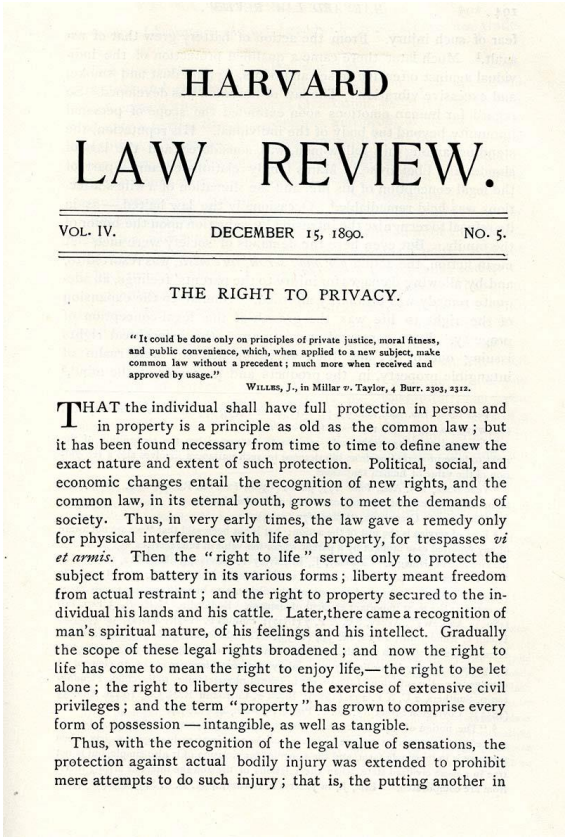
BASES DE DATOS PERSONALES

Abog. MARÍA DELIA ESPÓSITO

Introducción

- Derecho intimidad o vida privada y familiar
- Intromisión arbitraria
- "Derecho a que me dejen solo"
  - *Louis Brandeis y*
  - *Samuel Warren,*
  - *1890, Harvard Law Review*



HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

WILLES, J., in Millar v. Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession—intangible, as well as tangible.

Thus, with the recognition of the legal value of sensations, the protection against actual bodily injury was extended to prohibit mere attempts to do such injury; that is, the putting another in

Antecedentes normativos

- ONU
- Consejo Ministros Europa
- Legislación europea
- Estados Unidos

Elaboración Principios

- Principios aplicables al tratamiento (electrónico - automatizado) datos personales
- Directrices Consejo Ministros Europa
- Convenio 108, Estrasburgo (1981)
- Leyes europeas

Normas europeas

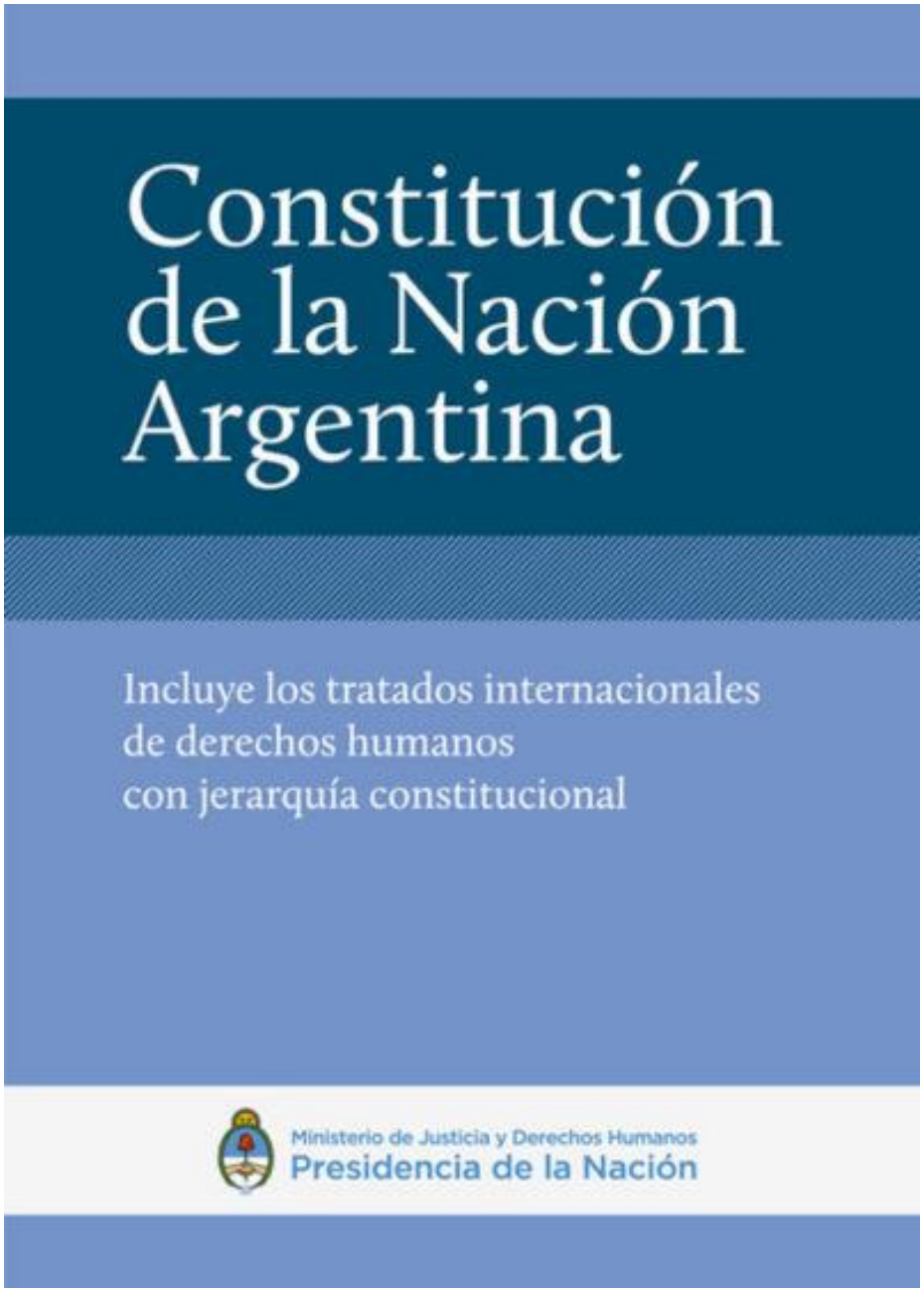
- Principios calidad datos personales
- Organismos (agencias) control
- Bancos datos públicos y privados
- Sanciones administrativas
- Sanciones penales
- Responsabilidad civil
- Incorporación en algunas constituciones

