ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

PROYECTO DE LEY

ADICIÓN DE LOS ARTÍCULOS 12 BIS, 12 TER Y UN INCISO F) AL ARTÍCULO 30 A LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES, LEY 8968 Y SUS REFORMAS

MARÍA MARTA CARBALLO ARCE
DIPUTADA

EXPEDIENTE N.° 24135

PROYECTO DE LEY

ADICIÓN DE LOS ARTÍCULOS 12 BIS, 12 TER Y UN INCISO F) AL ARTÍCULO 30 A LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES, LEY 8968 Y SUS REFORMAS

Asamblea Legislativa:

El presente proyecto de ley que busca establecer la obligatoriedad para los encargados de tratamiento de bases de datos de realizar una notificación a los titulares de los datos en un periodo de hasta 72 horas siguientes a detección de una violación de la seguridad de datos personales. Esta iniciativa tiene como objetivo fortalecer la protección de la privacidad de los individuos y garantizar una gestión responsable de la información personal en consonancia con los principios y estándares establecidos en el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

La revolución digital ha transformado la forma en que manejamos y compartimos información personal. La creciente interconexión de sistemas y la gestión masiva de datos personales han expuesto a los individuos a riesgos significativos, como la posibilidad de violaciones de seguridad que comprometen su privacidad. En este contexto, la protección de datos se ha vuelto crucial para preservar la confianza de los ciudadanos en la era digital.

El Reglamento General de Protección de Datos de la Unión Europea (GDPR), implementado en mayo de 2018, establece un marco legal sólido para la protección de datos personales. Uno de los principios fundamentales del GDPR es la transparencia en el tratamiento de datos, que implica informar a los individuos afectados cuando se produce una violación de seguridad que pueda afectar sus derechos y libertades.

Este proyecto de ley pretende perseguir los siguientes objetivos:

Fomentar la coherencia Internacional:

Adoptar principios del GDPR implica alinearse con estándares internacionales de protección de datos, facilitando la interoperabilidad y la cooperación transfronteriza. La coherencia normativa internacional fortalece la posición del país en la comunidad global y facilita el intercambio de datos de manera segura.

Fortalecer la Confianza del Consumidor:

La estandarización con el GDPR transmite a los ciudadanos un compromiso serio con la protección de su privacidad, generando confianza en las instituciones y las empresas que manejan sus datos. La confianza del consumidor es esencial para el crecimiento de la economía digital, ya que fomenta la participación activa en plataformas y servicios en línea.

Promover la Protección Reforzada de los Derechos Individuales:

Los principios del GDPR, como el derecho a la información y el consentimiento informado, refuerzan los derechos individuales de los ciudadanos sobre sus datos personales. Una legislación robusta inspirada en el GDPR garantiza que los ciudadanos tengan un mayor control sobre sus datos y estén informados sobre cómo se utilizan.

Impulsar la Prevención y Respuesta Efectiva ante Violaciones de Datos:

La notificación obligatoria de violaciones de seguridad, basada en el GDPR, permite una respuesta más rápida y efectiva ante incidentes, minimizando el impacto en los individuos afectados. La estandarización de procedimientos facilita la cooperación entre entidades públicas y privadas para abordar y mitigar las violaciones de datos de manera coordinada.

Facilitar el Comercio Internacional:

Cumplir con los estándares del GDPR facilita el flujo seguro de datos entre entidades en diferentes jurisdicciones, reduciendo barreras para el comercio internacional y fomentando la cooperación económica. Las empresas nacionales que se adhieren a principios reconocidos internacionalmente pueden beneficiarse de una posición competitiva más fuerte en el mercado global.

Estimular la Rendición de Cuentas y Sanciones Proporcionadas:

La estandarización con el GDPR fortalece la rendición de cuentas al establecer sanciones proporcionadas por incumplimientos, incentivando a las organizaciones a implementar medidas de seguridad adecuadas. Sanciones consistentes y proporcionadas contribuyen a disuadir prácticas irresponsables en el manejo de datos personales.

