

DÍA INTERNACIONAL DE PROTECCIÓN DE DATOS PERSONALES



2018

Conferencia Magistral

Datos personales sensibles

Lic. Eugenio Rosendoevgueni Monterrey Chepov





Introducción



Existe una coincidencia internacional respecto a que hay ciertas clases de datos personales que requieren de mayor protección, y que su tratamiento debe realizarse bajo condiciones especiales, en virtud de que hay cierta información correspondiente a la esfera más íntima del individuo, cuyo mal uso puede afectar sus derechos fundamentales.





Ante la falta de confianza existente entre la población acerca de la vigilancia estatal por diversas causas que a lo largo de la historia han quedado registradas, por ejemplo, durante la Segunda Guerra Mundial, la agresión Nazi implicó que el gobierno utilizara instrumentos de monitoreo y que se administrara un listado de personas de origen y creencias judías y con preferencias homosexuales, quienes fueron perseguidos por el régimen.

Es que se ha derivado en el interés del legislador y de las autoridades de datos personales y judiciales, de considerar y desarrollar un régimen especial de tratamiento para los denominados “datos personales sensibles”.





Datos personales sensibles

Definición

Datos personales sensibles

Definición



Son toda aquella información vinculada con una persona física, que revela sus aspectos más íntimos, es decir, más reservados y profundos.

Como un estándar internacional, también se define a esta información como aquella cuya difusión o utilización indebida pueda dar origen a discriminación o a un riesgo grave para su titular. Algunos instrumentos internacionales señalan como ejemplos de datos personales sensibles los de origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la salud o la sexualidad.



*Afiliación sindical se considera dato personal sensible únicamente en la LFPDPPP



Asimismo, se ha identificado que el concepto “datos personales sensibles” puede realizarse en la normativa de las distintas regiones y países de la siguiente manera:

Descriptiva

- Se exponen los requisitos que deben ser satisfechos a fin de que determinado dato personal sea considerado como sensible

Listado

- Se expone una lista de los datos que son considerados como sensibles, ejemplo: *el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, etc.*

Mixta

- Técnica de definición reúne las dos anteriores, donde se exponen las características de los datos sensibles y se enlista una serie de datos considerados como sensibles.



Definición de datos personales sensibles de distintas regiones y países

México

Mixta / Abierta
Aquéllos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste.

Australia

Listado / Cerrada
Ejemplos: origen racial o étnico, opiniones políticas, afiliación política, religión o ideas filosóficas, orientación sexual, antecedentes penales, entre otros.

Canadá

Mixta / Abierta
Se considera que cierta información (por ejemplo, registros médicos y registros de ingresos) casi siempre se considera confidencial, dependiendo del contexto.

Uruguay

Listado / Cerrada
Son los que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual

N. Zelanda

No establece de manera explícita definición, sin embargo tiene una ley específica en materia de protección de datos personales.

U.E.

Listado / Cerrada
Tratamiento de categorías especiales de datos.

EUA

Se regula de manera sectorial.



Información de salud

- México, Australia, Canadá, EUA, N. Zelanda, UE, Uruguay

Origen racial o étnico

- México, Australia, UE, Uruguay

Opiniones políticas

- México, Australia, UE, Uruguay

Creencias religiosas/Filosóficas/Morales

- México, Australia, UE, Uruguay

Información sexualidad

- México, Australia, UE, Uruguay

Biométricos

- Australia, EUA, UE

A nivel internacional se pueden encontrar definiciones muy similares, sin embargo, existen algunas diferencias en la determinación acerca de qué información se considera de este tipo, ya que depende de la cultura y el contexto.

Por ejemplo, mientras que en México el origen racial o étnico es un dato personal sensible (DPS), en Canadá o Estados Unidos no es así, y mientras que en Australia el número de seguridad social es considerado un DPS, en nuestro país o en Uruguay no.



