PRIVACY INTERNATIONAL

Las Claves para Mejorar
la Protección de Datos

Las Claves para Mejorar la Protección de Datos

August 2018

Índice

Introducción

El derecho a la privacidad es un derecho fundamental contemplado en muchas constituciones del mundo y en instrumentos internacionales de derechos humanos. Si bien comprende diversas facetas, uno de los aspectos esenciales que componen este derecho, y que resulta cada vez más relevante en la vida de las personas, es la protección de los datos personales.

Ya en 1988, el Comité de Derechos Humanos de las Naciones Unidas, el órgano encargado de realizar el seguimiento de la implementación del Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por sus siglas en inglés), reconoció la necesidad de implementar leyes de protección de datos para salvaguardar el derecho fundamental a la privacidad, reconocido en el artículo 17 de dicho pacto.

La protección de la privacidad en la era digital resulta fundamental para consolidar una gobernanza democrática efectiva y adecuada. Sin embargo, todavía se requieren marcos y procesos legales e institucionales, además de infraestructura para respaldar la protección de datos y el derecho a la privacidad, a pesar de que existe un mayor reconocimiento y una mayor conciencia de la importancia de ambos derechos. Al mismo tiempo, el creciente volumen y uso de datos personales, junto con la aparición de tecnologías que habilitan nuevas maneras de tratamiento y uso de los mismos, implica que es más importante que nunca regular un marco efectivo de protección de datos.

La protección de la privacidad es fundamental, y la mayoría de los Estados han adoptado algunas formas de protección. Sin embargo, los marcos suelen ser inadecuados y no han sido actualizados según los usos modernos que se hacen de los datos y el desafío que esto representa. Las leyes de protección de datos se deben actualizar para enfrentar las problemáticas que están surgiendo.

Durante las últimas tres décadas, Privacy International ha promocionado y propugnado el derecho a la privacidad y, a través de su red internacional, ha exigido la adopción y la implementación de las salvaguardas más estrictas posibles en materia de protección de datos en todo el mundo.

Con el paso de los años, algunas de estas problemáticas adquirieron mayor envergadura, y surgieron otras totalmente nuevas: el discurso dominante que ponemos en tela de juicio ha evolucionado y nuevos actores, tanto aliados como adversarios, han aparecido en el debate.

Sistemas de uso intensivo de datos

Los Gobiernos de todo el mundo están cambiando radicalmente sus políticas y su infraestructura con la esperanza de habilitar oportunidades económicas y atraer inversiones internacionales, garantizando la seguridad de sus sociedades y fortaleciendo sus instituciones. Elaboran permanentemente nuevas políticas que exigen obtener una mayor cantidad de datos de las personas: esto implica un cambio de grandes proporciones en la relación que se establece entre el individuo y el Estado mediante la acumulación de datos.

No se trata únicamente de los Gobiernos. La industria también tiene un papel esencial porque promueve ideas, respalda la venta de dichos sistemas, proporciona las herramientas y los servicios y también puede controlar datos. La realidad descrita da lugar a lo que llamamos sistemas de uso intensivo de datos: son sistemas que tratan los datos sobre las personas, generan información adicional sobre ellas y utilizan dicha información para tomar decisiones en relación con esas personas.

Debido a los sistemas de uso intensivo de datos, los Gobiernos y la industria encuentran con demasiada frecuencia nuevas oportunidades de vigilancia, generación de ganancias, y de mayor control. Existen algunas salvaguardas. El impulso de generar estos cambios es más fuerte en las economías emergentes, donde las salvaguardas legales y técnicas son más frágiles y donde existe poca o ninguna transparencia en los procesos de toma de decisiones. Asimismo, en estas economías, el Estado de derecho está restringido y las responsabilidades del sector privado son imprecisas. Lo que nosotros observamos es que, en la mayoría de los casos, no se están regulando ni controlando las innovaciones en materia de políticas y tecnología. Esto tendrá consecuencias significativas para la privacidad de las personas y transformará el ejercicio del poder: creará nuevas posibilidades de opresión, consolidará la desigualdad, la discriminación y la exclusión ya existentes y, potencialmente, dará lugar a nuevas formas de estas problemáticas.

También existen desafíos estructurales y sistémicos. Las consultas públicas, la transparencia en la asignación de recursos y el control o la auditoría del funcionamiento de estos sistemas suelen ser insuficientes o inexistentes. Asimismo, los Gobiernos confían cada vez con mayor frecuencia en la industria para implementar sistemas y ejecutar programas informáticos. De la misma manera, la industria está empezando a depender cada vez más de la autorización de los Gobiernos para acceder a los datos. Así, la línea divisoria entre Gobierno e industria se verá desdibujada, y las obligaciones y los deberes de cada parte se confundidas.

Si desea obtener más información acerca de nuestro trabajo sobre sistemas de uso intensivo de datos, visite el sitio web de Privacy International.

Explotación de datos

Cada vez con mayor frecuencia, todo lo que hacemos genera datos, dispongamos o no de un dispositivo. Nuestros dispositivos, nuestras redes e incluso nuestros hogares generan enormes cantidades de datos. Nuestros sistemas de transporte, automóviles, sistemas de pago y ciudades también generan datos a través de nuestra persona y sobre nosotros. Con todos estos datos, es posible que construyamos un mundo mejor, más justo, más limpio, más sustentable y seguro. Aunque también puede ocurrir lo contrario.

Nuestros dispositivos e infraestructuras están siendo diseñadas para facilitar la explotación de datos. Cada vez resulta más difícil para las personas controlar las formas en que se comparten y se tratan los datos sobre su vida.

Como resultado, la industria y el Gobierno están acumulando información sobre nosotros de manera impune. Aspiran a un mundo dominado por los datos, en el que puedan recoger nuestra información libremente, buscar patrones y similitudes, generar inteligencia y tomar decisiones sobre nosotros y nuestro futuro.

Todavía no estamos preparados para el futuro que ya se está consolidando. Nuestra legislación aún no logra abordar estos riesgos. Nuestras tecnologías no son seguras y filtran información. Como resultado, las personas no gozamos de seguridad.

Si desea obtener más información sobre nuestro trabajo relacionado con la explotación de datos, visite el sitio web de Privacy International.

Por qué hemos elaborado esta guía

Mediante el trabajo de su red internacional, Privacy International ha detectado que existen discrepancias y deficiencias en la protección de datos a nivel mundial:

- Algunos países todavía no cuentan con una legislación integral de protección de datos. Sin embargo, cerca de cuarenta países han iniciado procesos legislativos al respecto y están redactando proyectos de ley;
- Los países con leyes de protección de datos suelen tener problemas para implementarlas y ejecutarlas con eficacia, o no las han actualizado para abordar los usos (y abusos) actuales de datos personales y
- Las leyes integrales de protección de datos proporcionan el marco legal principal, incluidos los principios, los derechos y los regímenes de sanciones para proteger los datos personales. Es posible que también se requiera otra legislación sectorial (por ej. en el campo de las telecomunicaciones) para complementar el marco general de protección de datos.

Dada la diversidad del panorama jurídico, nuestras intervenciones nos exigen involucrarnos tanto en la elaboración de la nueva legislación como en la reforma de las leyes que ya existen, además de hacer un seguimiento de la implementación y la ejecución de dichos marcos.

Asimismo, Privacy International ha detectado que existe un problema sistémico: la participación limitada o nula de la sociedad civil y otras partes interesadas no estatales en los procesos de elaboración de estas políticas. Con frecuencia, el escaso compromiso no se debe a la falta de interés de las organizaciones de la sociedad civil, sino que es el resultado de desafíos estructurales e institucionales, como la falta de experiencia en estas temáticas dentro de dichas organizaciones o, de manera significativa, la falta de oportunidades para involucrarse: la elaboración de políticas suele realizarse en privado, a puertas cerradas.

Las organizaciones nacionales de la sociedad civil de todo el mundo deben participar en la elaboración de políticas y en las consultas relacionadas con la protección de datos, a fin de articular la seguridad y las salvaguardas necesarias para garantizar que el proceso sea inclusivo, abierto y transparente. En repetidas ocasiones, nuestra experiencia nos ha demostrado que cuanto más se involucran las organizaciones de la sociedad civil (de todas las disciplinas) en estos procesos de políticas, más y mejor informados están los actores del cambio, y más amplio es el discurso político: en última instancia, aspiramos a que la legislación y las políticas defiendan, respeten y promuevan los derechos fundamentales.

Esta guía fue elaborada para respaldar dichos esfuerzos y fortalecer la campaña global que tiene como objetivo consolidar la protección efectiva de los datos.

Acerca de la guía

La presente guía se elaboró a partir de la experiencia de Privacy International en materia de principios y estándares internacionales aplicables a la protección de la privacidad y los datos personales, y en virtud de su liderazgo e investigación en tecnologías modernas y tratamiento de datos.

La guía tiene el objetivo de colaborar con el análisis de la legislación de protección de datos, ya sea en el caso de:

- documentación técnica (para informar la elaboración de una ley);
- proyectos de ley (el borrador de una propuesta de ley);
- la legislación existente o
- propuestas para enmendar regímenes de protección de datos existentes.

La guía está estructurada para proporcionar un proceso analítico coherente y eficiente, abordando a su vez las diversas disposiciones que suelen incluirse en la legislación de protección de datos.

No proporciona una lista exhaustiva de todas las disposiciones ideales que deberían formar parte de una legislación de protección de datos. Por el contrario, se concentra en las áreas que, según nuestra experiencia, requieren un mayor compromiso y mejores directrices para garantizar que las leyes respeten las obligaciones nacionales e internacionales de derechos humanos a fin de proteger el derecho a la privacidad y otros derechos fundamentales, además de cumplir con los estándares y los principios de protección de datos a nivel internacional y regional.

Cada sección proporciona información orientadora acerca de cuál es el objetivo regularizador y cuáles son los diferentes elementos que debe incluir. Asimismo, de ser relevante, ofrece una guía y vocabulario para facilitar la elaboración de comentarios generales y específicos.

La guía cita ejemplos de todo el mundo. Hay un foco especial en ejemplos del marco de protección de datos de la Unión Europea, como uno de los marcos más integrales y recientes, además de ejemplos de orientaciones y tratados regionales e internacionales. Esta guía está dirigida a las organizaciones de la sociedad civil de todo el mundo, y puede ser adaptada para satisfacer los diferentes marcos nacionales y contextos locales.

PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

PARTE: 1

Protección de Datos

Protección de Datos

¿Qué es la Protección de Datos?

La protección de datos suele definirse como la legislación diseñada para proteger los datos personales. En las sociedades modernas, con el fin de empoderar a las personas a controlar sus datos y protegerlas de abusos, es esencial que la legislación de protección de datos restrinja y estructure las actividades de las empresas y los Gobiernos. En repetidas ocasiones, estas instituciones han demostrado que, a menos que existan normas que restrinjan su accionar, procurarán recoger y explotar la mayor cantidad de datos que estén a su alcance para conservarlos y compartirlos con terceros, sin decirnos absolutamente nada al respecto[1].

¿Por qué es Necesaria la Protección de Datos?

Cada vez que usted utiliza un servicio, compra un producto en línea, se registra para obtener un correo electrónico, visita al médico, paga sus impuestos, celebra algún contrato o solicita algún servicio, debe proporcionar datos personales. Empresas y agencias con las que probablemente usted jamás supo que interactuaba generan y recogen datos e información sobre su persona, sin que usted tenga conocimiento de ello. La única manera en que los ciudadanos y los consumidores pueden confiar en el Gobierno y las empresas es mediante prácticas rigurosas de protección de datos, con una legislación efectiva que contribuya a minimizar la vigilancia estatal y corporativa y la explotación de datos.

Desde la década del año 1960, y debido a la expansión de las capacidades de las tecnologías de la información, empresas y Gobiernos han conservado información personal en bases de datos. Estas bases de datos pueden ser objeto de búsquedas, y es posible editarlas o utilizarlas para establecer referencias cruzadas. Asimismo, también es posible compartir los datos almacenados con otras organizaciones del mundo.