Antecedentes internacionales

- Recomendaciones expertos Consejo Ministros Europa
  - *Normas nacionales*
    - Suecia (1970)
    - Francia (1978)
    - Dinamarca, Bélgica, etc
- Convenio 108, Estrasburgo, 1981

Antecedentes derecho argentino tutela privacidad

- CONSTITUCIÓN NACIONAL
- CÓDIGO CIVIL Y COMERCIAL
- LEYES


Constitución de la Nación Argentina
Incluye los tratados internacionales de derechos humanos con jerarquía constitucional
Ministerio de Justicia y Derechos Humanos
Presidencia de la Nación

ARTÍCULO 19

Las acciones privadas de los hombres que de ningún modo ofendan al orden y a la moral pública, ni perjudiquen a un tercero, están sólo reservadas a Dios, y exentas de la autoridad de los magistrados.

CONSTITUCIÓN NACIONAL ARGENTINA

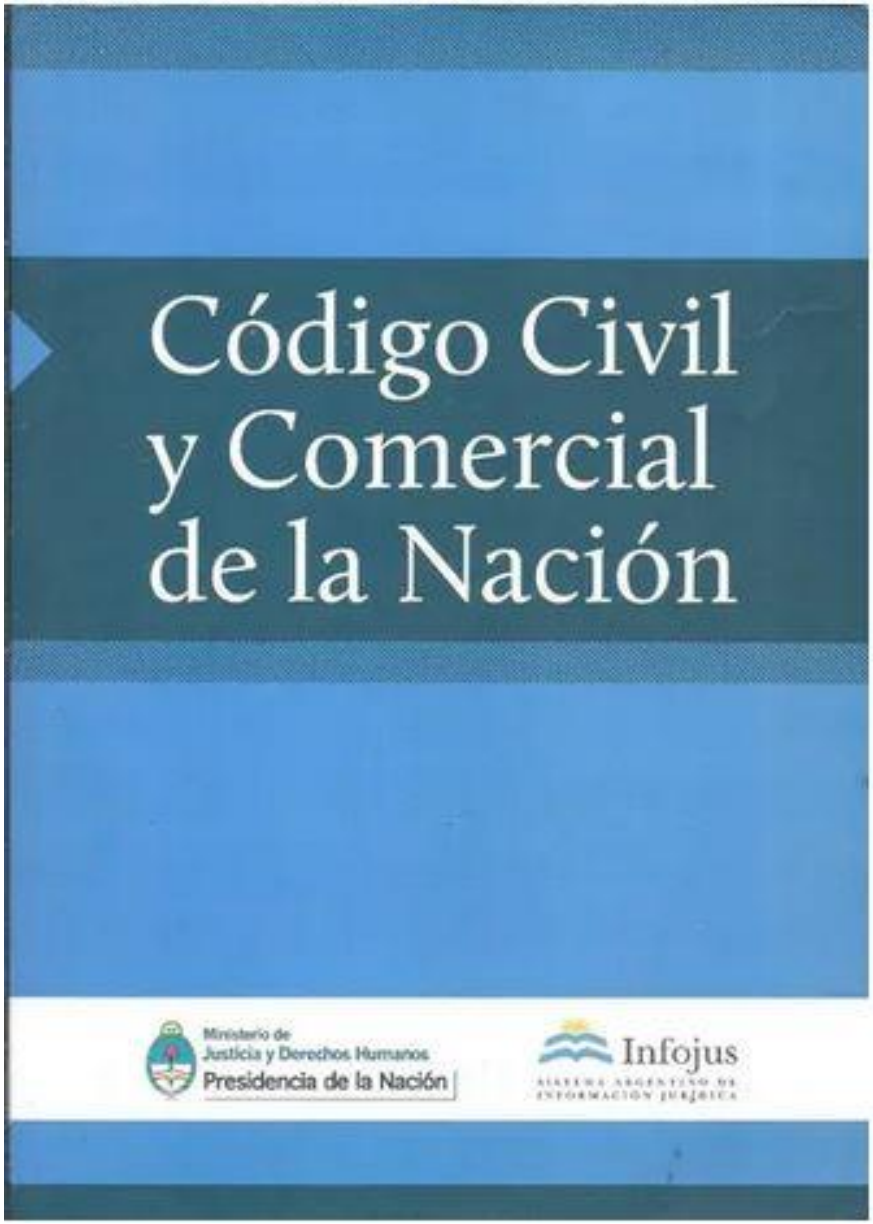
Ningún habitante de la Nación será obligado a hacer lo que no manda la ley, ni privado de lo que ella no prohíbe.

