COMPILADO DE APUNTES

ACTIVIDAD PROFESIONAL – LICENCIATURA EN CIENCIAS DE LA COMPUTACIÓN

PROTECCIÓN DE DATOS PERSONALES – ACCESO A LA INFORMACIÓN – PRIVACIDAD DE DATOS

Abog. Ana Tancredi

En general, la privacidad de los datos significa la capacidad de una persona para determinar por sí misma cuándo, cómo y hasta qué punto se comparte o se comunica a otros su información personal. Esta información personal puede ser el nombre, la ubicación, la información de contacto o el comportamiento en línea o en el mundo real. Al igual que alguien puede querer excluir a personas de una conversación privada, muchos usuarios de Internet quieren controlar o evitar que se recopilen ciertos tipos de datos personales.

¿Por qué es importante la privacidad de los datos?

La privacidad se considera un derecho humano fundamental, y las leyes de protección de datos existen para proteger ese derecho. La privacidad de los datos también es importante, porque para que las personas estén dispuestas a participar en Internet, tienen que confiar en que sus datos personales se tratarán de la forma adecuada. Las organizaciones utilizan las prácticas de protección de datos (Política de Privacidad de Datos, por ejemplo) para demostrar a sus clientes y usuarios que pueden confiar en ellos para tratar sus datos personales.

Los datos personales se pueden utilizar de forma indebida de varias maneras si no se mantienen privados o si las personas no tienen la capacidad de controlar cómo se utiliza su información los delincuentes pueden usar los datos personales para estafar o acosar a los usuarios. Las entidades pueden vender datos personales a anunciantes u otras partes externas sin el consentimiento del usuario, lo cual puede provocar que los usuarios reciban marketing o publicidad no deseados. Cuando se rastrean y vigilan las actividades de una persona, esto puede restringir su capacidad de expresarse con libertad, especialmente en estados con gobiernos represivos.

Para los individuos, cualquiera de estos resultados puede resultar perjudicial. Para una empresa, podrían dañar irremediablemente su reputación, además de acarrear multas, sanciones y otras consecuencias legales.

Además de las implicaciones en el mundo real que tienen las vulneraciones de la privacidad, muchas personas y países sostienen que la privacidad tiene un valor intrínseco: que la privacidad es un derecho humano fundamental en una sociedad libre, al igual que el derecho a la libertad de expresión.

A medida que los avances tecnológicos han mejorado la capacidad de recopilación de datos y de vigilancia, los gobiernos de todo el mundo han empezado a aprobar leyes que regulan los tipos de datos que se pueden recopilar sobre los usuarios, cómo se pueden utilizar, y cómo se deben almacenar y proteger.

Sin embargo, muchos defensores de la privacidad argumentan que las personas todavía no tienen suficiente control sobre lo que ocurre con sus datos personales. Es posible que los gobiernos de todo el mundo vayan aprobando diferentes leyes de privacidad de datos en el futuro.

REGULACIÓN NORMATIVA

1. **Constitución Nacional**

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

Art. 43.- "*Toda persona puede interponer acción expedita y rápida de amparo, siempre que no exista otro medio judicial más idóneo, contra todo acto u omisión de autoridades públicas o de particulares, que en forma actual o inminente lesione, restrinja, altere o amenace, con arbitrariedad o ilegalidad manifiesta, derechos y garantías reconocidos por esta Constitución, un tratado o una ley. En el caso, el juez podrá declarar la inconstitucionalidad de la norma en que se funde el acto u omisión lesiva.*

Podrán interponer esta acción contra cualquier forma de discriminación y en lo relativo a los derechos que protegen al ambiente, a la competencia, al usuario y al consumidor, así como a los derechos de incidencia colectiva en general, el afectado, el defensor del pueblo y las asociaciones que propendan a esos fines, registradas conforme a la ley, la que determinará los requisitos y formas de su organización.

Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística.

Cuando el derecho lesionado, restringido, alterado o amenazado fuera la libertad física, o en caso de agravamiento ilegítimo en la forma o condiciones de detención, o en el de desaparición forzada de personas, la acción de hábeas corpus podrá ser interpuesta por el afectado o por cualquiera en su favor y el juez resolverá de inmediato, aun durante la vigencia del estado de sitio".

2. **Ley N° 25.326 de Protección de Datos Personales y su Decreto Reglamentario N° 1558/2001**

Define y determina los principios rectores que deben cumplirse para la protección de los datos personales, definiéndolos y diferenciándolos de los datos sensibles. También establece los alcances del tratamiento de datos y las obligaciones de los sujetos responsables, así como los derechos de los titulares de los datos personales.