El riesgo y su relación con los datos personales sensibles



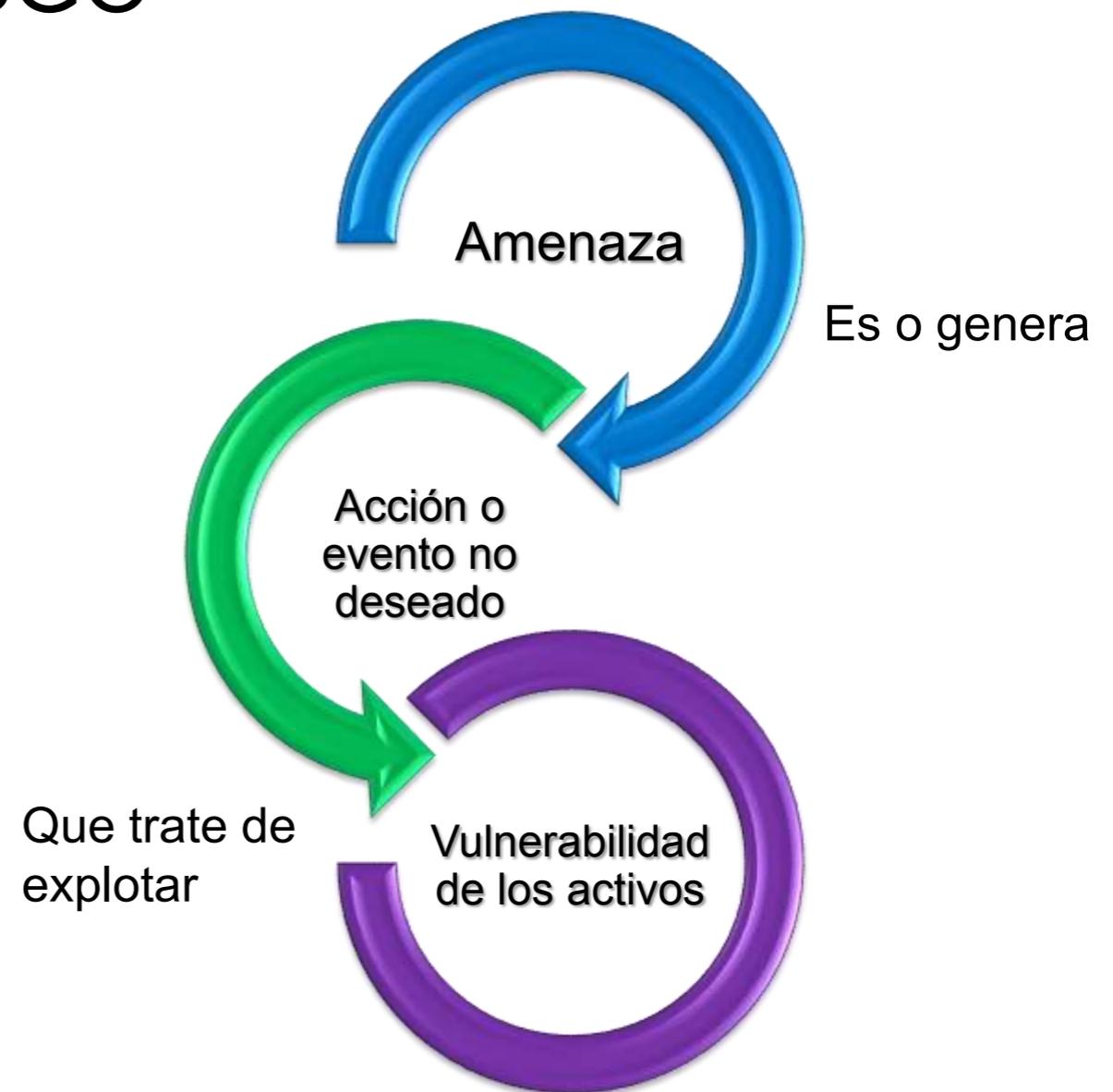
Para definir el **riesgo**, es necesario abordar los siguientes conceptos base interrelacionados





Estructura de un RIESGO

Los activos, las amenazas y las vulnerabilidades se combinan para generar **riesgos**. El riesgo es el potencial o la probabilidad de que ocurra un escenario donde una amenaza explote una o varias vulnerabilidades existentes, en un activo o grupo de activos, y que se produzca un impacto negativo o daño.





Los datos personales tienen un **riesgo intrínseco o inherente** al que están sujetos debido al valor que tienen para sus titulares, o para personas no autorizadas que puedan beneficiarse de ellos.



Por ejemplo, en el caso de dos bases de datos de un hospital, con una vulnerabilidad en común, y expuestas a un mismo tipo de amenaza, el riesgo inherente es el factor que determina el riesgo al que está expuesto cada sistema de tratamiento:





En este sentido, se puede inferir que los datos personales sensibles, categorizados por la LGPDPPSO y la LFPDPPP, poseen un riesgo inherente mayor que los datos personales generales. Es por ello, que ambas leyes establecen un régimen especial para su tratamiento y ordenan medidas de seguridad mayores.





Tratamiento de los datos personales sensibles en el mundo

Tratamiento de los datos personales sensibles en el mundo



Como se mencionó en la introducción, existe consenso internacional con relación a la existencia de ciertas clases de datos personales que requieren de mayor protección que otros, y que su tratamiento debe realizarse bajo ciertas condiciones.

Entre los tratamientos diferenciados para los datos sensibles, se compararon algunas jurisdicciones (México, Australia, Canadá, EUA, Nueva Zelanda, la Unión Europea y Uruguay), entre los que se encuentran:



Prohibición para su tratamiento por regla general o bajo condiciones muy limitadas;



El tipo de consentimiento que se requiere para su tratamiento –expreso o expreso y por escrito-;



Mayores medidas de seguridad para su tratamiento, y



La agravante de la sanción en caso de tratamiento indebido



Casos Relevantes



- **Transferencia no consentida de datos personales de salud por parte de institución financiera.**

En 2015, el INAI recibió una denuncia derivada de una supuesta transferencia de los datos personales de la titular y su cónyuge recabados por un banco a través de un contrato de apertura de crédito.