ARTÍCULO 18

El domicilio es inviolable, como también la correspondencia epistolar y los papeles privados;

CONSTITUCIÓN NACIONAL ARGENTINA

y una ley determinará en qué casos y con qué justificativos podrá procederse a su allanamiento y ocupación


Código Civil
y Comercial
de la Nación
Ministerio de
Justicia y Derechos Humanos
Presidencia de la Nación
Infojus

Artículo 52. Afectaciones a la dignidad

La persona humana lesionada en su intimidad personal o familiar, honra o reputación, imagen o identidad, o que de cualquier modo resulte menoscabada en su dignidad personal,

CÓDIGO CIVIL Y COMERCIAL

puede reclamar la prevención y reparación de los daños sufridos, conforme a lo dispuesto en el Libro Tercero, Título V, Capítulo 1.

Artículo 1770. Protección de la vida privada

El que arbitrariamente se entromete en la vida ajena y publica retratos, difunde correspondencia, mortifica a otros en sus costumbres o sentimientos, o perturba de cualquier modo su intimidad, debe ser obligado a cesar en tales actividades, si antes no cesaron, y a pagar una indemnización que debe fijar el juez, de acuerdo con las circunstancias.

CÓDIGO CIVIL Y COMERCIAL

Además, a pedido del agraviado, puede ordenarse la publicación de la sentencia en un diario o periódico del lugar, si esta medida es procedente para una adecuada reparación.

Artículo 53. Derecho a la imagen

Para captar o reproducir la imagen o la voz de una persona, de cualquier modo que se haga, es necesario su **consentimiento**, excepto en los siguientes casos: a) que la persona participe en actos públicos; b) que exista un interés científico, cultural o educacional prioritario, y se tomen las precauciones suficientes para evitar un daño innecesario;

CÓDIGO CIVIL Y COMERCIAL

c) que se trate del ejercicio regular del derecho de informar sobre acontecimientos de interés general. En caso de personas fallecidas pueden prestar el consentimiento sus herederos o el designado por el causante en una disposición de última voluntad. Si hay desacuerdo entre herederos de un mismo grado, resuelve el juez. Pasados veinte años desde la muerte, la reproducción no ofensiva es libre..

Antecedentes derecho argentino tutela privacidad

- "INDALIA *PONZETTI DE BALBÍN* c/ *EDITORIAL ATLÁNTIDA* S.A. s/ DAÑOS Y PERJUICIOS".
- SENTENCIA: 11 de Diciembre de 1984

Antecedentes normativos

- Constitución Nacional
  - Reforma 1994

HABEAS DATA

LEY 25.326

DE PROTECCIÓN DE DATOS PERSONALES

OBJETO

Protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, CN. Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.

Datos personales

- *Información susceptible de ser atribuida a una persona*

- *Información de cualquier tipo referida a personas humanas determinadas o determinables, inclusive los datos biométricos.*

- *Disociación de datos:*

  Permite separar los datos de un sujeto en particular (Estadísticas, censos, encuestas anónimas, etc)

Archivo, registro, base o banco de datos

- Designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso

Titular de los datos

- Toda persona cuyos datos sean objeto del tratamiento al que se refiere la ley.

Tratamiento de datos

- Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Principios tratamiento datos personales

- Licitud
- Finalidad
- Lealtad y transparencia
- Minimización de datos. Pertinencia
- Exactitud

Licitud

- La recolección de datos debe tener un fin legalmente válido
- Aspectos vida personal que deben preservarse
- Datos personales incluyen:
  - *Texto*
  - *Imagen*
  - *sonido*

Lealtad

- Cuando el responsable se abstenga de tratar los datos personales a través de medios engañosos o fraudulentos

Finalidad

- Debe ser explícita
- Fines determinados y legítimos
- No pueden utilizarse los datos para una finalidad distinta o incompatible con la expresada en la recolección
- Salvo, para fines estadísticos o históricos, encuestas anónimas, etc)

Minimización de datos. Pertinencia

- *Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que fueron recolectados.*

Exactitud

- Deben ser tratados de modo que sean exactos y completos.

- Ambigüedad - equivocidad

Proyecto 2018

- ***Limitación del plazo de conservación***

Los datos personales no deben ser mantenidos más allá del tiempo estrictamente necesario para el cumplimiento de la finalidad del tratamiento

Proyecto 2018

- *Períodos más largos*
  - *Exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos.*

Proyecto 2018. LICITUD

- *a. El titular de los datos dé su consentimiento para el tratamiento de sus datos para uno o varios fines específicos*
- *b. El tratamiento de datos se realice sobre datos que figuren en fuentes de acceso público irrestricto;*
- *c. El tratamiento de datos se realice en ejercicio de funciones propias de los poderes del Estado y sean necesarios para el cumplimiento estricto de sus competencias;*

Proyecto 2018. LICITUD

- *d. El tratamiento de datos sea necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*
- *e. El tratamiento de datos derive de una relación jurídica entre el titular de los datos y el responsable del tratamiento, y resulte necesario para su desarrollo o cumplimiento;*

Proyecto 2018. LICITUD

- *f. El tratamiento de datos resulte necesario para salvaguardar el interés vital del titular de los datos o de terceros, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del titular de los datos, y el titular de los datos esté física o jurídicamente incapacitado para dar su consentimiento;*

Proyecto 2018. LICITUD

- *g. El tratamiento de datos sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos del titular de los datos, en particular cuando el titular sea un niño, niña o adolescente.*

Proyecto 2018. CONSENTIMIENTO

- *Libre e informado*
- *Puede ser obtenido de forma expresa o tácita*
  - ***Expreso:*** *o por escrito, verbalmente, por medios electrónicos, así como por cualquier forma similar que la tecnología permita brindar.*
  - ***Tácito:*** *cuando surja de manera manifiesta del contexto del tratamiento de datos y la conducta del titular de los datos sea suficiente para demostrar la existencia de su autorización*

Proyecto 2018

Principio de responsabilidad proactiva.