Profundizaremos acerca de esta ley más adelante.

La Dirección Nacional de Registros de Datos Personales fue el organismo creado como autoridad de aplicación, el que fue reemplazado por la Agencia de Acceso a la Información Pública.

3. **Ley N° 27275 de Acceso a la Información Pública y su Decreto Reglamentario N° 206/2017**

Crea la Agencia de Acceso a al Información Pública como órgano de control de la ley de Datos personales y de Acceso a la Información pública. Ambos son derechos fundamentales y están inmersos en los Tratados Internacionales, la Corte Interamericana de DDHH fue pionera en declarar al acceso a la información pública como derecho humano, constitucionalizados desde 1994 a través también de la agregación del art 43 CN. Antes de la Reforma vimos que también los datos personales estaban protegidos a través del art 19 CN ya que se encuentra incluido en el Derecho a la Intimidad, a la privacidad.

La Agencia de Acceso a la Información Pública. Es un ente autárquico que funciona en el ámbito de la Jefatura de Gabinete de Ministros. Esta Agencia debe controlar la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, públicos o privados, destinados a dar informes. Debe garantizar el derecho al honor y a la intimidad de las personas y el acceso a la información.

Esta Agencia es el órgano administrativo dispuesto para el control de estas leyes y además es el responsable de velar por la Transparencia Activa de la gestión pública y de promover una cultura respetuosa de la privacidad.

(https://www.argentina.gob.ar/aaip)

El procedimiento del acceso a la información Publica y el Registro de Bases de datos de carácter privado se llevan a cabo a través de este organismo.

4. **Convenio 108 +. Ley 27.699 Protocolo modificatorio del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal**

Luego de haber sido aprobado el Convenio 108+ por parte de la Honorable Cámara de Diputados de la Nación el día 10 de noviembre de 2022, se promulgó la Ley 27.699 de Protección de las Personas con respecto al tratamiento automatizado de datos de carácter personal, publicada en el Boletín Oficial.

La Agencia de Acceso a la Información Pública impulsó la sanción y fue precursora al dictar distintas disposiciones a fin de alcanzar los parámetros del Convenio modernizado, en pos de dar respuesta a los nuevos desafíos que imponen las transformaciones tecnológicas y el desarrollo de la economía digital.

El Convenio 108+ es una versión modernizada del Convenio 108, suscripto en 1981 en la ciudad de Estrasburgo (Francia) y constituye el único instrumento multilateral de carácter vinculante en materia de protección de datos personales, que tiene por objeto proteger la privacidad de los individuos contra posibles abusos en el tratamiento de sus datos.

Argentina es parte del Convenio 108 desde el 1 de junio de 2019 y es el país número 33 en firmar el Convenio 108 modernizado.

Estos Convenios se firmaron para garantizar a todas las personas el respeto de sus derechos y libertades fundamentales, especialmente el derecho a la vida privada. La protección alcanza a

todas las personas que están en el territorio de alguno de los Estados parte del Convenio, sin que importe su nacionalidad o país de residencia.

Algunos de los puntos más destacados de la versión actualizada del Convenio 108+ son:

- Se reconocen nuevos derechos para los titulares de datos.
- Se actualizan los mecanismos de transferencias internacionales.
- Se amplía el concepto de datos sensibles, pasando a incluir datos genéticos y biométricos.
- Se obliga a informar incidentes de seguridad.
- Se incorporan requisitos más estrictos respecto a los principios generales sobre tratamiento de datos, como el principio de proporcionalidad, de minimización de datos y licitud.
- Se Incluye condiciones especiales para el tratamiento de datos personales de niños y niñas.
- Se refuerza la exigencia de la destrucción o anonimización de datos personales.

Tratamiento automatizado de datos personales

Cuando los datos personales están en un fichero automatizado, son datos que pueden ser tratados en forma automatizada. Por ejemplo: registro de datos; aplicación de operaciones lógicas aritméticas a esos datos; modificación de datos; borrado de datos; extracción de datos; difusión de datos.

Los Estados parte del Convenio están obligados a aplicar sus normas tanto a los ficheros de datos públicos como privados.