Se determinó un incumplimiento por parte de la institución financiera, imponiendo una sanción total de \$32'006,691.00 M.N.

Cabe señalar que una parte de multa fue duplicada por involucrar datos personales sensibles.



Vulneración de seguridad de datos personales – incluyendo sensibles- por el Departamento de Migración y Protección Fronteriza (DIPB)

En 2014, el Comisionado de Privacidad Australiana abrió una investigación en contra del DIPB por un reportaje que se publicó en el periódico *The Guardian* Australia que señalaba que en el portal de Internet del DIPB se encontraba disponible una base de datos con información personal de aproximadamente 10,000 solicitantes de asilo.

La investigación arrojó que la falla consistió en la publicación que cada mes realizaba la DIPB sobre estadísticas de detenciones migratorias. El documento contenía una gráfica insertada que habilitaba la información del archivo de Excel que fue utilizado para generar datos y que incluía información sobre aproximadamente 10,000 solicitantes de asilo, con nombres completos, género, ciudadanía, fecha de nacimiento, periodo de detención migratoria, datos de los cuales muchos eran de carácter personal sensible.

El caso es importante debido a que el Comisionado de Privacidad Australiano determinó que se debió considerar la sensibilidad de los datos para la toma de medidas de seguridad para evitar su pérdida.





Casos relevantes Estados Unidos



En diciembre de 2016, el investigador informático estadounidense Chris Vickery, alertó de la filtración de datos personales de altos funcionarios militares de Estados Unidos. Al parecer, la filtración se había llevado a cabo a través de *Potomac Healthcare Solutions*, un subcontratista del Gobierno de EUA que trabajaba para el Pentágono que proporciona servicios de salud a las organizaciones gubernamentales y militares.

Como seguimiento de la comunicación realizada por Chris Vickery, *Potomac Healthcare Solutions*, con el apoyo de una firma forense externa de tecnologías de la información, señaló que había realizado la investigación del incidente de seguridad que involucró el **acceso no autorizado de uno de sus servidores internos**, manifestando que su revisión inició inmediatamente después de los cuestionamientos realizados por Chris Vickery.

Aunque la información de este caso no ha sido oficialmente confirmado (toda la información fue obtenida directamente de la prensa), se considera relevante considerar que, en ocasiones, los incidentes de seguridad pueden ser causados por los terceros contratados para llevar a cabo el tratamiento de datos personales, incluidos datos personales sensibles, casos en los que las medidas tanto de seguridad como contractuales deben ser aún mayores.



Casos relevantes Nueva Zelanda



A un médico de una clínica perteneciente a un área suburbana le fue robado su maletín –el cual se encontraba en el interior de su auto-, en el cual llevaba una memoria USB con la información personal de algunos de sus pacientes. Dicha información detallaba el nombre y apellido de los mismos, así como los medicamentos recetados y su diagnóstico médico. Al enterarse, uno de los pacientes del doctor presentó su queja ante la Oficina del Comisionado de Privacidad de Nueva Zelanda.

En cuanto tuvo conocimiento de la vulneración, el director de la clínica decidió actuar de manera rápida y conforme a lo que señalaba la guía para reaccionar ante una vulneración a la privacidad.

Este caso represente un buen ejemplo de medidas administrativas y técnicas que puede tomarse para evitar vulneraciones de seguridad.





Información estadística y de interés

El valor de los datos personales en los mercados ilegales

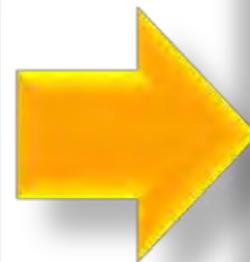


Precios estimados por tarjeta en dólares estadounidenses, por datos de tarjetas de pago robados



Saldo de la cuenta del servicio de pago online

- 400-1000 dólares
- 1000-2500 dólares
- 2500-5000 dólares
- 5000-8000 dólares



Precio estimado por cuenta

- 20-50 dólares
- 50-120 dólares
- 120-200 dólares
- 200-300 dólares



Conclusiones



- ✓ Se identifican **tratamientos diferenciados en diversa normativa internacional prevista para la regulación de los datos sensibles**, tales como:
 - a) **Tratamiento limitado.**
 - b) **Consentimiento expreso** para su tratamiento;
 - c) **Mayores medidas de seguridad**, y
 - d) **Agravante de la sanción** en caso de un tratamiento indebido.

- ✓ Los **datos personales sensibles tienen un valor** debido a los **beneficios que representan para un tercero.**

- ✓ El **INAI subraya la importancia de generar conciencia en el debido cuidado y tratamiento de los datos sensibles** como garantía para el ejercicio de otros derechos.



**DÍA INTERNACIONAL
DE PROTECCIÓN DE DATOS PERSONALES**



2018

Datos Personales Sensibles

GRACIAS