Cuando se generalizó la recogida y el tratamiento de datos, las personas empezaron a querer saber qué sucedía con la información una vez que la proporcionaban. ¿Quién tenía el derecho a acceder a los datos? ¿Se conservaba la información de manera adecuada? ¿Se recogía y se compartía sin que ellas lo supieran? ¿Podría utilizarse para discriminar o violar otros derechos fundamentales?

A partir de todas estas preguntas, y a raíz de la creciente preocupación pública, se diseñaron principios de protección de datos mediante numerosas consultas a nivel nacional e internacional. La región alemana de Hesse aprobó la primera ley en 1970. La Ley de Informe Equitativo de Crédito de 1970 de Estados Unidos también incluía elementos de protección de datos[2]. Estados Unidos lideró el desarrollo de un "código de prácticas justas de información" a principios de la década del año 1970, que continúa dando forma a la legislación de protección de datos de la actualidad. Casi en la misma época, el Reino Unido estableció un comité para revisar las amenazas por parte de empresas privadas, y llegó a conclusiones similares.

Inmediatamente después, surgieron leyes nacionales, primero en Suecia, Alemania y Francia. Hasta enero de 2018, más de 100 países han adoptado leyes de protección de datos, y otros 40 países se encuentran trabajando en iniciativas o proyectos de ley del mismo tipo[3] .

Con el transcurso del tiempo, se adoptaron también marcos legales a nivel regional. En 1980, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) elaboró sus directrices, que incluían "principios de privacidad". Inmediatamente después, entró en vigencia el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, del Consejo de Europa (el convenio se modernizó en 2018)[4] .

Considerando únicamente el volumen de datos generados y el rápido desarrollo de la tecnología (incluyendo la elaboración de perfiles y el seguimiento sofisticados, así como la inteligencia artificial), resulta obvio que algunas de las leyes existentes de protección de datos están desactualizadas y, por lo tanto, no son adecuadas para abordar la temática del tratamiento de la manera en que este se lleva a cabo actualmente. Los marcos normativos no reflejan el nuevo potencial del tratamiento de datos, que surgió con el avance de las tecnologías implementadas e incorporadas en los sistemas de gobernanza y los modelos empresariales.

Se ha informado que el 90 % de los datos mundiales del día de hoy se creó en los últimos dos años, y que cada dos días creamos la misma cantidad de datos que hemos creado desde el inicio de los tiempos hasta 2013.[5] En el momento en que se elaboraron muchos de los marcos de protección de datos, el mundo era un sitio muy diferente. Por ejemplo, muchas leyes se adoptaron incluso antes de que se crearan Google, Facebook y los smartphones (es decir, incluso mucho antes de que empezaran a usarse ampliamente).

Es posible que los marcos de protección de datos tengan sus limitaciones, las cuales estamos tratando de identificar y abordar mediante la exploración de las reglamentaciones adicionales para proporcionar las salvaguardas necesarias. Sin embargo, estos marcos ofrecen un punto de partida importante y fundamental para garantizar que se implementen rigurosas salvaguardas legales y regulatorias para proteger los datos personales.

Un marco estricto de protección de datos empodera a las personas, restringe las prácticas perjudiciales de datos y limita la explotación de la información. Resulta esencial establecer los tan necesarios marcos de gobernanza a nivel nacional y

mundial, para garantizar que las personas gocen de sólidos derechos sobre sus datos, imponer obligaciones estrictas a los responsables del tratamiento de dichos datos personales (tanto en el sector público como en el privado) y asegurar que sea posible utilizar robustas facultades de ejecución ante quienes violan estas obligaciones y protecciones.

Protección de Datos: Esencial para el Ejercicio del Derecho a la Privacidad

La privacidad es un derecho humano reconocido a nivel internacional. El artículo 12 de la Declaración Universal de Derechos Humanos (DUDH) proclama que

> **nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia... Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.**[6]

La DUDH ha sentado las bases para los tratados de derechos humanos a nivel internacional más importantes que, de la misma manera, consagran el derecho a la privacidad, incluido el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por sus siglas en inglés).

Ya en 1988, el Comité de Derechos Humanos de las Naciones Unidas, el órgano creado en virtud de tratados y encargado de realizar el seguimiento de la implementación del ICCPR, reconoció la necesidad de una legislación sobre protección de datos para salvaguardar el derecho fundamental a la privacidad, reconocido en el artículo 17 de dicho pacto.

> **La recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por autoridades públicas como por particulares o entidades privadas, deben estar reglamentados por la ley... Toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos... se han compilado o tratado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación.**[7]

En 2011, el entonces relator especial sobre la promoción y la protección del derecho de libertad de opinión y expresión de la ONU emitió un informe que destacaba de manera similar que "la protección de datos personales representa una forma especial de respeto por el derecho de privacidad"[8] . El informe observaba además que:

> **La necesidad de adoptar leyes claras para proteger los datos personales se ve incrementada aun más en la actual era de la información, en la que intermediarios recopilan y almacenan grandes volúmenes de datos, y existe una tendencia preocupante de los Estados a obligar o presionar a estos actores privados a entregar la información de sus usuarios**[9]

En 2013, también observó que el derecho a la privacidad incluye

> **la capacidad que tienen las personas de determinar quién registrará información sobre ellas y cómo [...] se utiliza dicha información.**[10]

En diciembre de 2016, la Asamblea General de la ONU aprobó una resolución (por consenso) sobre el derecho a la privacidad en la era digital, Res. AG 71/199, que reafirmó resoluciones anteriores de la Asamblea sobre la temática, haciendo hincapié en que:

> **los Estados deben respetar las obligaciones internacionales en materia de derechos humanos en lo referente al derecho a la privacidad [...] cuando exijan a terceros, incluidas las empresas privadas, la divulgación de datos personales**[11]

La privacidad y la protección de datos están intrínsecamente vinculadas. Las personas, en su condición de ciudadanos, clientes y consumidores, deben contar con los medios y las herramientas necesarias para ejercer su derecho a la privacidad y a protegerse de abusos que podrían sufrir tanto ellas como sus datos. También es importante que las obligaciones de quienes tratan los datos sean claras, de modo que tomen medidas para proteger la información, mitigar las interferencias con el derecho a la privacidad y puedan rendir cuenta cuando no cumplen con sus obligaciones. Esto debe respetarse particularmente cuando se trata de nuestros datos personales.

Los datos personales, como se menciona en detalle más abajo, son los datos relacionados con una persona (información tratada con medios automatizados,

o conservada en un sistema de archivo estructurado). La protección de datos se trata de salvaguardar nuestro derecho fundamental a la privacidad mediante la regulación del tratamiento de los datos personales: proporcionar a la persona derechos sobre sus datos y establecer sistemas de designación de responsabilidades y obligaciones claras para quienes controlan o llevan a cabo el tratamiento de los datos.

¿Es la Protección de Datos un Derecho?

Hace mucho tiempo que la protección de datos personales fue reconocida como un aspecto fundamental del derecho a la privacidad. En los últimos años, se la ha reconocido incluso como un derecho independiente. Por ejemplo, la protección de datos fue incluida como un derecho independiente en la Carta de los Derechos Fundamentales de la Unión Europea (2012/C 326/02), en el artículo 8 (además del artículo 7 de la Carta, que contempla el derecho a la privacidad). El artículo 8 afirma:

Protección de datos de carácter personal

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada, o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

En muchos países del mundo existe un derecho constitucional de habeas data, diseñado para proteger los datos de una persona, otorgándole el derecho de acceder a la información que se posee sobre ella, y permitiéndole presentar una reclamación ante el Tribunal Constitucional.

Artículo 5 de la Constitución de Brasil de 1988:
Se concederá "habeas data" para a) asegurar el conocimiento de información relativa a la persona del solicitante que conste en registros o bancos de datos de entidades gubernamentales o de carácter público; b) la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo.

Artículo 15 de la Constitución de Colombia, según la enmienda de 1995:
Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.

Para efectos tributarios judiciales y para los casos de inspección, vigilancia e intervención del Estado, podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.

¿Cómo Funciona la Protección de Datos?

No existen estándares de protección de datos reconocidos a nivel mundial. Sin embargo, los organismos regionales e internacionales han acordado códigos, prácticas, decisiones, recomendaciones e instrumentos de políticas.

Los instrumentos más significativos son:

- El Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa (n.º 108), 1981, según la enmienda de 2018
- Las Directrices de la Organización para la Cooperación y el Desarrollo Económicos, que regulan la protección de la privacidad y los flujos transfronterizos de datos personales (1980), según la enmienda de 2013
- Los Principios Rectores para la Reglamentación de los Archivos Computarizados de Datos Personales (resolución de la Asamblea General 45/95 y E/CN.4/1990/72).

También existen otros marcos regionales, entre los que se incluye el Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico (APEC, por sus siglas en inglés)[12] .

Si existe una legislación integral para la protección de datos, las organizaciones (públicas o privadas) que recopilan y utilizan datos personales de un individuo tienen la obligación de realizar el tratamiento de la información según dicha legislación.

La protección de datos debe garantizar que:

- Existan límites en la recopilación de datos personales y que se obtengan por medios lícitos y leales, y de manera transparente; Los fines para los que se utiliza la información estén especificados (a más tardar) al momento de la recopilación, y que solo se la utilice para los fines acordados. Los datos personales solo puedan divulgarse, utilizarse o conservarse para la finalidad original (es decir, los fines explicitados al momento de la recopilación), excepto que se cuente con el consentimiento de las personas o según lo disponga la ley. De igual modo, es necesario que la legislación garantice que los datos se eliminen cuando ya no sean necesarios para dicha finalidad
- Los datos personales, según sean generados y tratados, sean adecuados, relevantes y se restrinjan a la necesidad de la finalidad para la que se utilizará
- Los datos sean exactos y estén completos, y que se tomen medidas para garantizar su actualización
- Se adopten salvaguardas razonables de seguridad para proteger los datos personales de posibles pérdidas, accesos no autorizados, destrucción, uso, modificación o divulgación
- No existan encargados secretos del tratamiento, ni fuentes u operaciones de tratamiento secretas. También, que se informe a las personas sobre la recogida y el tratamiento de sus datos, al igual que sobre los fines para los que se utilizarán, quién(es) los controla(n) y quién está a cargo de su tratamiento
- Las personas cuenten con una gama de derechos que les permita controlar sus datos personales y todo tipo de tratamiento
- Quienes utilizan los datos personales deben rendir cuentas y demostrar su cumplimiento con los principios antes mencionados, además de facilitar y cumplir con el ejercicio de estos derechos, actuando en conformidad con las leyes aplicables que consagran dichos principios

Directrices de la OCDE para la Protección de la Privacidad y el Flujo Transfronterizo de Datos, actualizadas en 2013:

1. Principio de limitación de recogida
2. Principio de calidad de los datos
3. Principio de especificación de los fines
4. Principio de limitación de uso

5. Principio de salvaguardas de la seguridad
6. Principio de transparencia
7. Principio de participación individual
8. Principio de responsabilidad

Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, n.º 108, según la enmienda de 2018:

Artículo 5 (4):
Los datos de carácter personal que sean objeto de un tratamiento:
a. Se obtendrán y tratarán de manera leal y transparente;
b. Se recogerán para fines explícitos, especificados y legítimos, y no se deberán tratar de alguna manera incompatible con dichos fines. Asimismo, el tratamiento para fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos es, con las salvaguardas pertinentes, compatible con aquellos fines;
c. Serán adecuados, relevantes y no excesivos en relación con los fines de su tratamiento;
d. Serán exactos y, si fuera necesario, puestos al día;
e. Se conservarán bajo una forma que permita la identificación de los interesados durante un período de tiempo que no exceda el necesario para satisfacer los fines por los que dichos datos reciban tratamiento.