Obligaciones en el tratamiento automatizado de datos personales

Respecto del *tipo de datos* que puede registrarse, las obligaciones son:

- los datos registrados deben ser adecuados, pertinentes y no excesivos en relación con la finalidad para la que se registraron;
- los datos deben ser exactos y estar actualizados;
- los datos deben ser conservados de una manera que permita identificar a la persona dueña de esos datos por un tiempo no mayor al necesario para cumplir la finalidad del registro.

Respecto del *tratamiento de datos*, las obligaciones son:

- obtener y tratar los datos de una manera leal y legítima;
- registrar los datos para finalidades determinadas y legítimas;
- no usar los datos de manera incompatible con las finalidades para las que fueron registrados;
- tomar medidas para proteger los datos contra su posible destrucción o pérdida;
- tomar medidas para proteger los datos contra el acceso, modificación o difusión no autorizados.

No pueden ser tratados automáticamente los datos sensibles, es decir, aquellos que revelen: origen racial; opiniones políticas; convicciones religiosas o de otro tipo; datos personales relacionados con la salud; datos personales relacionados con la vida sexual; condenas penales. Estos datos sólo pueden ser tratados automáticamente cuando el derecho interno de cada país da garantías adecuadas.

Derechos de las personas con relación a sus datos personales

Cualquier persona tiene derecho a:

- conocer la existencia de un fichero automatizado de datos personales, su finalidad y la identidad de la autoridad controladora del fichero;
- obtener sin demora ni gastos excesivos información sobre si en el fichero existen datos sobre su persona. Tiene derecho a recibir información en forma clara;
- obtener la rectificación o el borrado de sus datos si fueron tratados en contra de las normas sobre protección de datos personales;
- contar con un recurso cuando no se le da la información o no se atiende su pedido de rectificación o borrado de datos.

Si el responsable de la base de datos toma decisiones basadas únicamente en el tratamiento automatizado de datos y eso perjudica al titular de los mismos, éste tiene el derecho de exigir que se le explique en forma clara la lógica que aplicó para tomar esa decisión.

Los Estados parte pueden limitar algunos de los derechos de las personas dueñas de los datos cuando es necesario por razones de seguridad, económicas o para la represión de infracciones penales.

Flujo de datos personales entre países

El Convenio prohíbe que un Estado parte niegue la transmisión de datos personales fuera de sus fronteras. Sin embargo, los países firmantes del Convenio pueden limitar la transmisión de datos personales cuando en su país esos datos tienen una protección particular. Esta excepción no puede aplicarse si el país que recibiría los datos también los protege de manera similar al país de origen.

Los Estados parte del Convenio deben asistir a cualquier persona extranjera para que pueda ejercer sus derechos de protección de datos personales.

Las personas que residen en un Estado parte pueden presentar reclamos por el tratamiento de sus datos personales en otro país por medio de la autoridad que su país designó para hacer cumplir el Convenio.

LEY DE PROTECCIÓN DE DATOS PERSONALES

1. OBJETIVOS DE LA LEY

- Protección Integral de los datos personales asentados en archivos, registros o bancos de datos Públicos o privados destinados a brindar informes; específicamente otorga la protección al "tráfico informático" de datos.
- Garantizar a las personas el control del uso de sus datos personales.

2. FINALIDAD DE LA LEY

Garantizar el derecho al honor y la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, conforme a lo establecido en el art 43 de la CN

La ley se refiere a los datos personales guardados en archivos, registros, bancos de datos públicos o privados y que están guardados para dar informes.

3. DEFINICIONES

DATOS PERSONALES

Información de cualquier tipo referido a las personas humanas o jurídicas. Puede ser cualquier tipo de información: datos de identidad, de domicilio, de deudas, etc. También por ejemplo la imagen en videos de sistema vigilancia también es un dato personal.

DATOS SENSIBLES

Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. La formación de archivos, bancos, o registros que almacenen información que revele este tipo de datos está prohibida (salvo excepciones que establece la ley).

Los datos biométricos son un tipo de dato personal obtenido por medio de un tratamiento técnico específico. Están relacionados con las características físicas, fisiológicas o de conducta de una persona humana que permiten su identificación única. Los datos genéticos son los datos referidos a las características genéticas heredadas o adquiridas de una persona humana que dan información sobre su fisiología o salud. Los datos genéticos se consideran datos personales de carácter sensible cuando identifican a una persona física y mediante esos datos se puede tener o revelar información sobre la salud o a la fisiología que pueda ser discriminatorio. Cuando los datos genéticos son datos personales de carácter sensible debe existir mayor cuidado de seguridad, confidencialidad, restricciones de acceso, uso y circulación.