El responsable o encargado del tratamiento debe adoptar las medidas técnicas y organizativas apropiadas a fin de garantizar un tratamiento adecuado de los datos personales y el cumplimiento de las obligaciones dispuestas por la presente ley, y que le permitan demostrar a la autoridad de control su efectiva implementación.

Consentimiento

- No es necesario cuando:
  - *Los datos se obtengan de fuentes de acceso público irrestricto*
  - *Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal*
  - *Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio*

Proyecto 2018: agrega correo electrónico e información crediticia

Datos sensibles

- *Datos personales que afectan la esfera íntima de su titular con potencialidad de originar discriminación.*

Datos sensibles

- *Datos que revelen*
  - Origen racial o étnico
  - Opiniones políticas
  - Convicciones religiosas, filosóficas o morales
  - Afiliación sindical
  - Relativos a salud
  - Relativos a sexualidad

Datos sensibles

Fundamento

Sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

Datos sensibles

Está prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles.

Proyecto 2018. TRATAMIENTO

- Consentimiento expreso del titular.
- Sea necesario para salvaguardar el interés vital del titular de los datos y éste se encuentre física o legalmente incapacitado para prestar el consentimiento.
- Sea efectuado por establecimientos sanitarios públicos o privados o por profesionales vinculados a la ciencia de la salud en el marco de un tratamiento médico específico.
- Se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- Se refiera a datos personales que el interesado haya hecho manifiestamente públicos.
- Razones de interés público en el ámbito de la salud pública o asistencia humanitaria en casos de desastres naturales.

Proyecto 2018. Tratamiento antecedente penales

- Tratamiento de datos relativos a antecedentes penales o contravencionales con el objeto de brindar informes a terceros sólo puede ser realizado por parte de las autoridades públicas competentes o bajo su supervisión.
- *El empleador que conserve un certificado, documento o información de antecedentes penales o contravencionales de sus empleados no puede cederlo a terceros, salvo con el consentimiento expreso del titular de los datos.*

Proyecto 2018. Datos de menores

En el tratamiento de datos personales de un niño, niña o adolescente, se debe privilegiar la protección del interés superior de éstos, conforme a la CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO y demás instrumentos internacionales que busquen su bienestar y protección integral

Es válido el consentimiento de un niño, niña o adolescente cuando se aplique al tratamiento de datos vinculados a la utilización de servicios de la sociedad de la información específicamente diseñados o aptos para ellos. En estos casos, el consentimiento es lícito si el niño, niña o adolescente tiene como mínimo TRECE (13) años.

Confidencialidad

- El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.
- El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.

Seguridad

- Otro principio es el de seguridad datos
- 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.

Proyecto 2018. Seguridad

- Considerar:
- *a) el riesgo inherente por el tipo de dato personal;*
- *b) el carácter sensible de los datos personales tratados;*
- *c) el desarrollo tecnológico;*
- *d) las posibles consecuencias de un incidente de seguridad para los titulares de los datos;*
- *e) los incidentes de seguridad previos ocurridos en los sistemas de tratamiento.*

Proyecto 2018. Incidentes

- ***Notificación de incidentes de seguridad a la autoridad de control . 72 horas***
- *La naturaleza del incidente*
- *Datos personales que pueden estimarse comprometidos*
- *Las acciones correctivas realizadas de forma inmediata*
- *Las recomendaciones al titular de los datos acerca de las medidas que éste pueda adoptar para proteger sus intereses*
- *Los medios a disposición del titular de los datos para obtener mayor información al respecto.*

Cesión

- Previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo
- El responsable del tratamiento a quien se ceden los datos personales queda sujeto a las mismas obligaciones legales y reglamentarias que el responsable cedente.

Cesión. Consentimiento

- Es revocable.
- El consentimiento no es exigido cuando:
  - *Así lo disponga una ley;*
  - *En los supuestos de datos públicos*
  - *Se realice entre dependencias de los órganos del Estado en forma directa.*

Cesión. Consentimiento

- *Se trate de datos personales relativos a la salud, y sea necesario por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados;*
- *Se hubiera aplicado un procedimiento de disociación de la información, de modo que los titulares de los datos sean inidentificables.*

Transferencia internacional de datos

- Prohibición de transferir datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

Transferencia internacional de datos

- No se requiere consentimiento:
- Colaboración judicial internacional.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos de la ley.
- Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable

Transferencia internacional de datos

- Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;
- Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico.