Directiva General sobre Datos Personales, Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, del 27 de Abril de 2016:

Principios presentados en el artículo 5:
1. Licitud, lealtad y transparencia
2. Limitación de la finalidad
3. Minimización de datos
4. Exactitud
5. Limitación del plazo de conservación
6. Integridad y confidencialidad
7. Responsabilidad proactiva

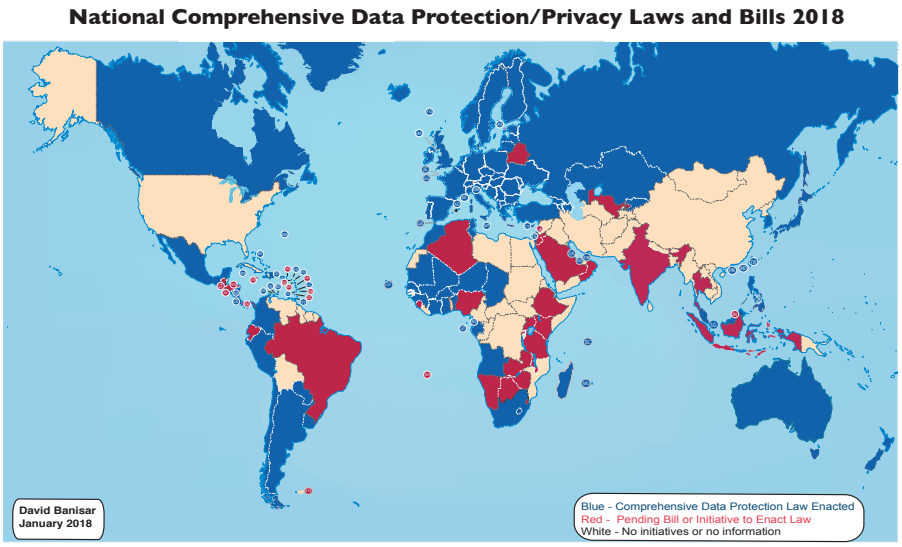
La responsabilidad debe ser el aspecto central de cualquier legislación que regule el tratamiento de datos personales y la protección de los derechos de las personas. Por lo tanto, un ente o autoridad reguladora debe estar a cargo de la ejecución de las normas de protección de datos. El alcance de las facultades otorgadas a estas autoridades varía de un país a otro, así como varía su independencia del Gobierno. Algunas jurisdicciones han establecido más de un organismo para la regulación del control y cumplimiento de la ley, y las facultades otorgadas dependen de que los datos sean tratados por entidades públicas o privadas, como es el caso de Colombia. Por ejemplo, estas facultades pueden incluir la capacidad de llevar a cabo investigaciones, actuar ante reclamaciones e imponer multas cuando una organización haya violado la ley.

Asimismo, debe ser posible acceder, a través de órganos jurisdiccionales, a recursos legales cuando ocurran violaciones a la ley de protección de datos, tanto mediante acciones individuales como colectivas (propuestos por ONG y grupos de consumidores).

En resumen, la protección de datos funciona a partir de principios clave que proporcionan a las personas derechos sobre sus datos: quienes realizan el tratamiento de los datos tienen obligaciones que cumplir en relación con dichos datos y, cuando no se respetan estos principios, derechos y obligaciones, deben existir mecanismos de control de la aplicación y vías de recurso.

La Protección de Datos Hoy en Día

Hasta enero de 2018, más de 100 países en todo el mundo han promulgado legislación integral de protección de datos, y cerca de 40 países están por aprobar también el mismo tipo de leyes. Es posible que otros países cuenten con leyes de privacidad que aplican a determinadas áreas, por ejemplo para niños o registros financieros. Sin embargo, no tienen leyes integrales de protección de datos.



Fuente: Banisar, David, Leyes y proyectos de ley integrales de protección de datos/la privacidad a nivel nacional 2018 (25 de enero de 2018). Disponible en SSRN: https://ssrn.com/abstract=1951416 o http://dx.doi.org/10.2139/ssrn.1951416

En los países en los que no existe un marco integral, la protección de datos se regula mediante leyes sectoriales, si es que está regulada. Por ejemplo, si bien fue una de las primeras leyes en el ámbito de la protección de datos, la Ley de privacidad de EE. UU. de 1974 aplica únicamente al Gobierno federal, mientras que leyes posteriores aplican sólo a sectores o grupos de personas específicos (por ej. la Ley de Protección de Privacidad en Línea para Niños, COPPA). Sin embargo, no existe una legislación integral de protección de datos hasta la fecha. Este enfoque sectorial todavía existe en muchos países, incluida India.

Un avance significativo en legislación de protección de datos fue la adopción del Reglamento General de Protección de Datos de la Unión Europea (RGPD), que entró en vigencia el 25 de mayo de 2018. El RGPD es integral y abarca casi todos los tipos de tratamiento de datos personales. Asimismo, resulta de importancia porque su implementación afectará no solo a los responsables del tratamiento de datos con base en la Unión Europea, sino también a todos quienes ofrezcan bienes o servicios a personas con base en la Unión Europea, o quienes realicen el seguimiento del comportamiento de dichas personas.

En mayo de 2018, hubo un nuevo avance al respecto con la enmienda del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa (n.º 108). Desde su adopción en 1981, más de 40 países europeos y nueve países que no son miembro del Consejo de Europa han utilizado el convenio como base de sus propios marcos de protección de datos. El texto modernizado del convenio reafirma los principios existentes y adopta nuevas disposiciones para fortalecer las obligaciones, la responsabilidad y los mecanismos de ejecución[13] .

Para obtener más información sobre la legislación de protección de datos, desglosada por país, consulte los informes de Privacy International[14] .

Protección de Datos: Una Pieza del Rompecabezas

En lo que refiere a la protección del derecho a la privacidad de las personas y de sus datos, la protección de datos es apenas una de las piezas del rompecabezas.

Los marcos generales de protección de datos no excluyen la adopción o aplicación de leyes sectoriales que regulen sectores determinados. Toda ley de protección de datos debe aclarar que su objetivo es proteger los derechos fundamentales de las personas, como el derecho a la privacidad y a la protección de datos personales. Por lo tanto, cualquier ley (actual o futura) que contradiga dicha protección, por ej. restringiendo estos derechos fundamentales, debe considerarse nula y sin efecto.

Se debe garantizar la adopción de la legislación correspondiente para regular las políticas y prácticas del Gobierno y el sector privado que interfieran con el derecho a la privacidad e impliquen el tratamiento de datos personales. Esta legislación podría regular, por ejemplo:

- La información y la tecnología
- Las fuerzas y los cuerpos de seguridad
- El comercio
- La educación
- La gobernanza electrónica
- Los servicios de atención de salud
- Las instituciones financieras y bancarias
- La protección al consumidor
- La ciberseguridad
- La responsabilidad por productos

Asimismo, la legislación debe garantizar la protección de las personas y sus datos, además de respetar su derecho a la privacidad

Una Guía Paso a Paso para la Protección de Datos

Si bien la legislación de protección de datos varía de un país a otro, existen algunos aspectos en común y requisitos mínimos respaldados por principios y estándares de protección de datos.

Las leyes suelen incluir algunas disposiciones generales que contemplan:

- El alcance de la ley
- Definiciones
- Los principios de protección de datos
- Las obligaciones de los responsables y los encargados del tratamiento
- Los derechos de los interesados
- El control y la ejecución.

Los otros capítulos de la guía describen y explican estas disposiciones generales con mayor detalle, presentando los componentes clave de la protección de datos mediante diversos ejemplos a nivel nacional y mundial.

Referencias

1 Consulte el texto completo en https://www.privacyinternational.org/explainer/41/101-data-protection

2 Robert Gellman, Prácticas justas de información: antecedentes básicos, abril de 2017, PDF disponible en: https://bobgellman.com/rg-docs/rg-FIPshistory.pdf

3 David Banisar, Leyes y proyectos de ley integrales de protección de datos/la privacidad a nivel nacional 2018, disponible en: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1951416 (última modificación el 25 de enero de 2018).

4 Protocolo de enmienda del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (ETS n.o 108), 128.va Sesión del Comité de Ministros, 18 de mayo de 2018, CM(2018) 2-final. Disponible en

5 Thomas A Singlehurst et al, La protección de datos y la privacidad electrónica, CitiGroup, marzo de 2017, p4. PDF disponible en https://www.citibank.com/commercialbank/insights/assets/docs/ePrivacyandData.pdf

6 Res. 217 (III) A de la AG, DUDH, art. 12 (10 de diciembre de 1948).

7 Doc. ONU HRI/GEN/1/Rev. 9, observación general n.o 16: artículo 17, apartado 10.

8 Doc. ONU A/HRC/17/27, apartado 58 (16 de mayo de 2011).

9 Id. apartado 56.

10 Doc. ONU A/HRC/23/40, ¶ 22 (17 de abril de 2013).

11 Res. AG 71/199, at 3; según Res. Consejo Derechos Humanos 34/7.

12 Marco de privacidad del Foro de Cooperación Económica Asia-Pacífico (APEC), diciembre de 2005, disponible en https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework

13 Consejo de Europa, Modernización del Convenio 108, Portal de la Unión Europea, disponible en https://www.coe.int/en/web/data-protection/convention108/modernised

14 Privacy International, Estado de privacidad, disponible en https://www.privacyinternational.org/reports/state-of-privacy

PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

PARTE: 2

Disposiciones Generales, Definiciones y Alcance

Disposiciones Generales, Definiciones y Alcance

Disposiciones Generales

Objeto y finalidad de la legislación

Esta sección debe proporcionar una finalidad o meta legítima de la legislación . Las buenas prácticas sugieren que esta sección haga referencia directa a los derechos fundamentales y las obligaciones internacionales relacionadas con derechos humanos, además de las responsabilidades que tiene el Estado según las leyes nacionales e internacionales. Asimismo, debe declarar explícitamente que la legislación cumplirá con todo lo anterior en su alcance y aplicación.

Se deben incluir los siguientes puntos:

1. Referencia al derecho a la privacidad y la protección de datos personales, según lo dispuesto por la Constitución, si correspondiera.
2. Referencia a las obligaciones internacionales y de derechos humanos, según lo establecido por tratados regionales e internacionales de los que el país sea firmante, si correspondiera:
    - El Pacto Internacional de Derechos Civiles y Políticos (ICCPR) de 1966
    - El Convenio Estadounidense sobre Derechos Humanos
    - La Declaración Estadounidense de Derechos y Obligaciones de los Ciudadanos
    - La Carta Árabe sobre Derechos Humanos
    - La Declaración de Derechos Humanos de la Asociación de Naciones del Sureste Asiático (ASEAN, por sus siglas en inglés)
    - El Convenio Europeo sobre Derechos Humanos
    - La Carta de la Unión Europea sobre los Derechos y las Libertades Fundamentales
    - La Carta Africana sobre los Derechos Humanos y de los Pueblos
    - La Carta Africana sobre los Derechos y el Bienestar del Niño y Otros tratados, si correspondiera.
3. Referencia a instrumentos regionales e internacionales sobre protección de datos que pueden o no ser legalmente vinculantes:
    - Las Directrices de la OCDE para la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales;
    - El Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa (n.º 108), según la enmienda de mayo de 2018
    - El Reglamento General de Protección de Datos de la Unión

Europea y la Directiva sobre las Fuerzas y los Cuerpos de Seguridad de la Unión Europea
- El Marco de Privacidad del Foro de Cooperación Económica de Asia-Pacífico (APEC, por sus siglas en inglés)
- La Comunidad Económica de Estados de África Occidental incluye una ley complementaria sobre protección de datos del año 2010
- El Convenio sobre Ciberseguridad y Protección de Datos Personales de la Unión Africana
- Otros tratados, si correspondieran.

La inclusión de estas referencias es necesaria por motivos legales, porque vincula la protección de datos personales con un derecho: si este derecho se viola o es objeto de interferencias, los afectados podrían verse perjudicados. El enfoque también sirve como una manera de humanizar la legislación de protección de datos: al elaborar las leyes y las políticas, se suele olvidar que los afectados por la legislación no son únicamente "sujetos de derecho" o "interesados", sino también personas. En lo referido a los términos del discurso, es esencial y beneficioso implementar un enfoque humano o de derechos civiles para garantizar que el marco de estos procesos de políticas sea constructivo.