Los datos biométricos que identifican a una persona son datos sensibles sólo cuando pueden revelar otros datos y el uso de esos otros datos puede provocar discriminación. Por ejemplo, cuando los datos biométricos revelan el origen étnico o dan información sobre la salud de la persona.

El Registro sobre antecedentes penales o contravencionales sólo pueden tenerlos las autoridades públicas competentes, en el marco de las leyes, ser solicitado por el interesado o por autoridad pública (juez)

ARCHIVO, REGISTRO BASE O BANCO DE DATOS

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

TRATAMIENTO DE DATOS

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

4. SUJETOS A LOS QUE REFIERE LA LEY

Titular Toda persona humana o jurídica cuyos datos sean objeto del tratamiento al que se refiere la ley

Responsable Persona humana o jurídica, pública o privada que es titular de un archivo, registro, base o banco de datos

Usuario de datos: Toda persona pública o privada que realice tratamiento de datos

5. PRINCIPIOS RECTORES PARA LA PROTECCIÓN DE DATOS PERSONALES

Pertinencia: Los datos personales que se recojan para su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos con relación al ámbito y finalidad para los que se hubieren obtenido

Finalidad: El tratamiento de los datos debe obedecer a un fin específico

Utilización no abusiva: Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención

Exactitud: Los datos deben ser exactos y actualizados en caso de que ello fuese necesario. Los datos total o parcialmente inexactos o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate

Limitación en el tiempo: Los datos deben ser destruidos cuando dejen de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados

Legalidad: La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley

Publicidad: Toda base de datos destinada al público y aquellas que exceden el uso exclusivamente personal deben inscribirse en el Registro Nacional de Bases de Datos

Control: Existencia de un organismo de control responsable del cumplimiento de la ley AAIP

Seguridad: El responsable 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, perdida, consulta o tratamiento no autorizado

Defensa de los datos sensibles: Ninguna persona puede ser obligada a proporcionarlos (con excepciones)

Consentimiento: El tratamiento de datos personales es ilícito cuando el titular no hubiere prestado su consentimiento libre, expreso, informado, el que deberá constar por escrito o por otro medio que permita se le equipare, de acuerdo con las circunstancias. El consentimiento expresado con otras declaraciones deberá figurar en forma expresa y desatacada, previa notificación al requerido de datos, de la finalidad para la que serán tratados, así como también el carácter obligatorio o facultativo de las respuestas

Excepciones al Consentimiento

La ley establece excepciones en el requerimiento previo del consentimiento del titular de los datos personales. Puede prescindirse del consentimiento cuando:

a. los datos se obtengan de fuentes de acceso público irrestricto

b. Se recaben para el ejercicio de funciones propias de los poderes del estado o en virtud de una obligación legal

c. Se trate de listados cuyos datos se limiten al nombre, DNI, identificación tributaria o previsional, ocupación, fechas de nacimiento y domicilio

d. Los datos deriven de una relación contractual, científica o profesional del titular de los datos y resulten necesarios para su desarrollo o cumplimiento

e. Se trate de ciertas obligaciones de información en operaciones financieras

6. DERECHOS DE LOS TITULARES DE DATOS PERSONALES

Oposición: Derecho a negarse a facilitar un dato de carácter personal en el caso de que no sea obligatorio hacerlo. Si bien no cuenta con un apartado especial como el resto de los derechos, la posibilidad de ejercicio se desprende del texto del inc. 1 del art 7 que expresamente reza que ninguna persona puede ser obligada a proporcionar datos sensibles.

Información: Se debe informar al momento de recolectar datos al titular:

a. la finalidad y destinatario de los datos

b. existencia de BD, identidad y domicilio del responsable

c. carácter obligatorio o facultativo de las respuestas

d. consecuencia de proporcionar datos o negativa a hacerlo

e. facultad del titular de ejercer los derechos de acceso, rectificación y supresión

Además de respetar los derechos sobre los datos personales y brindar la información solicitada, deben exhibir los derechos reconocidos por la ley en un lugar visible y de manera clara. Al exhibir la información sobre los derechos de los titulares, también tienen el deber de informar que la

Agencia de Acceso a la Información Pública es el organismo que recibe las denuncias y reclamos para proteger los datos personales. Toda esta información debe estar disponible antes de que se tomen los datos de las personas.