Fomentar la Innovación Responsable:

Un marco normativo alineado con el GDPR promueve la innovación responsable al exigir a las organizaciones considerar la privacidad desde el diseño en nuevas tecnologías y servicios. La protección de datos se convierte en un componente esencial de la responsabilidad corporativa, fomentando prácticas empresariales éticas y sostenibles.

Mejorar la Eficiencia Operativa:

La estandarización simplifica la gestión de la conformidad legal para las organizaciones al seguir un conjunto coherente de principios y normativas. Se reducen los costos asociados con la adaptación a diferentes regulaciones, facilitando la eficiencia operativa de las empresas.

En conclusión, este proyecto de ley tiene como propósito principal fortalecer la seguridad de los datos personales y consolidar la confianza de los ciudadanos en el manejo de su información en la era digital. La adopción de estas medidas refleja nuestro compromiso con los estándares internacionales de protección de datos y contribuirá a una sociedad digital más segura y ética.

Comparación con países de la región

Uruguay:

En el artículo 4 de la reglamentación de los arts. 37 a 40 de la ley 19.670 y art. 12 de la ley 18.331, referente a protección de datos personales establece que:

"El responsable del tratamiento, una vez que constate la ocurrencia de alguna vulneración de seguridad que incida en la protección de datos, deberá comunicarlo a la Unidad Reguladora y de Control de Datos Personales en un plazo máximo de **72 horas de conocida la vulneración**."

México:

En el Artículo 64 del Reglamento de la ley federal de protección de datos personales en posesión de los particulares, se establece que:

"El responsable deberá informar al titular las vulneraciones que afecten de forma significativa sus derechos patrimoniales o morales, **en cuanto confirme que ocurrió la vulneración** y haya tomado las acciones encaminadas a detonar un proceso de revisión exhaustiva de la magnitud de la afectación, y sin dilación alguna, a fin de que los titulares afectados puedan tomar las medidas correspondientes"

Panamá:

En el Artículo 37 del Reglamento de la 81 de protección de datos personales en, se establece que:

Notificación de violaciones de la seguridad de los datos personales. Cuando el responsable del tratamiento tenga conocimiento de una violación de seguridad, entendida ésta como cualquier daño, pérdida, alteración, destrucción, acceso, y en general, cualquier uso ilícito o no autorizado de los datos personales, aun cuando ocurra de manera accidental, en cualquier fase del tratamiento y que represente un riesgo para la protección de los datos personales, **notificará de inmediato dicho incidente a la autoridad de control y a los titulares afectados.**

La notificación que realice el responsable del tratamiento a los titulares afectados estará redactada en un lenguaje claro y sencillo.

En los tres casos anteriores, de países con los que compartimos no solamente la cercanía geográfica, sino que también compartimos similitudes socioeconómicas se

concluye que la normativa actual es muy permisiva y afecta a los titulares de los datos.

Es por las razones expuestas y justificadas con anterioridad, que se presenta a consideración de las señoras diputadas y los señores diputados el siguiente proyecto de ley para su discusión y aprobación.

ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE COSTA RICA

DECRETA:

ADICIÓN DE LOS ARTÍCULOS 12 BIS, 12 TER Y UN INCISO F) AL ARTÍCULO 30 A LA LEY DE PROTECCIÓN DE LA PERSONA FRENTE AL TRATAMIENTO DE SUS DATOS PERSONALES, LEY 8968 Y SUS REFORMAS

Artículo 1. Se adiciona un artículo 12 bis a la Ley de protección de la persona frente al tratamiento de sus datos personales, ley 8968 y sus reformas, para que en adelante se lea de la siguiente manera:

"Artículo 12 bis. Vulnerabilidad de seguridad. El responsable deberá informar al titular y a la Agencia sobre cualquier irregularidad en el tratamiento o almacenamiento de sus datos, tales como pérdida, destrucción, extravío, entre otras, como consecuencia de una vulnerabilidad de la seguridad o que tuviere conocimiento del hecho, para lo cual tendrá 72 horas a partir del momento en que ocurrió la vulnerabilidad, a fin de que los titulares de estos datos personales afectados puedan tomar las medidas correspondientes.