Proyecto 2018. Medios tecnológicos tercerizados

- Está permitido se garantice el cumplimiento de los principios y obligaciones establecidos en la Ley.
- El responsable del tratamiento debe realizar esfuerzos razonables para elegir un proveedor de servicios que garantice el cumplimiento de la Ley.
  - *El responsable del tratamiento responderá ante el titular de los datos y ante la autoridad de control por incumplimientos del proveedor.*
- El responsable del tratamiento debe realizar esfuerzos razonables para controlar que el proveedor del servicio de tratamiento de datos personales por medios tecnológicos tercerizados:

Proyecto 2018. Medios tecnológicos tercerizados

- El responsable del tratamiento debe realizar esfuerzos razonables para controlar que el proveedor

- **a. Cuente con una política de protección de datos personales o condiciones de servicio que no sean incompatibles con las disposiciones previstas en la Ley**
- **b. Informe los tipos de subcontrataciones que involucren los datos personales objeto del tratamiento sobre el que se presta el servicio, notificando al responsable del tratamiento de cualquier cambio que se produzca;**
- **c. No incluya condiciones en la prestación del servicio que lo autoricen o permitan asumir la titularidad sobre las bases de datos tratados bajo esta modalidad**

Conocimiento – Derecho acceso

- El conocimiento de la información personal que otros tienen sobre cada uno de nosotros, implica
  - *Derecho de acceso a esa información*
  - *Derecho a tener copia en soporte accesible y legible para el interesado*
  - *Eventual pedido rectificación, actualización, cancelación o confidencialidad*
- Art. 43 párrafo 3° Const. Nac. (1994) –Hábeas data -

Amplitud en la información

- Todos los datos
- Aun los no solicitados
- No puede revelar datos sobre terceros
  - *Comp.Dir.CE 46/95- Reglam.LORTAD*

Rectificación

- Datos falsos - Inexactos
- Datos desactualizados
- Datos discriminatorios
- Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable del tratamiento debe bloquear el dato, o bien consignar, al proveer información relativa a éste, la circunstancia de que se encuentra sometido a revisión.

Proyecto 2018. Oposición

- *Oponerse al tratamiento de sus datos o de una finalidad específica de éste, cuando no haya prestado consentimiento.*
- *Responsable*
  - *Debe dejar de tratar los datos personales objeto de oposición salvo que existan motivos legítimos para el tratamiento que prevalezcan sobre los derechos del titular de los datos.*

Proyecto 2018. Supresión

- *Los datos personales ya no sean necesarios en relación con los fines para los que fueron recolectados*
- *El titular de los datos revoque el consentimiento en que se basa el tratamiento de datos y éste no se ampare en otro fundamento jurídico*
- *El titular de los datos haya ejercido su derecho de oposición, y no prevalezcan otros motivos legítimos para el tratamiento de sus datos*
- *Los datos personales hayan sido tratados ilícitamente;*

Proyecto 2018. Supresión

- *Los datos personales deban suprimirse para el cumplimiento de una obligación legal.*
- ***NO PROCEDERÁ CUANDO***
  - *Pudiese causar perjuicios a derechos o intereses legítimos de terceros*
  - *Prevalezcan razones de interés público*
  - *Los datos deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las contractuales entre el responsable o encargado del tratamiento y el titular de los datos*
  - *El tratamiento de datos sea necesario para ejercer el derecho a la libertad de expresión e información.*

Vías para hacerlo efectivo

- Administrativas o prejudiciales
- Judiciales (hábeas data, amparo,etc)
  - *Ley 25326 (arts. 13 y 14)*
    - Leyes provinciales (Chacom Chubut,Río Negro, Neuquén, Sgo del Estero, Jujuy, Entre Ríos, Constitución Salta, etc.

Legitimación

- Activa
  - *Titular de los datos*
  - *Interpretación amplia: caso "Urteaga"*
- Pasiva
  - *Responsable banco datos*
  - *Usuarios banco datos*

Procedimiento

- Plazo 10 días hábiles para responder intimación
- Gratuidad (solo cada seis meses)
- Acreditar identidad
- Motivos por los que cree el intimado tiene sus datos

Claridad en la información

- Clara
- Sin codificaciones
- Explicada en lenguaje accesible nivel medio población

Forma (medios de proporcionarla)

- Escrita
- Verbal
- Soporte electrónico
- Videos, etc

Calidad de los datos

- Ciertos
- Adecuados
- Informes comerciales y patrimoniales:
  - *"significativos para evaluar solvencia"*
  - *Inobservancia o inadecuada interpretación Normas del Banco Central*

Informes comerciales y patrimoniales

Dos tipos de datos personales de carácter patrimonial

- Relativos a la solvencia económica y al crédito
  - Obtenidos de fuentes accesibles al público
  - De informaciones del interesado o con su consentimiento.

- Relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial
  - Facilitados por el acreedor o por quien actúe por su cuenta o interés.