Acceso: Derecho del titular de los datos a solicitar y obtener información de sus datos personales incluidos en los bancos de datos. Se complementa con la obligación que se les impone a los responsables de las bases de datos de permitir el ejercicio del derecho de acceso a su titular, a fin de que cualquier persona pueda conocer no solo si sus datos personales figuran en una base de datos sino también cuales son. Este derecho es la médula de lo que comúnmente se conoce como Habeas data

Contenido de la información: La información debe ser suministrada en forma clara, exenta de codificaciones y en su caso acompañada de una explicación en lenguaje accesible al conocimiento medio de la población de los términos que se utilicen. A su vez, la información debe ser amplia y versar sobre la totalidad del registro perteneciente al titular.

Rectificación, actualización, supresión: El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales en el plazo mínimo de 5 días hábiles de recibido el reclamo. El incumplimiento de esta obligación dentro del término acordado habilitará a promover acción de hábeas data. Siempre es posible exigir que corrijan el error o actualicen la información. En caso de los datos sensibles, es posible exigir que los supriman o los mantengan en secreto. Los responsables de la base de datos deben corregir el error dentro de los 5 días hábiles de presentado el reclamo y el trámite es gratuito.

Consulta: A la AAIP para solicitar información sobre la existencia de bases de datos personales, sus finalidades e identidad de sus titulares. El responsable de la base de datos esta obligado a otorgar gratuitamente la información de los datos de quien lo requiera dentro de los 10 días corridos.

7. DEBERES Y OBLIGACIONES DE LOS TITULARES DE LOS ARCHIVOS, REGISTROS, BANCOS O BASES DE DATOS QUE CONTENGAN INFORMACIÓN PERSONAL DE LOS CIUDADANOS

Además de los derechos de defensa legalmente reconocidos a los titulares de los datos de carácter personal, la ley establece una serie de garantías específicas tendientes a asegurar su respeto, cuyo incumplimiento puede ser sancionado. Estas garantías constituyen otros tantos deberes que pesan sobre la persona del responsable del archivo, registro, banco o base de datos.

Deber de secreto: Definido también como “deber de confidencialidad”, obliga al responsable del archivo, registro, banco o base de datos y a las personas que intervengan en cualquier fase del tratamiento de datos a respetar el secreto profesional respecto de estos, exigencia que debe subsistir aun después de finalizada la relación con el titular del archivo de datos. Tiene como objetivo evitar que la información salga del círculo de personas a quienes está dirigida, habida cuenta de que sobre los archivos o bases de datos pesa una presunción de secreto.

Deber de registro: Pone en cabeza de los usuarios y responsables de los archivos, registros, bases o bancos de datos que contienen información personal, la exigencia de inscribirlos en el Registro Nacional de Bases de Datos Privadas habilitado por la AAIP. La inscripción de archivos, registros, bancos y bases de datos debe comprender como mínimo la siguiente información: a) Nombre y domicilio del responsable; b) Características y finalidad del archivo; c) Naturaleza de los datos personales contenidos en cada archivo; d) Forma de recolección y actualización de

datos; e) Destino de los datos y personas físicas o de existencia ideal a las que pueden ser transmitidos; f) Modo de interrelacionar la información registrada; g) Medios utilizados para garantizar la seguridad de los datos, debiendo detallar la categoría de personas con acceso al tratamiento de la información; h) Tiempo de conservación de los datos; i) Forma y condiciones en las que las personas pueden acceder a los datos referidos a ellas y los procedimientos a realizar para la rectificación y actualización de los datos.

Excepciones del deber de registro: Todos aquellos archivos, registros, bancos o bases de datos con fines de publicidad que se encuentren adheridos a alguna cámara, asociación y/o colegio profesional del sector que disponga de un Código de Conducta homologado por la AAIP están exceptuados de este deber. En estos casos, serán dichas cámaras, asociaciones y/o colegios profesionales quienes deberán inscribirse, acompañando una nómina con el nombre, apellido y domicilio de sus asociados, quienes, por estatuto, deberán estar obligatoriamente adheridos a dicho Código de Conducta.

Deber de información: Es la contracara del derecho de información que tienen los titulares de los datos personales. La ley exige que cuando se recolecten datos de carácter personal que requieran el consentimiento de sus titulares, el responsable del tratamiento ponga a disposición de los mismos una serie de informaciones que le permitan decidir en forma libre la conveniencia de proporcionar datos referidos a su persona. Dicha información deberá indicar qué se va a hacer con los datos, quiénes serán los destinatarios de la información y la identidad y dirección del responsable del archivo o base de datos. Este deber también es exigido en los casos de cesión de datos a terceros, oportunidad en la que el titular de los datos debe ser informado sobre la finalidad de la cesión, la identidad del cesionario y los elementos que permiten realizar dicha cesión.