Dentro de este mismo plazo deberá iniciar un proceso de revisión exhaustiva para determinar la magnitud de la afectación, y las medidas correctivas y preventivas que correspondan

La comunicación al interesado a que se refiere este artículo no será necesaria si esto supone un esfuerzo desproporcionado; en este caso se optará, en su lugar, por un a comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los titulares"

Artículo 2. Se adiciona un artículo 12 ter a la Ley de protección de la persona frente al tratamiento de sus datos personales, ley 8968 y sus reformas, para que en adelante se lea de la siguiente manera:

"Artículo 12 ter. Información mínima. El responsable deberá informar al titular y a la Agencia, en caso de vulnerabilidades de seguridad, al menos lo siguiente:

a) La naturaleza del incidente;

b) Los datos personales comprometidos;

c) Las acciones correctivas realizadas de forma inmediata; y,

d) Los medios o el lugar, donde puede obtener más información al respecto."

Artículo 3. Se adiciona un inciso f) al artículo 30 de la Ley de protección de la persona frente al tratamiento de sus datos personales, ley 8968 y sus reformas, para que en adelante se lea de la siguiente manera:

"Artículo 30. Faltas graves

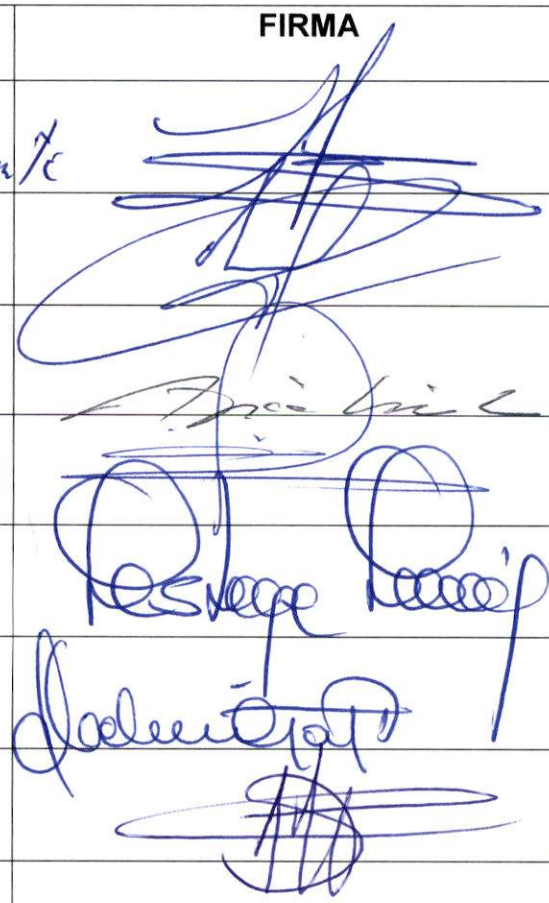
(...)

f) Negarse injustificadamente a informar al titular y a la Agencia sobre cualquier irregularidad en el tratamiento o almacenamiento de sus datos, tales como pérdida, destrucción, extravío, entre otras, como consecuencia de una vulnerabilidad de la seguridad o que tuviere conocimiento del hecho en el plazo establecido en el artículo 12 bis y 12 ter de la presente ley."

Rige a partir de su publicación.

María Marta Carballo Arce

Diputada

NOMBRE	FIRMA
Horacio Mauricio Bogarín	
Carlos Andrés Rojas M	
Alejandro Naranjo Castro	
Daniela Rojas Salas	
Lesbeye Bejarques León	
Helina Araya Rojas	
Carlos Felipe García M	