Objeto del Convenio 108 modernizado para proteger a las personas

La enmienda realizada al Convenio 108 en mayo de 2018 evidencia un cambio en la consideración del rol y la finalidad de la protección de datos, ya que modificó su marco para concentrarse en la protección de las personas, sus datos y sus derechos fundamentales:

> **"La finalidad del presente convenio es proteger a todas las personas, cualquiera sea su nacionalidad o residencia, en relación con el tratamiento de sus datos personales. De esta forma, se contribuye a respetar sus derechos humanos y libertades fundamentales, y en particular su derecho a la privacidad."**

Definiciones

Los términos fundamentales y más frecuentes en la ley deben definirse claramente desde el principio.

Nuestra experiencia nos ha demostrado que existen términos y definiciones específicos que deben utilizarse en la legislación y que, sin embargo, suelen estar ausentes o definidos incorrecta o inadecuadamente, incluso aquellos que detallan a qué y a quiénes se aplica la ley. Las definiciones que se brindan a continuación tienen el objetivo de abordar esta clase de deficiencias, que suelen ser comunes.

Datos personales

Con el reciente avance de los mecanismos de tratamiento de datos como resultado del progreso de la tecnología y la mayor inteligencia e información que puede obtenerse a partir de datos no procesados, es esencial que la legislación proporcione una definición integral y clara del término "datos personales", dado que la ley se aplicará sobre la base de dicha definición. La terminología puede variar y, en algunos países, como en los EE. UU., los datos personales se definen como " información identificable de manera personal".

En general, es común que la definición de "datos personales" sea relativamente amplia. Sin embargo, en algunas ocasiones, tiene un alcance restringido y no considera, por ejemplo, instancias adicionales del tratamiento de datos, o los datos que pueden identificar a una persona indirectamente.

Una definición de ejemplo es la que encontramos en el RGPD de la Unión Europea:

> **"cualquier información relativa a una persona física identificada o identificable ("el interesado"). Se considerará persona física identificable a toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona…(RGPD)"**

La Evolución del Concepto de Datos Personales

Es necesario actualizar y ampliar la definición de "datos personales": debe incluir todos aquellos datos utilizados para identificar a una persona, directa o indirectamente. Los tipos de identificadores se desarrollarán con la tecnología: por ejemplo, hoy en día existe un amplio consenso en que la dirección IP es un dato personal.

En octubre de 2016, el Tribunal de Justicia de la Unión Europea (TJUE) dictaminó que el término "datos personales" "debe interpretarse en el sentido de que una dirección IP dinámica registrada por un proveedor de servicios de medios en línea, con ocasión de la consulta por una persona de un sitio de Internet que ese proveedor hace accesible al público, constituye respecto a dicho proveedor un dato personal, en el sentido de la citada disposición, dado que el proveedor de acceso a Internet dispone de los medios legales que le permiten identificar a la persona a través de información adicional que el proveedor de Internet tiene sobre ella".

Asimismo, existen métodos de tratamiento de datos (como la elaboración de perfiles, el seguimiento y el control) que no requieren un nombre o dirección específicos, ni ningún otro identificador directo para identificar a las personas, y que afectan la manera en que se tratan los datos. La identificación indirecta es un elemento clave que debe incluirse en la definición de datos personales.

En la era de la vinculabilidad de datos, la desanonimización de conjuntos de datos y el avance de la inteligencia artificial, existe también la inquietud de que otras formas de datos puedan convertirse en datos personales, al dar lugar a que una persona sea identificada e identificable de manera inequívoca. La firma de movimientos e identificadores de dispositivos, incluido el comportamiento de las personas que hacen uso de dichos dispositivos, pueden vincularse entre transacciones sensibles y no sensibles. Toda definición en la legislación debe considerar que es posible revelar, derivar, inferir y predecir datos personales a partir de otros datos.

Fuente: Comisión Europea, ¿Qué son los datos personales? Disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

Ejemplos de Datos Personales:

- nombre y apellidos,
- domicilio,
- dirección de correo electrónico, del tipo nombre.apellido@empresa.com,
- número de documento nacional de identidad,
- datos de localización (como la función de los datos de localización de un teléfono móvil),
- dirección de protocolo de Internet (IP),
- el identificador de una cookie,
- el identificador de la publicidad del teléfono,
- los datos en poder de un hospital o médico, que podrían ser un símbolo que identificara de forma única a una persona.

Datos personales sensibles

Es común que se distingan determinados datos personales como "datos sensibles", una categoría especial de datos que, al ser tratada, requiere niveles adicionales de protección. Esta categoría de datos implica la existencia de mayores salvaguardas, además de limitaciones a las bases jurídicas permitidas para su tratamiento.

La mayoría de las leyes no proporcionan una definición sino que ofrecen una lista de datos que constituyen los datos personales sensibles, o una lista de categorías especiales de datos personales. Sin embargo, en algunas jurisdicciones como Colombia, las disposiciones sobre datos personales sensibles se refieren a datos que pueden impactar en la privacidad de las personas, o datos cuyo uso indebido puede resultar en discriminación[1].

En general, las categorías de datos identificados como sensibles están vinculadas con las formas de discriminación abordadas en los instrumentos de derechos humanos y las protecciones constitucionales que consagran la no discriminación[2].

No existe una lista exhaustiva de lo que constituyen datos personales sensibles. Sin embargo, existe amplio consenso en que los datos relacionados con la siguiente información son datos personales sensibles:

(a) el origen racial o étnico de una persona,
(b) las opiniones políticas,
(c) las convicciones religiosas o filosóficas, u otras convicciones de naturaleza similar,
(d) la afiliación sindical,
(e) los datos relativos a la salud física o psíquica,
(f) los datos relativos a la orientación sexual,
(g) la comisión o presunta comisión de delitos, o cualquier proceso por delitos cometidos o que se presumen cometidos, la resolución de dicho proceso o la sentencia de cualquier órgano jurisdiccional en dicho proceso,
(h) los datos biométricos,[3]
(i) los datos genéticos.[4]

También se deben considerar otras categorías que podrían incluirse, por ejemplo, los datos financieros, los números de seguridad social y los datos relativos a niños. Algunos países también han debatido sobre la posibilidad de agregar otras categorías de datos que requieren protección adicional debido a su "sensibilidad" dentro de su propio contexto nacional. Por ejemplo, en India, la "información de casta" se considera un dato personal sensible.[5] El hecho de que los Gobiernos tengan en consideración el contexto y las realidades locales es un paso importante para garantizar que se establezcan las salvaguardas relevantes en la legislación.

También es importante que la más elevada protección incluya los datos que revelan datos personales sensibles: mediante la elaboración de perfiles y el uso de información relacionada (por ej. usar el historial de compra de una persona para

inferir una afección médica) es posible que los encargados del tratamiento de los datos infieran, deriven y anticipen datos personales sensibles sin que se les hayan proporcionado explícitamente dichos datos.

Tratamiento

Algunas definiciones de "tratamiento" no abarcan todo el espectro de posibles "tratamientos", y se limitan a la recogida de información.

La definición de "tratamiento" debe ser amplia e inclusiva, en lugar de exhaustiva. De esta manera, se alentaría a los países a pensar de manera innovadora y progresista en respuesta a los avances tecnológicos en los métodos de análisis de datos.

La definición de tratamiento debe abarcar el ciclo de vida completo de los datos, desde su creación hasta su eliminación, además de su uso para revelar otro tipo de información.

Una definición de ejemplo:

> **"Cualquier operación o conjunto de operaciones realizadas sobre datos personales, o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción"** [6]

Teniendo esto en cuenta, Privacy International propone que la definición de "tratamiento" incluya específicamente la generación de datos. Se trata de una actividad que, hasta la fecha, no ha sido abordada explícitamente en la legislación de protección de datos, y que debe ser regulada y controlada. Asimismo, es una actividad por la que las personas deben recibir protección.

Esta sugerencia se basa en un análisis de Privacy International que demostró que los problemas relacionados con lo que se conoce como "explotación de datos" suelen comenzar con una generación excesiva de información, debido a que la generación es la condición previa para el tratamiento posterior. Esta generación excesiva de datos recogidos a través de los sistemas y los servicios que utilizamos, junto con las causas principales como la falta de conciencia, transparencia y responsabilidad, dan lugar al problema fundamental de desequilibrio de poder en un mundo dominado por los datos. Sumar esta actividad a la definición de

"tratamiento" complementaría el "principio de limitación de uso" y el concepto de "minimización de datos".

Responsables y encargados del tratamiento de datos

Los mecanismos de responsabilidad y ejecución son fundamentales para consolidar con éxito la protección de los datos personales. La legislación debe identificar claramente las partes responsables del cumplimiento de la ley, al igual que sus obligaciones y deberes.

Con el paso del tiempo, la terminología utilizada para hacer referencia a los responsables y los encargados del tratamiento de datos personales ha ido evolucionando. Si bien el vocabulario varía según los diferentes marcos de protección de datos, existen dos entidades que tienen el control de los datos personales o están a cargo del tratamiento de dichos datos: los responsables y los encargados respectivamente.

El responsable del tratamiento de los datos es la persona física o jurídica, pública o privada que, sola o junto con otros, determina los fines y los medios del tratamiento de los datos personales, es decir, el "por qué" y el "cómo".

El encargado del tratamiento es la persona física o jurídica, pública o privada que, sola o junto con otros, realiza el tratamiento de los datos personales por cuenta del responsable del tratamiento, es decir, suele limitarse a proporcionar soluciones técnicas, los "métodos y los medios" de tratamiento.

Elaboración de perfiles

Se trata de un término relativamente nuevo. Sin embargo, es esencial que tenga un reconocimiento explícito en la legislación de protección de datos, debido al uso que se hace de los datos para derivar, inferir y predecir otro tipo de información sobre las personas, y debido a los desafíos que plantean la minería de datos y el aprendizaje de máquina, entre otras técnicas innovadoras.

La siguiente definición de "elaboración de perfiles" se incluye tanto en la Ley de Privacidad de Datos de Filipinas de 2012 (sección 1. [p]) y en el RGDP (artículo [4]):

> **"Toda forma de tratamiento automatizado consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física**[7]

Alcance y Aplicación de la Legislación

Ámbito de aplicación material

¿A qué se debe aplicar la reglamentación?

La legislación se debe aplicar a los datos automatizados y al tratamiento automatizado de datos, así como a los formatos estructurados de conservación manual de datos. Esto significa que una legislación de protección de datos debe abarcar todas las prácticas de tratamiento de datos en ordenadores, teléfonos, dispositivos que forman parte de la Internet de las cosas, y también en registros en papel.

El alcance sugerido de aplicación, según se establece en el artículo 2 (1) del RGPD, es:

> **“…al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero”**

En el artículo 4 (6) se define el término “fichero”:

> **“todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica”**

¿A quiénes se debe aplicar la reglamentación?

Es esencial que esta sección de cualquier legislación proporcione claridad en cuanto a quiénes se aplica la ley. La legislación de protección de datos debe aplicarse a instituciones tanto públicas como privadas. Es una práctica inaceptable que las instituciones públicas (incluidas las agencias de inteligencia, y las fuerzas y los cuerpos de seguridad) estén completamente exentas de las obligaciones para proteger los datos personales de los interesados, o que las exenciones sean excesivamente amplias o vagas.

Además de limitar el alcance de la ley a las “personas naturales”, existe amplio consenso en que el tratamiento para fines domésticos o personales debe estar exento de la aplicación. Algunas jurisdicciones incluyen criterios adicionales para esta exención. En el mundo de Internet, donde la línea divisoria entre lo profesional

y lo personal es cada vez más difusa, se debe considerar cómo definir y explicar esta exención a los interesados.

Instituciones públicas y privadas: dos entidades, dos reglamentaciones

Algunos países han elegido tener dos (o más) legislaciones independientes que se apliquen al Gobierno y a las empresas privadas, a nivel nacional. Es el caso de Canadá y México, por ejemplo. En la Unión Europea, existe una legislación independiente para las autoridades encargadas del tratamiento de datos personales a los efectos de la aplicación de la ley.

Privacy International recomienda que la legislación integral de protección de datos se aplique a organismos públicos y privados. En ninguna circunstancia se debe eximir completamente a los organismos públicos o privados de respetar los principios de protección de datos y los derechos de las personas, o de estar sujetos a mecanismos independientes de control y ejecución.

