo 9 de la Ley de Protección de datos se establece el deber de éstos de garantizar medidas de seguridad de datos a fin de evitar la adulteración, pérdida, consulta o tratamiento no autorizado de los datos personales, estando expresamente prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad y seguridad.

La Agencia de Acceso a la Información Pública **(**AAIP**),** como autoridad de Aplicación a través de su Resolución 47/2008 (Guía de Medidas de Seguridad Recomendadas en Medios Informatizados) reguló las medidas de seguridad mínimas esperadas en el tratamiento de datos personales y en sus dictámenes y resoluciones recomienda notificar estos incidentes a la autoridades de aplicación (Resolución 47/2018) y a los titulares de datos (Resolución 332/2020).

Sin embargo, no existe en la actualidad ninguna ley que establezca la obligación de notificar estos incidentes de seguridad de datos, tanto a la Autoridad de Aplicación como a los titulares de los datos.

Es por ello que la presente iniciativa propone incluir en el art. 9 de la ley 25.326, que establece el deber de seguridad expresamente, esta obligación de notificar los incidentes de seguridad de datos que se produzcan.

Cabe mencionar que se tomaron de base antecedentes como el Proyecto de Ley de Protección de Datos Personales que el Poder Ejecutivo Nacional envió al Honorable Congreso de la Nación en septiembre de 2018 por Mensaje MEN-2018-147-APN-PTE (art 20), el anteproyecto de Ley de Protección de Datos Personales" publicado en el sitio web oficial de la Agencia de Acceso a la Información Pública e incluso lo dispuesto en la Resolución AAIP 47/2018.

A diferencia del Reglamento Europeo el presente proyecto propone que este incidente a la seguridad además de notificarse a la Autoridad de Aplicación deba notificarse

también a los titulares de los datos y realizar las denuncias penales ante las autoridades pertinentes.

Con respecto a las condiciones de implementación de la mencionada obligación, siguiendo la propuesta del Reglamento de la UE 2016/679, se propone que sólo se exija la notificación ante un incidente de seguridad que probablemente constituya un riesgo para los titulares. De lo contrario, podría caerse en rigorismos formales que ocasionarían tal exceso de notificación que los titulares de los datos ni prestaran atención a esas notificaciones y a su vez, se abrumaría a la Autoridad de Aplicación impidiendo se avocara a casos donde realmente ameritase su intervención, esto es, casos de efectivo daño material.

En cuanto al plazo se establece el responsable del tratamiento deberá notificarlo a la Autoridad de Aplicación y al titular de los datos, sin dilación indebida y de ser posible dentro de las 72 horas desde que haya tomado conocimiento de ella. Se prevé la posibilidad de que este plazo se extienda a 10 días siempre que se acrediten motivos justificados.

Asimismo, se propone regular el contenido mínimo de la notificación, a fin de que se incluya en ella: a) la naturaleza del incidente, b) la categoría de datos personales comprometidos, c) identificación de titulares afectados, d) *posibles consecuencias del incidente, e)* medidas adoptadas para remediarlo y en su caso para mitigar los posibles efectos negativos, f) medidas correctivas aplicadas para evitar futuros incidentes, g) recomendaciones al titular de los datos acerca de las medidas que este pueda adoptar para proteger sus intereses, h) Los medios a disposición del titular de los datos para obtener mayor información al respecto.

Por último, se establece que el responsable del tratamiento deberá dejar documentado todo incidente de la seguridad de los datos personales.

La filtración de datos es un tema recurrente y preocupante, por lo que a fin de poder tomar conocimiento de los incidentes que se produzcan y principalmente para mitigar los daños ocasionados y evitar futuros incidentes consideramos necesario incluir en forma urgente en la legislación la obligación de notificarlos.

Por todo lo expuesto, solicito a mis padres me acompañen en la aprobación del presente proyecto de ley.

Firmante: **Gabriela BESANA**