"significativos para evaluar solvencia"

- Los datos que pueden tratarse deben ser significativos para evaluar la solvencia económico-financiera de los afectados

  - *durante los últimos 5 años*

  - *O 2 años (obligación extinguida), debiéndose hacer constar dicho hecho*

Proyecto 2018. Información significativa:

- *a. El momento en que se produce la mora del deudor;*
- *b. Las modificaciones en las clasificaciones que otorgan al deudor las entidades crediticias;*
- *c. El inicio de la acción judicial de cobro;*
- *d. La sentencia judicial que dispone el pago de la deuda;*

Proyecto 2018. Información significativa

- *e. La fecha de la apertura del concurso de acreedores o de la declaración de quiebra*
- *f. Aquella otra información que defina el órgano de control.*

- ***No se considera última información significativa si se trata de una mera repetición de la misma información***

Derecho a Información

- El responsable o usuario del banco de datos, le comunicará, a su solicitud, al titular de los datos:
  - *las informaciones, evaluaciones y apreciaciones que sobre él hayan comunicado últimos seis meses (12 meses)*
  - *nombre y domicilio del cesionario (cuando sean datos obtenidos por cesión)*

Proyecto 2018. Información significativa

- *Cuando se deniegue al titular de los datos la celebración de un contrato, solicitud de trabajo, servicio, crédito comercial o financiero, sustentado en un informe crediticio, deberá informársele tal circunstancia, así como la empresa que proveyó dicho informe y hacerle entrega de una copia de éste.*

Denominación del deudor[1]	Entidad[2]	Periodo[3]	Situación[4]	Monto[5]	Días de atraso[6]	Observaciones[7]
ESPOSITO MARIA DELIA	BANCO SANTANDER RIO S.A.	04/18	1	172	N/A	-
ESPOSITO MARIA DELIA	BANCO ITAU ARGENTINA S.A.	04/18	1	27	N/A	-
ESPOSITO MARIA DELIA	INDUSTRIAL AND COMMERCIAL BANK OF CHINA	04/18	1	6	N/A	-

Conservación de datos

- Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

Sanciones Administrativas

- Inobservancia de la ley.
- Responsables o usuarios de archivos, registros, bases o bancos de datos públicos, y privados destinados a dar información, se hubieren inscripto o no en el registro correspondiente.

Proyecto 2018. Información significativa

- *a. Apercibimiento;*
- *b. Multa de hasta el equivalente a QUINIENTOS (500) Salarios Mínimos Vitales y Móviles.*
- *c. Suspensión de las actividades relacionadas con el tratamiento de datos hasta por SEIS(6) meses;*
- *d. Cierre temporal de las operaciones relacionadas con el tratamiento de datos una vez transcurrido el término de suspensión sin que se hubieren adoptado las medidas correctivas ordenadas.*
- *e. Cierre inmediato y definitivo de la operación que involucre el tratamiento de datos sensibles.*

Sanciones Penales

Reglamento General de Protección de Datos (RGPD) Unión Europea

Obtención de datos personales

- Establece un estándar más alto para la recopilación de datos personales. Por defecto, cada vez que una empresa quiera obtener información de un ciudadano de la UE, **primero necesitará su consentimiento explícito.**

Reglamento General de Protección de Datos (RGPD) Unión Europea

Obtención de datos personales

Aplicación de los principios de

- *Privacidad por defecto*
  - *Los datos personales no sean accesibles, sin la intervención de la persona*
- *Privacidad desde el diseño*
  - *Que la protección de datos esté presente desde las primeras fases de desarrollo y no sea una capa añadida a un producto o sistema*

Reglamento General de Protección de Datos (RGPD) Unión Europea

Medidas de seguridad

- Las compañías deben crear mecanismos de certificación definidos por ley, con el fin de disminuir el riesgo legal e incrementar la confianza de los usuarios.

Reglamento General de Protección de Datos (RGPD) Unión Europea

Conservación

- Los datos deben conservarse durante el menor tiempo posible. Este plazo debe tener en cuenta los motivos por los que se necesita el tratamiento de los datos, así como las obligaciones legales de conservar los datos durante un tiempo determinado.
- Solo se podrán conservar aquellos datos que estén actualizados.

Reglamento General de Protección de Datos (RGPD) Unión Europea

Sanciones por incumplimiento

- Multas
- 10 millones de euros o el 2% del volumen de negocio total anual.
- 20 millones de euros o el 4% del volumen de negocio total anual global (Multinacionales).

Impacto en Argentina

- Alcanza a cualquier empresa u organización que almacene datos digitales de ciudadanos de la unión europea.

Agencia de Acceso a la Información Pública

- Órgano de control creado en el ámbito Nacional, para la efectiva protección de los datos personales.

- Tiene a su cargo el Registro de las Bases de Datos.
  - Es el medio que la ley otorga para conocer y controlar a los registros, archivos, bases o bancos de datos que traten datos personales

INSCRIPCIÓN

- Toda base de datos pública y privada destinada a proporcionar informes.

- Bases de datos que no sean para un uso exclusivamente personal.

Destinado a dar informes

- Aquel registro, archivo, base o banco de datos que permita obtener información sobre las personas, se transmitan o no a terceros

VIDEOVIGILANCIA

- Una imagen o registro fílmico constituyen, a los efectos de la Ley N° 25.326, un dato de carácter personal, en tanto que una persona pueda ser determinada o determinable...".

VIDEOVIGILANCIA

- La base de datos de videovigilancia debe ser declarada.

VIDEOVIGILANCIA

- **Manual de videovigilancia**
- Forma de la recolección.
- Referencia de los lugares, fechas y horarios en los que se prevé que operarán.
- Plazo de conservación de los datos.
- Mecanismos técnicos de seguridad y confidencialidad previstos.

VIDEOVIGILANCIA

- Medidas dispuestas para el cumplimiento de los derechos del titular del dato contemplados en los artículos 14, 15 y 16 de la Ley 25326.

- Los argumentos que justifiquen la toma de fotografías para el ingreso al predio, en caso de disponerse dicha medida de seguridad.

