

# **DERECHO INFORMÁTICO**

Protección de Datos Personales

(Parte II)

# **PROTECCIÓN DE DATOS PERSONALES**

## **CLASIFICACIÓN DE DATOS PERSONALES**

# **PROTECCIÓN DE DATOS PERSONALES**

## **1-DATOS SENSIBLES**

# **PROTECCIÓN DE DATOS PERSONALES**

## Ley 25.236

Son aquellos datos personales íntimos que requieren una reserva.

- Art. 2.- Datos que revelen: información de origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, información referente a la salud o vida sexual.
- Art 7.- Principio general: ninguna persona puede ser obligada a proporcionarlos (art. 7, inc. 1).

Excepción: solo se pueden recolectar y tratar:

- 1) cuando medien razones de interés general autorizadas por Ley;
- 2) cuando su uso sea para finalidades estadísticas o científicas y no puedan ser identificados sus titulares.

Está prohibida la base de datos que contengan información que revelen datos sensibles, excepción: iglesia católica y asociaciones religiosas y organizaciones políticas y sindicales. Y autoridad publica competente (datos relativos a antecedentes penales o contravencionales)

# PROTECCIÓN DE DATOS PERSONALES

Ley 26.879 crea el Registro Nacional de Datos Genéticos vinculados a Delitos contra la Integridad Sexual

ART2: Tiene por Finalidad: facilitar el esclarecimiento de los hechos vinculados a tales delitos, con el objeto de individualizar a las personas responsables.

ART 3: El Registro almacenará y sistematizará la información genética asociada a una muestra o evidencia biológica que hubiere sido obtenida en el curso de una investigación criminal y de toda persona condenada con sentencia firme por los delitos enunciados en el artículo 2° de la presente ley. Asimismo, respecto de toda persona condenada se consignará:

a) Nombres y apellidos, apodos, seudónimos o sobrenombres; b) Fotografía actualizada; c) Fecha y lugar del nacimiento; d) Nacionalidad; e) Número de documento de identidad y autoridad que lo expidió; f) Domicilio actual, para lo cual el condenado, una vez en libertad, deberá informar a la autoridad los cambios de domicilio que efectúe.

Datos Genéticos: información asociada a una muestra o evidencia biológica obtenida en el curso de una investigación penal y de toda persona condenada con sentencia firme por delitos contra la integridad sexual.

Datos de carácter sensible y reservado: sólo serán suministrados al Ministerio Público Fiscal, jueces y tribunales en el marco de una causa en la que se investigue alguno de estos delitos.

# PROTECCIÓN DE DATOS PERSONALES

## Datos de Salud:

Están protegidos por la Ley 25.236 y 26.529. Es decir, tienen doble protección.

### Ley 25.236

- Art. 8: los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud, pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando el secreto profesional.

### Ley 26.529

- Art. 2, c): toda actividad médico - asistencial tendiente a obtener, clasificar, utilizar, custodiar y transmitir información y documentación clínica del paciente, debe observar:
- el estricto respeto por la dignidad humana y la autonomía de la voluntad,
- el debido resguardo de la intimidad y confidencialidad de sus datos sensibles.

Art. 13: Historia Clínica Informatizada: aquella confeccionada en soporte magnético que asegure su integridad, autenticidad y recuperabilidad.

Arts. 14 y 19: el paciente es el titular de la misma, y a su simple requerimiento debe suministrársele copia autenticada por autoridad de la institución asistencial dentro de las 48 horas de solicitada.

Art. 20: ante la negativa, demora o silencio podrá interponerse la acción de habeas data para el acceso y obtención.

# **PROTECCIÓN DE DATOS PERSONALES**

## **2- SUPUESTOS ESPECIALES**

# **PROTECCIÓN DE DATOS PERSONALES**

## Art 23. Ley 25.326

Fines policiales: los datos registrados con estos fines se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

Fines de defensa nacional o seguridad pública: los datos recabados por las fuerzas armadas o de seguridad, organismos policiales o de inteligencia, sin consentimiento de los afectados, se limitará a los necesarios para el estricto cumplimiento de las misiones legalmente asignadas para la defensa nacional, seguridad pública o represión de los delitos.



# **PROTECCIÓN DE DATOS PERSONALES**

## **3- INFORMACIÓN CREDITICIA**

# **PROTECCIÓN DE DATOS PERSONALES**

Datos de Información Crediticia: Art. 26 Ley 25.326

Interés contrapuesto: protección del crédito vs quienes incurrieron en mora pero cumplieron su obligación y por ello tienen un “derecho al olvido”.

Derecho al olvido: principio según el cual ciertas informaciones deben ser eliminadas de los archivos transcurrido un determinado espacio de tiempo desde el momento en que acaeció el hecho a que se refieren.