La OCDE ha hecho hincapié en que todas las exenciones a la protección incluidas en una legislación de protección de datos a título de soberanía nacional, seguridad nacional y orden público (ordre public), deberán:

a) limitarse a la mínima cantidad posible y
b) darse a conocer públicamente.

La legislación debe contemplar específicamente el desarrollo y la inclusión de estándares aplicables a la protección de datos personales recogidos y tratados para los fines de seguridad pública, defensa, seguridad estatal e investigación, o prevención de delitos penales.

Estas disposiciones deben, como mínimo, identificar los organismos públicos obligados a recoger y tratar datos personales, respetar y proteger totalmente el derecho a la privacidad y cumplir con los principios de legalidad, necesidad y proporcionalidad identificados por los expertos internacionales en derechos humanos, todo bajo el control de un organismo externo.

Mantengamos los Ojos Abiertos Ante las Exenciones (Especialmente las Generales)

Es muy común que los Gobiernos incluyan exenciones de obligaciones y derechos individuales. Las razones más recurrentes son:

- **seguridad nacional**
- **defensa**
- **seguridad pública**
- **la prevención, investigación, detección o el enjuiciamiento de**
- **delitos penales**
- **intereses públicos**
- **inmigración**
- **intereses económicos o financieros, incluidas las cuestiones presupuestarias y fiscales**
- **salud y seguridad públicas**
- **la protección de la independencia y los procesos de la justicia el control, la inspección o las obligaciones regulatorias relacionadas con el ejercicio de funciones de autoridades oficiales en materia de seguridad, defensa, otros intereses públicos de importancia o la prevención de delitos**
- **la protección de las personas, o los derechos y las libertades de terceros o**
- **la ejecución de legislación civil.**

Las exenciones generales nunca son justificables. En los pocos casos en que son justificables, deben aplicarse únicamente a circunstancias restringidas. Es esencial garantizar que todas las exenciones:

1. **se definan y estén establecidas claramente en la ley**
2. **respeten los derechos y las libertades fundamentales de las personas**
3. **sean medidas necesarias y proporcionales en una sociedad democrática**
4. **solo sean aplicables en los casos en los que, de lo contrario, se perjudicaría el fin legítimo perseguido.**

Excepciones

Una excepción común al alcance de la legislación de protección de datos es el tratamiento de datos personales a cargo de agencias de seguridad e inteligencia. Por lo tanto, resulta esencial que:

1. Todo tratamiento de datos personales, incluida la información inactiva (es decir, las bases de datos gestionadas por el Gobierno), a cargo de agencias de seguridad, agencias de inteligencia y las fuerzas y los cuerpos de seguridad esté sujeto a la legislación de protección de datos.
2. La legislación sea integral y proporcione los más elevados estándares de protección. Todas las excepciones deben ser limitadas, descritas claramente, precisas y sin ambigüedades, darse a conocer públicamente e interpretarse estrictamente según los principios de necesidad y proporcionalidad. Este enfoque ante las excepciones garantizaría que la protección contemplada en la legislación de protección de datos no sea redundante en relación con las funciones de las agencias de seguridad e inteligencia.

Si no se definen y limitan adecuadamente estas excepciones, se socavará la confianza pública en la protección de datos.

Las organizaciones de la sociedad civil y los integrantes de mecanismos de derechos humanos expresan su preocupación por el intercambio de información en actividades de inteligencia

El intercambio de información en actividades de inteligencia que se realiza sin transparencia y de manera irrestricta e injustificada amenaza el fundamento del sistema de derechos humanos y el Estado de derecho. Se debe estipular el régimen de las transferencias de datos personales fuera del territorio nacional realizadas por servicios de inteligencia (dicho régimen debe al menos estar en consonancia con el régimen de transferencias internacionales de datos personales incluido en otra sección de la ley).

El Tribunal Europeo de Derechos Humanos ha expresado su preocupación en cuanto al intercambio de información en actividades de inteligencia, y la necesidad de más regulación y control:

> **Las prácticas cada vez más extendidas de los Gobiernos de transferir e intercambiarse información recuperada mediante actividades secretas de vigilancia... constituyen otro factor que requiere particular atención al momento de realizar una supervisión externa y tomar medidas correctivas**

Al revisar la implementación que hizo el Reino Unido del Pacto Internacional de Derechos Civiles y Políticos, el Comité de Derechos Humanos de las Naciones Unidas destacó específicamente la necesidad de adherir al artículo 17, "incluyendo los principios de legalidad, proporcionalidad y necesidad", al igual que la necesidad de implementar "mecanismos de control efectivos e independientes para el intercambio de datos personales en prácticas de inteligencia".

En el Reino Unido, la Ley de Protección de Datos de 2018 no regula el intercambio transfronterizo de datos personales a cargo de servicios de inteligencia. La sección relevante otorga facultades casi irrestrictas para las transferencias transfronterizas de datos personales a cargo de agencias de inteligencia, sin niveles adecuados de protección.

Privacy International, junto con otras organizaciones de derechos humanos, ha exigido mayor responsabilidad, transparencia y control en los acuerdos de intercambio de inteligencia. Todas las excepciones para los servicios de inteligencia deben interpretarse estrictamente en conformidad con la legislación, y deben ser necesarias y proporcionales para un fin legítimo. Estos acuerdos deben ser objeto de la legislación de protección de datos.

Ámbito de aplicación territorial

La legislación de protección de datos moderna debe tener en cuenta que los datos, incluidos los datos personales, cruzan fronteras. Este hecho da lugar a significativas y complejas problemáticas jurisdiccionales, incluidos posibles conflictos entre las leyes nacionales aplicables. Privacy International cree que la legislación de protección de datos debe concentrarse en las personas: esto significa garantizar que los datos personales de los individuos estén protegidos, independientemente de que la información reciba un tratamiento dentro o fuera del territorio donde se encuentran.

Es posible lograr este tipo de protección de diferentes maneras, por ejemplo garantizando que la legislación:

- Se aplique a los responsables y los encargados del tratamiento establecidos en el país, incluso si el tratamiento se lleva a cabo fuera de la jurisdicción de dicho país
- Se aplique al tratamiento de datos personales realizado por los responsables y los encargados establecidos fuera de la jurisdicción del país donde se encuentra el interesado
- Regule las condiciones para la transferencia de datos personales fuera del territorio del país.[8]

El alcance y la aplicación territoriales de una legislación de protección de datos pueden ser poco claros, y suelen interpretarse de manera muy estrecha, entendiéndose que la ley aplica únicamente al sitio donde se realiza el tratamiento de los datos, es decir, que aplica únicamente a las entidades con base en una jurisdicción en particular, lo que podría ser utilizado por las empresas como fundamento para no ofrecer protección a los usuarios.[9] Sin embargo, dada la globalización de la infraestructura, ya no es adecuado pensar que la protección de datos está restringida a las fronteras del territorio nacional: los marcos de protección de datos han comenzado a exigir una interpretación que contemple la aplicación extraterritorial, de modo que las personas no se vean desprovistas de la protección a la que tienen derecho, a causa del sitio donde los responsables y los encargados del tratamiento tienen su base.

Por ejemplo, en el alcance del RGPD, el artículo 3 incluye a los responsables y encargados del tratamiento que ofrezcan bienes o servicios a individuos en la Unión Europea, o que hagan un seguimiento del comportamiento de personas en la Unión Europea (incluido el seguimiento en línea).

Los legisladores tienen la obligación de proteger los derechos de las personas en su jurisdicción, incluido el derecho a la privacidad y la protección de datos. Por lo tanto, para que las personas no se vean desprovistas de la protección a la que tienen derecho, los marcos de protección de datos deben ser claros en lo concerniente a cómo se aplica la ley y cómo esta protege a las personas en cada una de las siguientes situaciones:

- El responsable/encargado del tratamiento está establecido en la jurisdicción relevante, incluso si el tratamiento se realiza en otro lugar
- El responsable/encargado del tratamiento no está establecido dentro de dicha jurisdicción pero realiza el tratamiento de los datos personales de una persona en dicha jurisdicción y
  Los datos se transfieren a terceros que se encuentran fuera de dicha jurisdicción.

Referencias

1 Artículo 5 de la Ley 1581 de 2012 de Colombia.

2 Un ejemplo es el artículo 2, apartado 2, del Convenio Internacional de Derechos Económicos, Sociales y Culturales, según lo interpretado en la observación general n. o 20: La no discriminación en derechos económicos, sociales y culturales. Disponible en: http://www.refworld.org/docid/4a60961f2.html

3 Los datos biométricos son datos personales que se obtienen a partir de procedimientos técnicos específicos relacionados con las características físicas, fisiológicas o de comportamiento de una persona física, y que permiten o confirman su identificación única, por ejemplo imágenes del rostro o datos dactiloscópicos, artículo (4) (14) del RGDP de la UE.

4 Los “datos genéticos” son datos personales relativos a las características genéticas heredadas o adquiridas de una persona física, que proporcionan una información única sobre su fisiología o su salud, y que se obtienen en particu lar del análisis de una muestra biológica de dicha persona, artículo (4) (13) del RGPD de la UE.

5 Documento técnico del Comité de Expertos para un Marco de Protección de Datos para India, sección 4.3, PDF disponible en http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_18122017_final_v2.1.pdf, pp. 43

6 Esta es la definición proporcionada por el RGPD.

7 Comisión Nacional de Privacidad, La implementación de normas y reglamentos de la Ley de privacidad de Datos de 2012, disponible en https://privacy.gov.ph/implementing-rules-and-regulations-of-republic-act-no-10173-known-as-the-data-privacy-act-of-2012/

8 La definición de “establecimiento” ha sido considerada por el Tribunal de Justicia de la Unión Europea en la Directiva de Protección de Datos de 1995, en el caso de C- 230/14 Weltimmo (consulte los apartados 28, 30 y 31) y C-131/12 Google Spain (consulte el apartado 52).

9 Privacy International, ¿Por qué las empresas como Facebook deben comprometerse a aplicar el RGPD a nivel mundial? Disponible en https://privacyinternational.org/feature/1754/why-should-companies-facebook-commit-applying-gdpr-globally

PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

PARTE: 3

Principios de Protección de Datos

Lealtad, legalidad y transparencia

El tratamiento de datos personales debe ser lícito, leal, y efectuado de manera transparente.

Limitación de finalidad

Los datos personales deben ser tratados para fines específicos, explícitos y legítimos, que deben ser declarados al momento de su recogida, y su tratamiento posterior debe ser compatible con dicha finalidad.

Minimización

El tratamiento de datos personales debe ser adecuado, relevante y limitado a la necesidad o al propósito para el cual están siendo tratados.

Exactitud

El tratamiento de datos personales debe ser exacto y completo, y deben adoptarse medidas para asegurar que permanezcan actualizados.

Limitación de conservación

Los datos personales deben ser almacenados solamente por el período de tiempo necesario para los fines por los que los datos fueron tratados.

Integridad y confidencialidad

Deben adoptarse medidas apropiadas para garantizar la seguridad de los datos y sistemas de tratamiento de información, y para proteger los datos personales contra la pérdida, acceso no autorizado, destrucción, uso, modificación o difusión.

Responsabilidad

Quienes hagan tratamiento de datos personales deben rendir cuentas del cumplimiento con los principios antes señalados y de sus obligaciones, facilitando el ejercicio de derechos por parte de los titulares de datos personales y cumpliendo con los mismos.

Principios de Protección de Datos

Si existe una legislación integral para la protección de datos, las organizaciones públicas o privadas que recopilan y utilizan la información personal de un individuo tienen la obligación de tratar la información según dicha legislación. El tratamiento de datos personales debe realizarse en conformidad con diversos principios derivados de marcos regionales e internacionales.

Lealtad, Legalidad y Transparencia

OCDE: "Deben existir límites a la recogida de datos personales, y dichos datos deben obtenerse por vías lícitas y leales y, si correspondiera, con el conocimiento o consentimiento del interesado."