Deber de seguridad: El responsable del tratamiento de datos de carácter personal debe adoptar las medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado que permitan detectar desvíos, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Deber de velar por la seguridad de los datos: Consiste en el respeto necesario por parte del responsable y los usuarios de los archivos, registros, bancos o bases de datos, de las reglas establecidas para la recepción, tratamiento, uso, conservación, almacenamiento y cesión de datos, conjugadas con los principios generales de protección de datos. De esta manera, la calidad estará medida de acuerdo a los parámetros de pertinencia, proporcionalidad, lealtad, congruencia, exactitud y accesibilidad por parte del titular de los datos.

Cumplimiento del deber de dar acceso a los datos: El responsable de un archivo, registro, banco o base de datos que almacenan datos de carácter personal debe suministrar información amplia sobre la totalidad del registro perteneciente al titular de los datos personales que solicite el acceso de los mismos. El informe debe ser claro, exento de codificaciones y, en caso de ser necesario, debe entregarse acompañado de una explicación escrita en lenguaje accesible al conocimiento medio de la población. Esta información puede suministrarse por escrito, por medios electrónicos, telefónicos, de imagen u otro medio idóneo a tal fin, a opción del titular de los datos personales, no obstante lo cual, pueden, además, ofrecerse los siguientes medios alternativos de información: visualizarse en la pantalla; informe escrito entregado en el domicilio del requerido; informe escrito remitido al domicilio denunciado por

el requirente; transmisión electrónica de la respuesta, siempre que esté garantizada la identidad del interesado y la confidencialidad, integridad y recepción de la información; cualquier otro procedimiento que sea adecuado a la configuración e implementación material del archivo, registro, base o banco de datos, ofrecido por el responsable o usuario al mismo.

No siempre se debe cumplir con el deber de dar acceso a los datos; este deber cuenta con una clara excepción que permite que los responsables o usuarios de archivos, registros, bancos o bases de datos públicos puedan denegar, mediante resolución fundada, la información solicitada por los titulares de datos de carácter personal, cuando por intermedio de ello se pudieran obstaculizar actuaciones judiciales o administrativas en curso, vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y del medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas.

Deberes de rectificación, cancelación y supresión: Después de recibir un reclamo realizado por una persona cuyos datos personales se encuentran registrados en un archivo, registro, banco o base de datos, o al advertir un error o falsedad en la información, el responsable o usuario del mismo debe proceder a la rectificación, supresión o actualización de la información registrada. Este deber es la consecuencia lógica del principio de pertinencia, pues si solo pueden tratarse los datos que sean a la finalidad que lo justifica, aquellos que hayan dejado de serlo por los motivos que fueren no pueden seguir siendo objeto de tratamiento. Existen excepciones al deber de supresión, pues este no procede cuando pudiese causar perjuicios o derechos o intereses legítimos de terceros o cuando existiera una obligación legal de conservar los datos. De la misma forma, los responsables o usuarios de los archivos, registros, bancos o bases de datos públicos pueden, mediante decisión fundada, denegar la rectificación o la supresión de los datos de carácter personal solicitada por el titular de los mismos en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

Deber de bloqueo: Es el deber que tienen los titulares de archivos, registros, bancos o bases de datos de bloquear el registro referido a una persona durante el transcurso del proceso de verificación y rectificación de los errores o falsedades que pudieran haberse denunciado, período durante el cual, en caso de proveerse información relativa al titular de los datos personales analizados, se deberá aclarar que dichos datos se encuentran sometidos a revisión.

Deber de controlar la cesión a terceros: Este deber constituye el registro último y fundamental de la pretensión legal de preservar la intimidad de los datos incorporados en archivos o bases de datos. Si bien la regla general impide ceder tales datos, la cesión puede efectuarse, siempre y cuando concurran los siguientes requisitos: consentimiento del afectado; que la cesión constituya un requisito para el cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y el cesionario; que la cesión le sea informada al titular de los datos, indicándose además la finalidad de la cesión, la identidad del cesionario y los elementos que permiten hacerlo.

Deber de información al cesionario: El responsable o usuario de un archivo, registro, banco o base de datos que proceda a rectificar, cancelar o suprimir información de carácter personal relativa a una persona que hubiera sido previamente cedida a terceros, debe notificar de esta rectificación o supresión al cesionario.