VIDEOVIGILANCIA

- **Informar previamente al público**
  - *La existencia de cámaras de seguridad (sin que sea necesario precisar su ubicación puntual).*
  - *Los fines para los que se captan las imágenes.*
  - *Los datos de contacto del responsable de la base de datos, para que las personas puedan ejercer sus derechos como titulares de datos personales.*

OTROS REQUISITOS

- Manual de seguridad adecuado
- Política de privacidad.

Política de privacidad.

- Definición del Objeto de la política de Protección de Datos Personales

- Definición de términos de la política

- Principios de protección de datos personales de la política aplicables a la empresa

Política de privacidad.

- Confidencialidad de los datos personales, con referencia a los convenios de confidencialidad del personal y terceros que presten servicios.
- Seguridad de los datos personales
- Transferencia Internacional de datos personales

Política de privacidad.

- Publicidad directa
- Prestaciones de servicios de tratamiento de datos por cuenta de terceros
- Derechos de los titulares de los datos (personal, clientes y proveedores) y procedimientos para responder a su ejercicio.

Disposición 18/2015

"GUIA DE BUENAS PRACTICAS EN PRIVACIDAD PARA EL DESARROLLO DE APLICACIONES"

Objeto

- Brindar las herramientas necesarias para facilitar que todos los actores involucrados en el desarrollo de aplicaciones contemplen la protección de datos personales como un aspecto fundamental en el diseño de los programas de software.

Guía. Consentimiento

- 1) INTRODUCCIÓN

- 2) PRINCIPIOS DE PRIVACIDAD

- a. **Consentimiento del titular de los datos.**

Recaba el consentimiento de los titulares, y al mismo tiempo infórmales que estarás recabando su información y los usos que le darás.

Finalidad

b. Finalidad

Los datos que tus aplicaciones recolecten sólo pueden ser utilizados conforme a la finalidad que originó la recolección. Si la aplicación que desarrollas está destinada a la gestión contable de un comercio, la información personal que se recabe puede utilizarse para llevar la contabilidad, liquidar impuestos, llevar inventarios y todas las finalidades compatibles a una gestión contable, pero no podría utilizarse para llevar adelante una campaña publicitaria, porque se estaría cambiando la finalidad del tratamiento.

Calidad

c. Calidad de los datos

Los datos personales que tus aplicaciones recaben y almacenen deben ser ciertos, adecuados, pertinentes y no excesivos en relación a la finalidad que motivaron su recolección. No pueden ser obtenidos por medios desleales o fraudulentos y deben ser destruidos cuando hayan dejado de ser útiles. Además tenés la obligación de almacenarlos de manera tal que se facilite el ejercicio de los derechos de sus titulares.

Seguridad

d. Seguridad

La seguridad de la información es un aspecto importante de la protección de datos.

Evalúa los riesgos de seguridad que tu aplicación puede aparejar, teniendo en cuenta la sensibilidad de la información personal que recolecta y almacena.

Verifica que tu aplicación, si utiliza datos personales, respete las mejores prácticas en seguridad de la información.

Confidencialidad

e. Confidencialidad

Los datos personales de los que tomes conocimiento por el tratamiento que realices son confidenciales. Está prohibido revelarlos.

Esta obligación alcanza a cualquier persona que intervenga en cualquier etapa del desarrollo e inclusive subsiste aun finalizada la relación contractual.

Privacidad aplicada al desarrollo

- 3) PRIVACIDAD APLICADA AL DESARROLLO

- a. **Los OCHO (8) pasos básicos para desarrollar resguardando la privacidad**

i. Contempla la privacidad en todos los procesos de tu organización

ii. Desarrolla las aplicaciones con el concepto de “Privacidad desde el Diseño”.

Privacidad aplicada al desarrollo

- Privacy by design
- “Privacidad desde el diseño” es un enfoque en el que desde el origen mismo del diseño de un sistema, aplicación o dispositivo se contempla la protección de la privacidad. Desde esta perspectiva, la preocupación por la protección de los datos personales no debe ser analizada posteriormente a la finalización del desarrollo, como si se tratara de un anexo, sino que debe estar presente en todas las etapas del proceso. La privacidad debe ser considerada en todas las fases del ciclo de vida del sistema, aplicación o dispositivo

Privacidad aplicada al desarrollo

iii. Establece una Política de Privacidad clara y fácilmente accesible por los titulares del dato.

iv. Configura por defecto como “activadas” las opciones de privacidad.

Privacy by default

Es un concepto de desarrollo de software que establece que la configuración de la privacidad debe estar activada de manera predeterminada, de manera tal que implique un acto de voluntad del titular desactivar o compartir información personal.

Privacidad aplicada al desarrollo

v. Permite a los titulares del dato que elijan y controlen.

vi. Limita la cantidad de datos que recolectas o retienes. No recolectes o almacenes información personal que tu sistema, aplicación o dispositivo no necesite. Controla no recolectar o almacenar datos sensibles salvo que estés autorizado a hacerlo. Establece una política para la eliminación de datos personales que ya no te sean útiles.

Privacidad aplicada al desarrollo

vii. Asegura los datos personales recabados.

viii. Asume la responsabilidad. Designa a un "responsable de privacidad" o asume vos mismo la responsabilidad del resguardo de los datos personales que hayas tratado.

Privacidad aplicada al desarrollo

Privacy-Enhancing Technologies (PET)

Se trata de un sistema de medidas, herramientas y aplicaciones que protegen la privacidad de la información mediante la eliminación o minimización de los datos personales.

De ese modo se previene el procesamiento innecesario o indeseado de datos personales, sin la pérdida de la funcionalidad del sistema de información.