Convenio 108: "Los datos personales se tratarán legítimamente" y "los datos personales se tratarán... lealmente y de manera transparente". (Artículo 5 [3] y [4] [a])

RGPD: Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado". (Artículo 5 [1] [a])

Los datos personales deben ser tratados de manera lícita y leal. Este principio es fundamental para enfrentar prácticas como la venta o transferencia de datos personales obtenidos de manera fraudulenta. La "lealtad y la transparencia" son esenciales para garantizar que los datos de las personas no se utilicen de manera inesperada. "Lícitos" significa que los datos deben tratarse de una manera que respete el Estado de derecho y que satisfaga un fundamento legal para el tratamiento. Un "fundamento legal" es una justificación restringida para tratar los datos de las personas, que está establecida en la ley (por ej. el consentimiento), lo que trataremos en la sección de "Fundamentos legales para el tratamiento".

¿Por qué importa este principio?

Es fundamental que la persona esté informada claramente y sepa cómo se tratará su información, así como quién lo hará. Si existe la intención de compartir los datos de una persona con terceros, pero el responsable del tratamiento no se maneja con transparencia sobre este hecho y no informa claramente al interesado, es probable que los datos personales del interesado no hayan sido obtenidos de manera leal, por lo que el tratamiento no se considerará transparente.

Por ejemplo, en Irlanda, una empresa de seguros se puso en contacto con uno de sus clientes para darle información sobre una nueva tarjeta de crédito. Sin embargo, no quedó claro para el cliente el hecho de que no era la empresa de seguros la que le proporcionaría la nueva tarjeta y que los datos, en cambio, se habían transferido a un banco para ser tratados (es decir, el banco era el responsable del tratamiento de los datos, y este hecho no había sido aclarado a la persona durante la comunicación recibida por parte de la empresa de seguros). Por lo tanto, se resolvió que los datos no fueron tratados de manera leal.[1]

No solo basta con informar claramente lo que se hará con los datos de las personas: los criterios de legalidad incluidos en este principio implican que una entidad debe tener una justificación para tratar los datos, que satisfaga un fundamento legal.

Limitación de Finalidad

OCDE: "La finalidad para la que se recogen datos personales debe especificarse a más tardar al momento de la recogida, y el uso siguiente debe estar limitado a satisfacer dicha finalidad o aquellas que no sean incompatibles con la misma, y de la manera especificada en cada ocasión que se cambie la finalidad"

Convenio 108: b. "Los datos personales sometidos a tratamiento deben ser recopilados para fines explícitos, especificados y legítimos, y no deben ser tratados de alguna manera incompatible con dichos fines. Asimismo, el tratamiento para fines de archivo en interés público, fines de investigación científica o histórica, o fines estadísticos debe estar sometido a las salvaguardas apropiadas, compatibles con aquellos fines". (Artículo 5 [4] [b])

RGPD: "Los datos personales se deberán recoger con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de

acuerdo con el artículo 89 (1), el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales". (Artículo 5 [1] [b])

Todos los datos personales deben recogerse para fines determinados, específicos y legítimos. Todo tratamiento ulterior debe ser compatible con los fines iniciales (es decir, el punto de recogida). En esencia, esto significa que no es aceptable declarar que se necesitan los datos de una persona para una finalidad, y luego utilizarlos para otra sin notificarlo ni contar con una justificación.

Los avances tecnológicos (y la generación, recolección y análisis en masa de datos que los acompañan) implican que estos principios son más importantes que nunca. La finalidad del tratamiento y el uso propuesto de los datos deben definirse y explicarse claramente a los interesados. Si los datos van a utilizarse para una finalidad diferente a la original, entonces se deberá informar de ello adecuadamente al interesado, junto con identificar una condición jurídica para dicho tratamiento. Es posible que esto requiera obtener un consentimiento adicional. Es particularmente importante que los datos personales sensibles no sean tratados para fines diferentes a los establecidos originalmente.

Esto resulta especialmente relevante en el caso de procesos como el análisis de "big data" y otros tipos de datos. Por ejemplo, la industria de los intermediarios de información prospera gracias al restablecimiento de los fines del uso de los datos:[2] acumulan datos de un vasto número de fuentes, luego los compilan, los analizan, establecen perfiles y comparten perspectivas con sus clientes. Esto significa que una gran cantidad de datos compartidos para un fin se utilizan para una finalidad diferente, de maneras inesperadas, por ejemplo para la publicidad dirigida.

Los datos personales no deben divulgarse, ni estar disponibles o utilizarse para ningún otro fin que no sea el especificado, en conformidad con el "principio de limitación de finalidad".

Sin embargo, existen dos excepciones comunes a este principio. Es aceptable si se realiza:

a) con el consentimiento del interesado o
b) por la autoridad de la ley.

Si bien existe un amplio consenso sobre estas dos excepciones a los principios de limitación de uso, es frecuente que se abuse de ellas o que se apliquen inadecuadamente. En el caso de (a), el consentimiento debe ser válido: no debe ser condicional, obtenido mediante casillas preseleccionadas, y los detalles de estos fines diferentes no deben ocultarse en letra pequeña ni ser expresados en jerga legal (inaccesible para el promedio de los interesados). En el caso de (b), esta excepción ha sido utilizada para permitir amplios acuerdos de intercambio de

datos entre organismos e instituciones del Estado en el ejercicio de sus funciones, por ejemplo, datos proporcionados para fines de atención médica o educación se utilizan para fines migratorios.

Estas exenciones generales amenazan con debilitar la protección ofrecida por la legislación, de modo que resulta fundamental que todas las disposiciones que establezcan excepciones se interpreten de manera estricta para que: el principio de limitación de finalidad no resulte redundante e inválido para las funciones del Estado y los intercambios de información entre agencias estatales, y para que existan límites a la utilización del consentimiento, por ejemplo en los casos donde haya un desequilibrio de poder.

Asimismo, en relación con la limitación de finalidad, el texto de la legislación podría proporcionar diversos fines que no sean incompatibles con este principio.

Entre estos fines se podrían incluir, por ejemplo, los siguientes:

- Fines de archivo en interés público o
- Fines científicos, estadísticos o históricos.

Resulta esencial que estos fines tengan un alcance restringido, y que los términos antes mencionados se definan con mayor precisión para proporcionar claridad sobre lo que podría implicar cada uno de ellos.

¿Por qué importa el principio de limitación de finalidad?

Si no se establecen limitaciones claras en el punto de recogida en lo relativo a los usos de los datos, estos podrían usarse para otros objetivos a lo largo de su ciclo de vida, lo que tendría consecuencias perjudiciales para las personas y daría lugar a abusos. Existe un número creciente de casos en los que se está socavando y eludiendo el principio de limitación de finalidad. Por ejemplo, Aadhaar, la base nacional de datos biométricos de India, fue establecida originalmente en 2009 con el objetivo de estandarizar las bases de datos gubernamentales. Sin embargo, con el transcurso del tiempo, el proyecto se ha vuelto más ambicioso y ahora está siendo utilizado para distintos fines, que incluyen desde las admisiones en las escuelas hasta la obtención de certificados de defunción.[3]Eurodac es una base de datos biométricos que fue establecida en el año 2000 con el objetivo de permitir que los Estados miembros de la Unión Europea verificaran si una persona que buscaba asilo político había aplicado anteriormente para recibirlo en otro país europeo, o si estaba recibiendo beneficios sociales de otro país de la Unión. Ahora, la base de datos se está utilizando para una nueva finalidad. La reglamentación actualizada de Eurodac, que entró en vigor en julio de 2015, permite ahora el "uso de la base de datos de Eurodac de huellas digitales de personas que solicitan asilo político para prevenir, detectar e investigar delitos de terrorismo y otros tipos de delitos graves".[4]

Minimización

OCDE: "Los datos personales deben ser pertinentes a los fines para los que son utilizados, hasta el grado que sea necesario para dichos fines, y deben ser exactos, estar completos y mantenerse al día".

Convenio 108: "Los datos personales sometidos a tratamiento deberán ser adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". (Artículo 5 [4] [c])

RGPD: "Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados". (Artículo 5 [1] [c])

La minimización es un concepto clave en la protección de datos, tanto desde la perspectiva de los derechos de una persona como de la seguridad de la información. La legislación debe estipular con claridad que únicamente se tratarán los datos necesarios y pertinentes al fin declarado. Cualquier excepción a esta estipulación debe ser muy limitada y definirse con suma claridad.

- **Necesidad:** garantizar que el alcance de la recogida de datos no sea mayor al necesario, en función de los fines para los que se usarán dichos datos. La prueba debe ser la utilización del método menos intrusivo para alcanzar una meta legítima.

La "prueba de finalidad" –como la ha llamado la OCDE– "frecuentemente involucrará la problemática de determinar si se perjudicará o no a los interesados con datos recogidos que sean incorrectos o estén incompletos y desactualizados". El concepto de necesidad también implica la realización de una evaluación para saber si es posible lograr el mismo fin de una manera menos intrusiva, es decir, utilizando una menor cantidad de datos.[5]

- **Relevancia:** Todos los datos tratados deben ser pertinentes a los fines establecidos.

¿Por qué importa el principio de minimización de datos?

Este principio requiere que quienes estén a cargo del tratamiento de los datos consideren cuál sería la cantidad mínima de datos necesarios para lograr un fin. Los encargados del tratamiento deberán conservar dicha cantidad y no una cantidad mayor: no es aceptable recoger información adicional alegando que podría ser útil posteriormente, o porque no se ha considerado si será necesaria en un escenario específico.

Por ejemplo, sería excesivo tratar datos precisos y detallados de la localización de los automóviles conectados para un fin que implique el mantenimiento técnico o la optimización de modelos.[6]

El principio de minimización de datos es incluso más integral en la era de la "big data", cuando los avances tecnológicos han mejorado radicalmente las técnicas analíticas de búsqueda, agregación y referencia cruzada de grandes conjuntos de datos para desarrollar inteligencia y perspectivas.[7] Con la promesa y la esperanza de que una mayor cantidad de datos permitirá entender con precisión el comportamiento humano, existe un interés y una intención sostenida de acumular vastas cantidades de datos. Es urgente desafiar este discurso y garantizar que únicamente se traten los datos necesarios y pertinentes a un fin específico.

Exactitud

OCDE: "Los datos personales deben ser pertinentes a los fines para los que son utilizados, en la medida en que sean necesarios para dichos fines, y deben ser exactos, estar completos y mantenerse al día".

Convenio 108: "Los datos personales sometidos a tratamiento deben ser exactos y, de ser necesario, actualizados". (Artículo 5 [4] [d])

RGPD: "Los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan". (Artículo 5 [1] [d])

Los datos personales deben ser exactos durante todo el proceso de tratamiento, y se deben tomar medidas razonables para garantizar que así sea. Esto incluye los siguientes elementos:

- **Exactitud:** todos los datos tratados deben ser exactos durante todo su ciclo de vida
- **Integridad:** todas las categorías de datos deben ser lo más completas que sea posible, para que la omisión de datos relevantes no lleve a inferir información diferente a la que pueda ser obtenida si los datos estuviesen completos
- **Actualización:** se deberán actualizar todos los datos conservados que puedan ser sometidos a un tratamiento adicional, en conformidad con las disposiciones contempladas en la legislación de protección de datos
- **Limitación:** los datos personales podrán ser tratados (y conservados) únicamente durante el periodo requerido para el fin por el que se recogieron y conservaron.

Los elementos anteriores reafirman los derechos de los interesados a acceder a sus datos personales y corregir aquellos que estén incompletos, que sean inexactos o estén desactualizados, todo lo cual debe estar estipulado en la legislación de protección de datos.

¿Por qué importa el principio de exactitud?