Derecho al olvido: los bancos pueden tratar estos datos hasta:

- - 5 años desde la última información adversa archivada (dato significativo) que demuestre que la deuda era exigible (Decreto 1558/2001); una sentencia, una demanda, una carta documento.
- - 2 años desde la cancelación de la deuda

# **PROTECCIÓN DE DATOS PERSONALES**

## **4- SERVICIOS DE DATOS INFORMATIZADOS**

(cloud computing )

# **PROTECCIÓN DE DATOS PERSONALES**

## Prestación de Servicios Informatizados de Datos Personales: Art. 25 Ley 25.326

- 1) Titular de los datos.
  - 2) Responsable del Tratamiento (Base de Datos).
  - 3) Encargado del Tratamiento por cuenta del Banco de Datos (Cloud Computing).
1. Cuando por cuenta de terceros se presten servicios de tratamiento de datos personales, éstos no podrán aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederlos a otras personas, ni aun para su conservación.
  - 2. Una vez cumplida la prestación contractual los datos personales tratados deberán ser destruidos, salvo que medie autorización expresa de aquel por cuenta de quien se prestan tales servicios cuando razonablemente se presuma la posibilidad de ulteriores encargos, en cuyo caso se podrá almacenar con las debidas condiciones de seguridad por un período de hasta dos años.

# **PROTECCIÓN DE DATOS PERSONALES**

## Cloud Computing (Computación en la Nube)

- Servicio prestado a través de Internet que consiste:
- en la migración de información, datos, informaciones de negocios y actividades informáticas de una persona u empresa,
- a computadoras y sitios de Hosting de un tercero (la Nube) para almacenarse en forma remota,
- con quien se celebra un contrato a tal fin, por el cual se permite tener acceso a la información y software necesarios en cada oportunidad que se requiera vía web.

# **PROTECCIÓN DE DATOS PERSONALES**

## Software as a Service (SaaS)

Servicio de aplicaciones que se ofrecen desde una plataforma online administrada por el proveedor, sin necesidad que el usuario descargue el software.

El usuario usa el servicio y el proveedor almacena la información.

Satisface a múltiples usuarios con un mismo software (comunicación, negocios, esparcimiento, etc.).

## Platform as a Service (PaaS)

Un nivel más avanzado. Permite al usuario con conocimiento de lenguaje de programación la posibilidad de desarrollar e implementar aplicaciones como Java, etc. Ofrece herramientas de desarrollo y un entorno donde alojar sus propios servicios.

## Infrastructure as a Service (IaaS)

Se ofrece un servicio de almacenamiento y procesamiento de datos, permitiendo que el usuario acceda a ellos en forma remota y desde cualquier dispositivo mediante una clave.

Se paga por consumo de recursos: espacio en disco utilizado y base de datos; tiempo de almacenamiento; back up y transferencia de datos; gestión de redes; seguridad y planes de contingencia ante amenazas.

# **PROTECCIÓN DE DATOS PERSONALES**

El contrato de prestación de servicios por encargo debe:

- disponer que el encargado del tratamiento sólo actúa siguiendo instrucciones del responsable del tratamiento; y que las obligaciones de seguridad también incumben al encargado del tratamiento.
- contener los niveles de seguridad previstos en la Ley N° 25.326 (Protección de datos personales) y Disposiciones de la DNPDP (Dirección Nacional de Protección de Datos Personales); y las obligaciones de confidencialidad y reserva.
- Los datos tratados no pueden aplicarse o utilizarse con un fin distinto al que figure en el contrato de servicios, ni cederse a otras personas aún para su conservación.
- Cumplida la prestación contractual los datos deben ser destruidos; salvo autorización expresa del Banco de Datos, cuando razonablemente se presuma la posibilidad de ulteriores encargos; en cuyo caso se podrán almacenar en condiciones de seguridad por un período de hasta 2 años.

# **PROTECCIÓN DE DATOS PERSONALES**

## **5- MARKETING DE COMPORTAMIENTO**

(cookies y spam )



# **PROTECCIÓN DE DATOS PERSONALES**

## **“cookies”**

Las “Cookies” son pequeños archivos que se bajan automáticamente en el navegador de la computadora o dispositivo móvil del usuario, cuando éste ingresa a los sitios web.

- almacenan y remiten información sobre el comportamiento online del usuario.
- El almacenamiento y tratamiento de esta información permite crear un perfil que determina gustos, intereses, hábitos de consumo y capacidad de compra del usuario, para luego hacerle llegar ofertas de bienes y servicios mediante publicidad personalizada (“spam”).
- Son un medio de obtención de información importante para los departamentos de marketing de las empresas que hacen publicidad en Internet.

# **PROTECCIÓN DE DATOS PERSONALES**

## **“cookies”**

**Sistema “Opt-in”** (suscripción voluntaria): Actualmente, los sitios web que utilicen “cookies” deben solicitar autorización al usuario y esta debe manifestarse en forma previa, expresa y voluntaria para la inserción de las mismas.

**Sistema “Opt-out”**: Presume que las personas han dado el consentimiento para la instalación de “Cookies” en computadoras o dispositivos móviles hasta tanto el destinatario exprese su negativa.