En caso de que una base de datos no cumpla con los requisitos que establece la ley para la protección de sus datos personales, o impidan al titular conocer o corregir sus datos personales, el titular podrá ejercer las siguientes acciones:

- Solicitar al responsable de los archivos o banco de datos (Preferentemente por escrito)
- Denunciar el hecho ante la Agencia Nacional de Acceso a La Información Pública
- Acción judicial HABEAS DATA (Protección de los derechos de privacidad, honor, identidad y dignidad de la persona humana)

La acción de protección procede para conocer los datos personales almacenados en archivos, registros o bases de datos públicas o privadas destinados a dar informe y para conocer su finalidad. En caso de falsedad, inexactitud, desactualización de la información de que se trate, o el tratamiento de datos cuyo registro se encuentre prohibido en la ley (información sensible) para exigir su rectificación, supresión, confidencialidad o actualización.

Las personas que pueden ejercer esta acción (Legitimados) son:

Personas Humanas: El afectado, sus tutores o sucesores en línea directa o colateral hasta el segundo grado, por sí o por apoderado

Personas Jurídicas, sus representantes legales o apoderados

Defensor del Pueblo: Interviene como participe coadyuvante (puede o no intervenir en el proceso)

PROBLEMAS A LOS QUE SE ENFRENTAN LOS USUARIOS A LA HORA DE PROTEGER SU PRIVACIDAD EN INTERNET

A medida que el uso de Internet ha ido aumentando a lo largo de los años, también lo ha hecho la importancia que tiene la privacidad de los datos. Los sitios web, las aplicaciones y las plataformas de las redes sociales a menudo necesitan recopilar y almacenar datos personales de los usuarios para poder prestar sus servicios. Sin embargo, algunas aplicaciones y plataformas pueden exceder las expectativas de los usuarios en lo que respecta a la recopilación y uso de datos, afectando a la privacidad de los usuarios mucho más de lo esperado. Puede que otras aplicaciones y plataformas no pongan las protecciones adecuadas en torno a los datos que recogen, lo que puede dar lugar a una fuga de datos que ponga en peligro la privacidad del usuario.

Sequimiento en línea: el comportamiento de los usuarios se rastrea en línea con regularidad. Las cookies suelen registrar las actividades de un usuario, y aunque la mayoría de los países exigen que los sitios web avisen a los usuarios del uso de cookies, puede que los usuarios no sean conscientes de hasta qué punto las cookies registran su actividad.

Perder el control de los datos: con tantos servicios en línea de uso común, puede que las personas no sean conscientes de cómo se comparten sus datos, más allá de los sitios web con los que interactúan en línea, y puede que no tengan capacidad de decisión sobre lo que sucede con sus datos.

Falta de transparencia: es frecuente que para utilizar aplicaciones web, los usuarios tengan que proporcionar datos personales como el nombre, correo electrónico, número de teléfono o ubicación; además, las políticas de privacidad asociadas a esas aplicaciones pueden ser densas y difíciles de entender.

Redes sociales: ahora es más fácil que nunca encontrar a alguien en línea utilizando las redes sociales, y las publicaciones en redes sociales pueden revelar más información personal de lo que los usuarios creen. Además, las plataformas de redes sociales suelen recopilar más datos de los que los usuarios son conscientes.

Ciberdelincuencia: muchos atacantes intentan robar datos de los usuarios para cometer fraudes, poner en riesgo sistemas seguros o venderlos en mercados clandestinos a grupos o personas que los utilizarán con fines maliciosos. Algunos atacantes utilizan ataques de phishing para intentar engañar a los usuarios con el fin de que revelen información personal; otros intentan poner en riesgo los sistemas internos de las empresas que contienen datos personales.

PROBLEMAS A LOS QUE SE ENFRENTAN LAS EMPRESAS A LA HORA DE PROTEGER LA PRIVACIDAD DE LOS USUARIOS

Comunicación: en ocasiones, las organizaciones tienen dificultades para comunicar con claridad a sus usuarios qué datos personales recopilan y cómo los utilizan.

Ciberdelincuencia: los atacantes se dirigen tanto a usuarios individuales como a organizaciones que recogen y almacenan datos acerca de estos usuarios. Además, a medida que más aspectos de una empresa se conectan a Internet, la superficie de ataque aumenta.

Fugas de datos: una fuga de datos puede suponer una vulneración considerable de la privacidad de los usuarios si se filtran datos personales, y los atacantes siguen perfeccionando las técnicas utilizadas para provocar dichas fugas.