Cada vez con mayor frecuencia, los procesos de toma de decisiones y elaboración de políticas dependen de los datos. Sin embargo, si los datos no son exactos y no están actualizados, existe un alto riesgo de que el resultado del proceso de toma de decisiones también sea inexacto. En los casos más graves, esto podría dar lugar a la decisión de no otorgar a una persona el acceso a servicios públicos o programas de bienestar, o que no se le permita acceder a préstamos. Por ejemplo, ha habido casos de personas a las que equivocadamente se les denegó un préstamo o una hipoteca de su casa porque la empresa a cargo de revisar la calificación crediticia tenía información incorrecta (lo que había disminuido la evaluación de “excelente” a “insatisfactoria”), o porque las instituciones bancarias habían registrado información inexacta, convirtiendo así a una persona en un cliente no deseable.[8]

Limitación de conservación

Convenio 108: "Los datos personales sometidos a tratamiento automatizado deberán conservarse de una manera que permita la identificación de los sujetos de datos por una cantidad de tiempo que no supere el periodo necesario para los fines por los que los datos fueron tratados [Artículo 5(e)]

RGPD: "Los datos personales sometidos a tratamiento deberán conservarse de una manera que permita la identificación de los interesados únicamente durante el periodo necesario para los fines por los que los datos fueron tratados; es posible conservar los datos personales durante periodos más prolongados siempre y cuando sean tratados únicamente para fines de archivo en interés público o para fines estadísticos, en conformidad con el artículo 89 (1), sujeto a la implementación de las medidas técnicas y organizativas apropiadas requeridas por la presente reglamentación para salvaguardar los derechos y las libertades de los interesados". (Artículo 5 [1] [e])

Los datos personales deben conservarse únicamente durante el periodo requerido por el fin para el que se recogieron y almacenaron. Esto reforzará y clarificará la obligación de eliminar los datos al final de su tratamiento, lo que debe incluirse en otra disposición.

La legislación debe estipular claramente que los datos no deben conservarse más tiempo de lo necesario para el fin por el que se obtuvieron originalmente. Cualquier excepción a esta estipulación debe ser muy limitada y definirse con suma claridad.

El hecho de que el responsable del tratamiento de los datos podría encontrar otro uso para ellos no justifica una conservación indefinida o generalizada. El tiempo necesario que se deben conservar los datos dependerá del contexto. Sin embargo, deben existir al respecto otras obligaciones legislativas y orientaciones regulatorias. Para que las personas sean informadas de manera leal sobre el tratamiento de sus datos, es obligatorio comunicarles también cuánto tiempo se conservarán dichos datos. Por lo tanto, es imperativo que la legislación incentive a los responsables del tratamiento a implementar el principio de minimización de datos, reduciendo así la recogida de información y evitando su conservación por más tiempo del necesario.

Los responsables del tratamiento deben establecer cronogramas de conservación que especifiquen los periodos que deben retenerse todos los datos que poseen. Estos cronogramas deben revisarse de manera periódica. La conservación de los datos personales es diferente de la eliminación de los datos personales a solicitud del interesado, lo que también debe estar contemplado en la legislación. Después del tiempo necesario, los datos personales deben eliminarse de manera segura. Si se retienen los datos de forma anonimizada (y no seudonimizada) por un tiempo mayor al periodo de conservación, se deben considerar atentamente las implicancias y consecuencias para la privacidad de los interesados.

¿Por qué importa el principio de limitación de conservación?

Incluso si los datos han sido tratados de manera leal, lícita y transparente, y respetando los principios de limitación de finalidad, minimización y exactitud, es esencial garantizar que no se conservarán durante más tiempo del requerido por el fin para el que se han recogido.

Cualquier interferencia con el derecho a la privacidad y la protección de los datos debe ser necesaria y proporcional. La conservación general de datos no respeta en ningún sentido esta obligación, como se confirmó en 2014, cuando el Tribunal de Justicia Europeo revocó la Directiva de Conservación de Datos, definiendo la conservación obligatoria de datos como "una interferencia con los derechos fundamentales de prácticamente la totalidad de la población europea... cuando dicha interferencia no haya sido restringida de manera precisa mediante disposiciones para garantizar que se limite de hecho a lo estrictamente necesario". Esta decisión representó un sólido reconocimiento de autoridad de las salvaguardas que deben existir para proteger nuestro derecho a la privacidad.[9]

La conservación indefinida de datos no es únicamente una violación de los derechos de una persona, sino también un riesgo para los encargados de su tratamiento. Si no se limita el periodo de conservación, aumentan los riesgos de seguridad y surge la inquietud de que podrían utilizarse para nuevos fines únicamente porque todavía están disponibles y se puede acceder a ellos. Si los datos se vuelven obsoletos, existe el riesgo de que los procesos de toma de decisiones sean insatisfactorios, lo que tendría graves implicancias.

En la era de la vigilancia estatal y corporativa extendida y no regulada, es esencial que existan limitaciones estrictas a la conservación de datos para mitigar posibles interferencias ilegales con el derecho a la privacidad. [10]

Integridad y Confidencialidad

OCDE: "Los datos personales deben estar protegidos mediante salvaguardas de seguridad razonables contra riesgos como pérdidas o acceso no autorizado, destrucción, uso, modificación o divulgación".

Convenio 108: "Cada parte deberá garantizar que el responsable del tratamiento y, si correspondiera, el encargado, adopte las medidas de seguridad adecuadas para la protección de datos contra el acceso, la destrucción, la pérdida, el uso, la modificación o la difusión no autorizados o accidentales". (Artículo 7 [1])

RGPD: "Los datos personales deberán ser tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas" (Artículo 5 [1] [f])

Los datos personales, tanto los que se encuentran almacenados como los que están en tránsito, al igual que la infraestructura de la que depende el tratamiento, deben estar protegidos por medidas de seguridad contra riesgos como el acceso, el uso o la divulgación ilegal o no autorizada, pérdidas, destrucción o daños que puedan sufrir los datos.

Entre las salvaguardas de seguridad se pueden incluir:

- Medidas físicas, es decir, seguros en las puertas y tarjetas de identificación
- Medidas organizativas, es decir, controles de acceso a la información
- Medidas relativas a la información, como la codificación (la conversión de un texto en código), y el monitoreo de amenazas
- Medidas técnicas, tales como la encriptación, seudonimización, o anonimización.

Otras medidas organizativas incluyen la prueba periódica de la adecuación de estas medidas, la implementación de políticas de protección de datos y seguridad de la información, y la capacitación y adhesión a códigos de conducta reconocidos.

¿Por qué importa el principio de salvaguardas de seguridad?

Si no se toman medidas de seguridad para proteger los datos y garantizar la seguridad de la infraestructura, la información será vulnerable a amenazas, violaciones y accesos ilegales. Hay múltiples ejemplos de violaciones de datos como resultado de un sistema de seguridad frágil.

Por ejemplo, en marzo de 2016, se filtró la información personal de más de 55 millones de votantes filipinos después de una violación a la base de datos de la Comisión Electoral (COMELEC). En septiembre de 2016, la Comisión Nacional de Privacidad concluyó que había existido una violación al sistema de seguridad, mediante la cual se pudo acceder a la base de datos de COMELEC, que incluía datos personales y sensibles, y otro tipo de información que podía llegar a utilizarse para habilitar el fraude de identidad. Los datos personales de la base de datos comprometida incluían información de pasaportes, números de identificación fiscal, nombres de propietarios de armas de fuego e información sobre sus armas y direcciones de correos electrónicos. Mediante un informe[11] preliminar, se detectó que uno de los indicadores de negligencia por parte de la COMELEC fueron las vulnerabilidades de su sitio web y la falta de seguimiento periódico para detectar violaciones al sistema de seguridad.

En julio de 2016, debido a fallas de seguridad, se publicó una base de datos de la municipalidad de São Paulo en Brasil, que expuso información[12] personal de aproximadamente 650 000 pacientes y agentes públicos del sistema de salud pública (SUS). Entre los datos se incluían direcciones, números de teléfono e incluso información médica. También se divulgaron datos relacionados con etapas de embarazos y casos de aborto.

Principio de responsabilidad

OCDE: "El responsable del tratamiento de los datos debe rendir cuentas del cumplimiento de las medidas que dan efecto a los principios antes mencionados".

Convenio 108: "Cada parte garantizará que el responsable del tratamiento de datos y, si correspondiera, el encargado, adopte las medidas necesarias para cumplir con las obligaciones del presente convenio y pueda demostrar, sujeto a la legislación doméstica adoptada en conformidad con el artículo 11, apartado 3, en particular en relación con la autoridad de control competente dispuesta en el artículo 15, que el tratamiento de datos a su cargo se lleva a cabo en conformidad con las disposiciones del presente convenio". (Artículo 10 [1])

RGPD: "El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo [13] ("responsabilidad proactiva")". (Artículo 5 [2])

La entidad que realiza el tratamiento de los datos personales, en su capacidad de responsable o encargado del mismo, debe dar cuenta del cumplimiento de los estándares y de tomar las medidas necesarias para dar efecto a las disposiciones provistas en la legislación de protección de datos. Quienes tengan la responsabilidad del tratamiento de los datos deben ser capaces de demostrar cómo cumplen con la legislación de protección de datos, incluidos los principios, sus obligaciones y los derechos de las personas.

¿Por qué importa el principio de responsabilidad?

El principio de responsabilidad es fundamental para que el marco de protección de datos sea efectivo. Reúne todos los demás principios y exige a quienes realizan el tratamiento de datos de personas (ya sea una empresa o una autoridad pública) asumir la responsabilidad de demostrar el cumplimiento de sus obligaciones. En la práctica, esto significa que quienes están a cargo del tratamiento deben demostrar más transparencia y proactividad en la manera en que manipulan los datos, en conformidad con sus obligaciones. Deben ser capaces de explicar, demostrar y probar que respetan la privacidad de las personas, tanto ante las entidades reguladoras como ante las personas.

La importancia del principio de responsabilidad resulta más evidente al considerar contextos en los que no existen mecanismos de responsabilidad, es decir, donde no existe una estructura mediante la cual informar las violaciones a la legislación.

Por ejemplo, en Sudáfrica, la Ley de Protección de la Información Personal (PoPI) se adoptó en 2013, y contemplaba el establecimiento de reguladores de la información, aunque este cuerpo no se materializó hasta abril de 2017. En la actualidad, las violaciones de datos en Sudáfrica no suelen informarse: en 2015, se registraron solo cinco violaciones de datos en el país.[14] Se espera que esta realidad cambie significativamente a medida que la ley PoPI entre en vigor, porque las partes responsables se verán obligadas jurídicamente a divulgar la información sobre las violaciones de datos en caso de que sucedan.

Los mecanismos de responsabilidad resultan de importancia para investigar las violaciones y exigir el rendimiento de cuentas a las entidades sujetas a la ley. En 2017, luego de que se hiciera pública una violación importante de datos de la aplicación de taxis Uber en 2016, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales de México (INAI) solicitó a Uber información sobre la cantidad de "usuarios, conductores y empleados mexicanos" que habían sido afectados.[15] El instituto también solicitó a Uber información sobre las medidas que estaba tomando la empresa para mitigar los daños y proteger la información de los clientes.