Privacy-Enhancing Technologies

i. Herramientas de gestión de la privacidad, que permitan al titular elegir y controlar la forma en que sus datos son recolectados y usados.

ii. Herramientas de protección de la privacidad

1. *Disociación de datos*
2. *Seudonimización*
3. *Seguridad de la información*
4. *Metadatos*
5. *Encriptación*

Aspectos técnicos para aplicaciones

- **Aspectos técnicos para aplicaciones**
- Correcta utilización de los permisos
- Si se trata de una aplicación móvil, verifica que los permisos que requiere sean los estrictamente necesarios para el funcionamiento adecuado. Las personas guardan en sus dispositivos móviles información muy personal, y una mala administración de los permisos los dejará vulnerables. Un ejemplo típico del mal uso de los permisos es una aplicación de linterna que requiera acceso a los contactos del titular del dato o a su calendario.

Geolocalización

ii. Geolocalización

Si tu aplicación accede a datos de localización, debes notificar y obtener el permiso del titular del dato, incluso si se trata de metadatos de geolocalización de fotos o videos.

Política de privacidad

- **a. Establecimiento de una Política de Privacidad.**
- Que explique claramente qué tipo de información se recaba, cómo se usa y con quién la compartes.
- Simple y, en la medida de lo posible, estandarizada, de manera tal que se facilite su lectura y comprensión por parte de los titulares de datos.

Política de privacidad

- **a. LINEAMIENTOS**

1. Debe contener una definición del Objeto de la Política de Privacidad.
2. Debes incluir una definición de los términos utilizados en la política
3. Debe reflejar los principios de protección de datos personales aplicables al tratamiento de datos que haga la aplicación

Política de privacidad

4. Si compartes o transfieres los datos con un tercero, debes notificarlo en forma destacada en tu política y cumplir con los requisitos de la cesión de datos.

5. Contemplar la confidencialidad de los datos personales (artículo 10, LPDP), con referencia a los convenios de confidencialidad del personal y terceros que presten servicios, y de cualquier otra persona u organización que puedan entrar en conocimiento de los datos personales que trata la aplicación.

Política de privacidad

6. Hacer mención a la política de seguridad de los datos personales, y la aplicación de la Disposición DNPDP N° 11/06 (manual de seguridad).
7. Contempla, en el caso que el tratamiento de datos incluya su transferencia al exterior, los

requisitos para una Transferencia Internacional de datos personales.

8. En el caso que el uso de la información personal incluya la finalidad de publicidad, debe

contemplarse el cumplimiento de las obligaciones específicas para este tipo de tratamiento

Política de privacidad

9. Prestaciones de servicios de tratamiento de datos por cuenta de terceros.

10. Establece el procedimiento para cumplir con los derechos de los titulares de los datos (derechos de acceso, rectificación, supresión y bloqueo).

11. Comunica mediante la Política quien es el Encargado de Protección de Datos

Control de la información

- 5) CONTROL DE LA INFORMACIÓN PERSONAL POR PARTE DE SUS TITULARES

- Bríndales a quienes hagan uso de tus aplicaciones y a los titulares de los datos en general el control de su información personal, particularmente cuando se trata de información sensible, íntima o cuando se le den usos que no sean los obvios o comunes.

Aplicaciones móviles

- 6) APLICACIONES MÓVILES

- Las aplicaciones desarrolladas para dispositivos móviles generalmente tendrán la limitación del tamaño de la pantalla. Deberás ser creativo para poder mostrar la información de tu Política de Privacidad de una manera que le resulte útil a los titulares de datos con el desafío adicional que genera un espacio pequeño como la pantalla de un teléfono celular.

TÉCNICAS SUGERIDAS

- a. Separar la información en distintas capas.

Clasificá la información que brindas en tu Política de Privacidad, separarla en distintas capas y colocá la más importante en las capas superiores.

Luego ofrece hipervínculos para aquellos que quieran profundizar más y conocer los detalles.

Aplicaciones móviles

- b. Proveer al titular del dato un tablero de privacidad

Podría ser útil ofrecer una herramienta de configuración de privacidad, con un diseño atractivo y amigable que le permita al titular del dato elegir fácilmente las opciones de privacidad.

Aplicaciones móviles

- c. Utilizar técnicas para llamar la atención del titular del dato.

    1. *Gráficos*

    2. *Colores*

    3. *Sonidos*

Uso de aplicaciones por niños

- 7) USO DE APLICACIONES POR NIÑOS

- Si tu aplicación puede ser usada por niños o adolescentes, deberás procurar un cuidado especial.

- Son una población vulnerable, y por lo tanto, será necesario que incorpores salvaguardas especiales para resguardarlos.

Uso de aplicaciones por niños

- - Limita al máximo el tipo y la cantidad de información que sobre ellos recolectas.

- - Contempla estrictas medidas de seguridad sobre la información que necesariamente debas recabar.

- - Evita compartir información personal de menores con terceros.

Uso de aplicaciones por niños

- - Bríndales información adecuada a su nivel de comprensión sobre el uso responsable de sus datos y alerta sobre los peligros que se relacionan a una mala utilización.
- Siempre que corresponda, obtén el consentimiento de sus padres. Establece mecanismos de resguardos para mantenerlos informados acerca de los usos que se hacen de la información personal de los menores.

Otras consideraciones

- Mencionar contacto con la Agencia de Acceso a la Información Pública

- Ley aplicable