Amenazas internas: los empleados internos o los proveedores podrían acceder a los datos de forma inapropiada si estos no se protegen de forma adecuada.

Algunas de las tecnologías más importantes para la privacidad de los datos son: La ***encriptación*** es una forma de ocultar información al codificarla de forma que parezcan datos aleatorios. Solo aquellos que cuenten con la clave de encriptación pueden descifrar la información.

El ***control de acceso*** garantiza que solo las partes autorizadas accedan a los sistemas y a los datos. El control de acceso se puede combinar con prevención de pérdida de datos (DLP) para impedir que los datos confidenciales salgan de la red.

La ***autenticación en dos fases*** es una de las tecnologías más importantes para los usuarios habituales, ya que dificulta que los atacantes obtengan un acceso no autorizado a las cuentas personales.

Estas son solo algunas de las tecnologías que hay disponibles en la actualidad para proteger la privacidad del usuario y mantener los datos más seguros.

COOKIES

Una *cookie* es un pequeño archivo de datos, enviado por un sitio web cuando este es visitado, que se almacena en la computadora, tableta o teléfono del usuario y recopila información sobre su navegación y comportamiento en internet.

TIPOS DE COOKIES

***Cookies* temporales o permanentes:** las temporales sólo permanecen en el navegador hasta que se abandona la página web. Las *cookies* permanentes, en cambio, quedan en el disco de la computadora para que la página que las ejecuta pueda leerlas e identificar al usuario cada vez visita la página.

***Cookies* propias o de terceros:** las propias son las que utiliza una página web y que fueron diseñadas por esa misma web. Las *cookies* de terceros se caracterizan porque son generadas por servicios o proveedores externos a la web que se visita.

***Cookies* técnicas o de preferencias:** las técnicas sirven para optimizar el funcionamiento de la web y no pueden ser desactivadas. Las *cookies* de preferencias almacenan las preferencias y configuraciones en los sitios web a los que se accedió anteriormente. Por ejemplo, para recordar el idioma predeterminado o el tipo de navegador que utiliza.

***Cookies* publicitarias o de marketing:** sirven para gestionar la publicidad que se incluye en los sitios web. A través de estas *cookies* se analiza de forma continuada tu comportamiento en la web, las páginas en las que se ingresa o las búsquedas que se realizan y se crea un perfil con los intereses del usuario, que puede venderse o cederse a anunciantes para mostrarte publicidad que pueda ser relevante para vos.

FINALIDAD DE LAS COOKIES

Las *cookies* tienen 2 funciones principales:

Recordar accesos: hacen que las páginas web puedan identificar un dispositivo con sus configuraciones y recordar al usuario y qué hizo antes dentro de ellas para ofrecer una experiencia de navegación web más fluida y dinámica.

Crear un patrón de los hábitos de navegación rastreando la actividad del usuario: ciertas *cookies* tienen usos de vigilancia más invasiva. Pueden servir para conocer los hábitos de navegación del usuario, pero también para identificarlo como usuario según las páginas que visita. Esta función es la más conflictiva porque puede afectar tu privacidad.

Las *cookies* no son peligrosas de por sí. No pueden infectar los dispositivos con virus ni otro tipo de *malware*. El principal peligro está en su capacidad de hacer un seguimiento de tu historial de navegación y afectar tu privacidad. Cuantas menos *cookies* se permiten, más privacidad puede asegurarse a la hora de navegar por internet, pero se experimentará una menor personalización en la experiencia de navegación. La principal razón para aceptarlas es que le permitirán al usuario acceder a los contenidos de los sitios más rápidamente. Es importante configurar las *cookies* y eliminarlas periódicamente.

BIBILIOGRAFÍA:

- Ley N° 25326 de Protección de Datos Personales y su Decreto Reglamentario N° 1558/2001
- https://www.argentina.gob.ar/justicia/derechofacil/leysimple/datos-personales
- Ley N° 27275 de Acceso a la Información Pública y su Decreto Reglamentario N° 206/2017
- https://www.argentina.gob.ar/justicia/derechofacil/leysimple/acceso-la-informacion-publica
- Ley 27.699 Protocolo modificatorio del Convenio para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal
- Privacidad de Datos: https://www.cloudflare.com/es-es/learning/privacy/what-is-data-privacy/
- Protección de Datos Personales, Sharchman, José M, 2019
- Guía sobre el uso de las cookies, Agencia española de Protección de Datos, 2019