Referencias

1 Comisión de Protección de Datos (Irlanda), Estudio de caso 1/01, disponible en https://www.dataprotection.ie/docs/Case-Study-1-01-Bank-and-Insurance-Company/121.htm

2 Privacy International, ¿Cómo obtienen nuestros datos las empresas?, disponible en https://www.privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

3 The Centre for Internet and Society, La Ley Aadhaar y su incumplimiento con la ley de protección de datos en India, 14 de abril de 2016, disponible en https://cis-india.org/internet-governance/blog/aadhaar-act-and-its-non-compliance-with-data-protection-law-in-india y Usha Ramanathan, Aadhaar: desde la compilación de una base de datos gubernamental hasta la creación de una sociedad bajo vigilancia, Hindustan Times, enero de 2018, disponible en https://www.hindustantimes.com/opinion/aadhaar-from-compiling-a-govt-database-to-creating-a-surveillance-society/story-Jj36c6tVyHJMjOhCI8vnBN.html

4 Costica Dumbrava, Los sistemas de información europeos en el área de la justicia y los asuntos domésticos: una perspectiva general, Blog del Servicio de Investigación Parlamentario Europeo, 15 de mayo de 2017, disponible en https://epthinktank.eu/2017/05/15/european-information-systems-in-the-area-of-justice-and-home-affairs-an-overview/

5 Por ejemplo, consulte el caso CJEU de Osterreichischer Rundfunk C-138/01 2003.

6 Commission National Informatique & Libertes, Paquete de cumplimiento: vehículos conectados y datos personales, PDF disponible en https://www.cnil.fr/sites/default/files/atoms/files/cnil_pack_vehicules_connectes_gb.pdf

7 Privacy International, Big Data - Documento explicativo, disponible en https://privacyinternational.org/explainer/1310/big-data

8 Maria LaMagna, La razón por la que se rechazó su solicitud de préstamo puede no tener nada que ver con su calificación crediticia, MarketWatch, 29 de marzo de 2017, disponible en https://www.marketwatch.com/story/the-reason-your-loan-application-is-rejected-may-have-nothing-to-do-with-your-credit-score-2017-03-29; Anna Tims, El error cometido por Equifax en mi calificación crediticia casi me cuesta una hipoteca, The Guardian, 14 de febrero de 2017, disponible en https://www.theguardian.com/money/2017/feb/14/credit-rating-remortgage-equifax-experian-callcredit y Anna Tims, La manera en que las agencias de calificación crediticia pueden ayudar o destruir a las personas, The Guardian, 17 de julio de 2017, disponible en https://www.theguardian.com/money/2017/jul/17/credit-score-angencies-break-lives-lenders-no-mortgage

9 Tribunal de Justicia de la Unión Europea, El Tribunal de Justicia declara inválida la Directiva de Conservación de Datos, Curia, PDF disponible en https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

10 Privacy International, La vigilancia en tela de juicio, disponible en https://www.privacyinternational.org/programmes/contesting-surveillance y Privacy International, La explotación de datos en tela de juicio, disponible en https://www.privacyinternational.org/programmes/challenging-data-exploitation

11 Foundation for Media Alternatives, La Comisión Nacional de Privacidad emitirá informe sobre la violación de la base de datos de Comelec, disponible en http://www.fma.ph/?p=399

12 Raphael Hernandes, Gestao Haddad expoe na internet dados de pacientes de rede publica, Folha de S. Paulo, 6 de julio de 2016, disponible (en portugués) en http://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados-de-pacientes-da-rede-publica.shtml

13 El apartado 1 del artículo 5 del RGPD describe los principios relacionados con el tratamiento de datos personales.

14 Duncan Alfreds, Sudáfrica no hace públicas las violaciones de datos – asegura empresa experta, Fin24, 26 de febrero de 2016, disponible en https://www.fin24.com/Tech/Cyber-Security/sa-fails-to-make-data-breaches-public-expert-20160226

15 R3D: Red en Defensa de los Derechos Digitales, El INAI pide a Uber revelar si robo masivo de datos afectó a usuarios mexicanos, disponible (en español) en https://r3d.mx/2017/12/01/inai-pide-a-uber-revelar-si-robo-masivo-de-datos-afecto-a-usuarios-mexicanos/#more-4034

PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

PARTE: 4

Derechos de Los Interesados

Derechos de Los Interesados

Derecho a la información

Las personas deben ser informadas acerca de cómo se procesan sus datos personales, tanto cuando se los han proporcionado directamente a un responsable del tratamiento de datos como cuando el responsable lo ha obtenido de otra fuente, como un tercero.

Derecho al acceso

Las personas deben ser informadas cuando sus datos personales están siendo recogidos, y deben tener la capacidad de obtener (tanto solicitar como recibir) información sobre el procesamiento de sus datos personales

Derecho a oposición

Las personas deben tener el derecho de oponerse a que sus datos personales sean tratados.

Derechos a la rectificación, bloqueo y borrado

Las personas deben tener el derecho de rectificar, borrar o bloquear sus datos personales, para asegurar que cualquier tratamiento sobre los mismos sea preciso, completo y actualizado.

Derechos relacionados al perfilamiento y la toma automatizada de decisiones

Todos los derechos contenidos en la ley deben aplicar al perfilamiento y la toma automatizada de decisiones, e incluir el derecho a requerir intervención humana o impugnar tales decisiones.

Derecho a la portabilidad de datos

Las personas deben tener el derecho de obtener todos sus datos personales del responsable del tratamiento de datos en un formato universal que sea legible por máquinas, o que esos datos puedan ser portados a otro servicio en caso de que lo soliciten.

Derecho a tutela judicial efectiva

Las personas deben tener el derecho a interponer recursos judiciales efectivos cuando consideren que sus datos personales no han sido tratados en conformidad con la ley.

Derecho a compensación

Una persona cuyos derechos han sido violados tienen el derecho a obtener una compensación por los daños -materiales o morales- que hayan sufrido.

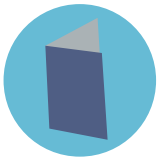
Derechos de Los Interesados

Un componente fundamental de cualquier legislación de protección de datos es la contemplación de los derechos de las personas, a quienes se suele llamar interesados.

Estos derechos deben aparecer al inicio de la ley, debido a que se consideran aplicables a toda la legislación y subyacen a todas las disposiciones. Estos derechos imponen obligaciones positivas a los responsables del tratamiento de los datos, y su cumplimiento debe ser exigido ante autoridades y órganos jurisdiccionales independientes de protección de datos.

Como mínimo, se deben incluir los siguientes derechos:

- Derecho a la información,
- Derecho al acceso,
- Derechos a la rectificación, el bloqueo y la eliminación
- Derecho de objeción,
- Derecho a la portabilidad de datos,
- Derechos relacionados con la elaboración de perfiles,
- Derechos relaconados con las decisiones automatizadas,
- Derecho a recursos judiciales efectivos,
- Derecho a indemnización y responsabilidad.



Derecho a la Información

Las personas deben recibir información sobre cómo se está llevando a cabo el tratamiento de sus datos personales, ya sea que los hayan proporcionado directamente a un responsable de tratamiento, o que el responsable los haya obtenido de otra fuente.

Las personas deben recibir al menos la siguiente información:

- la identidad del responsable del tratamiento (y los datos de contacto)
- la finalidad del tratamiento
- el fundamento legal del tratamiento
- las categorías de datos personales
- los destinatarios de los datos personales
- si el responsable del tratamiento tiene el objetivo de transferir los datos a un tercer país, y el nivel de protección provista
- el tiempo que se conservarán los datos personales
- la contemplación de los derechos del interesado

- el derecho a presentar una reclamación ante la autoridad de control
- la existencia de una elaboración de perfil, incluido el fundamento legal, el significado y las consecuencias previstas que dicho tratamiento tendrá para el interesado
- la existencia de un proceso de toma de decisiones automatizadas y, al menos, información significativa sobre la lógica implicada, el significado y las consecuencias previstas que dicho tratamiento de los datos tendrá para el interesado
- la fuente de la que se obtienen los datos personales (si no se obtienen a través del interesado)
- si la provisión de datos es obligatoria o voluntaria
- las consecuencias de no proporcionar los datos.

La toma de decisiones informadas y el conocimiento de sus derechos

Las personas deben recibir información sobre cuándo, por qué motivo y cómo se están tratando sus datos personales, a fin de que puedan tomar una decisión informada para determinar si utilizar o no un sistema o un servicio, compartir sus datos y ejercer sus derechos.

Las funcionalidades y los aspectos técnicos de los servicios implican que, a nivel técnico, el responsable del tratamiento podría estar tratándolos incluso sin que la persona lo supiera. Por ejemplo, algunas aplicaciones realizan un tratamiento de vastas cantidades de datos sobre sus usuarios. Sin embargo, el usuario recibe poca o ninguna información sobre este hecho, y cuando se le informa al respecto, no la comprende. En el caso de la aplicación NaMo, los permisos relacionados con los datos no eran obligatorios y solo podían encontrarse en la sección “Obtenga más información” de la aplicación. Como consecuencia, los usuarios no recibieron información sobre qué datos eran sometidos a tratamiento por la aplicación al descargarla.[1]

Derecho al Acceso

Para permitir a un interesado ejercer y gozar de sus derechos, y para que el cumplimiento de esos derechos sea efectivo, el interesado debe poder obtener (es decir, solicitar y recibir de vuelta) información sobre la recogida, el almacenamiento o el uso de sus datos personales. La información debe incluir, al menos, la confirmación de que un responsable está a cargo del tratamiento de los datos sobre dicha persona, la finalidad del tratamiento, su fundamento legal, de qué fuente se obtuvieron los datos, con quién o quiénes podrían compartirse/se han compartido y durante cuánto tiempo se conservarán, además de información sobre cómo se utilizan dichos datos en la elaboración de perfiles y la toma de decisiones automatizadas. Esta información debe estar acompañada por una copia de los datos solicitados.

No basta únicamente con respetar el derecho. La legislación debe proporcionar requisitos mínimos, incluso para obtener datos relacionados con dichos requisitos. Entre estos requisitos se incluyen:

- Lapso de tiempo: el procedimiento de obtención de datos debe llevarse
- Costo: obtener información sobre el tratamiento y una copia de sus datos personales no debe representar ningún costo para las personas.
- Formato: la información proporcionada al interesado debe estar en un formato inteligible para él y que no requiera contar con ninguna experiencia o conocimiento en particular para ser comprendida.
- Explicación y apelación: si la solicitud es denegada, el interesado tiene el derecho a que se le informe por qué motivos, y el derecho a apelar dicha denegación. Asimismo, si la apelación resulta exitosa, el interesado debe tener el derecho a que se eliminen, rectifiquen, completen o enmienden los datos.
- Claridad: si habrá exenciones a este derecho, deberán estar establecidas claramente en la legislación, y se deberá explicar su aplicación al interesado.

Los derechos de acceso son una herramienta importante para que las personas, los periodistas y la sociedad civil puedan investigar, revisar y exponer la manera en que se tratan sus datos personales. Una legislación clara y prescriptiva es el punto de partida necesario para gozar de estos derechos en la práctica.

El Derecho al Acceso en la Práctica

El derecho al acceso es un derecho esencial para que las personas sepan qué datos personales están siendo tratados y de qué manera. Acceder a sus datos permite posteriormente a las personas corroborar que estén siendo tratados en conformidad con la ley y sus expectativas y que sean exactos, además de determinar si desean tomar medidas adicionales, como ejercer su derecho de objeción. Esto puede ayudarlas a saber por qué se tomaron decisiones, y también a exponer prácticas de datos abusivas. Este sería el caso de contextos como el empleo, la atención de la salud, la educación, los servicios financieros o los servicios en línea. En Privacy International hemos realizado solicitudes de acceso para entender cómo se están tratando los datos sobre automóviles[2] y cómo utilizan nuestros datos las empresas, por ejemplo los intermediarios de información, en un ecosistema de datos mayormente oculto.[3] Se han utilizado solicitudes de acceso para conocer el uso de datos en elecciones,[4] aplicaciones de citas[5] y proveedores de telecomunicación,[6] para mencionar tan solo algunos ejemplos.

Derechos de los interesados en las directrices de la OCDE

Principio de transparencia

12. Debe existir una política general de transparencia en cuanto a los desarrollos, las prácticas y las políticas relacionadas con los datos personales. Se debe disponer oportunamente de los medios para establecer la existencia y la naturaleza de los datos personales y la principal finalidad de su uso, al igual que la identidad y la residencia habitual del responsable del tratamiento.

Principio de participación individual

13. Toda persona debe tener el derecho a:
a) obtener de parte de un responsable del tratamiento, o de alguna otra manera, la confirmación de que dicho responsable posee o no datos suyos;
b) recibir datos relativos a su persona dentro de un periodo razonable;
con un cargo, si existiera, que no sea excesivo, de manera razonable y en un formato que le resulte oportunamente inteligible;
c) recibir las explicaciones pertinentes si una solicitud realizada según los subapartados (a) y (b) es denegada, y tener la posibilidad de apelar dicha denegación e[7]
d) impugnar los datos relativos a su persona y, si la impugnación es exitosa, exigir que dichos datos se eliminen, rectifiquen, completen o enmienden.

Derechos a la Rectificación, el Bloqueo y la Eliminación

Todo interesado tiene el derecho a rectificar y bloquear (restringir) datos tratados sobre su persona para garantizar que sean exactos, que estén completos y se mantengan actualizados, y que no se utilicen para tomar decisiones sobre su persona cuando la exactitud sea impugnada.

Toda persona debe tener el derecho a exigir que el responsable del tratamiento corrija, actualice o modifique los datos si fueran inexactos, erróneos, confusos o estuvieran incompletos.

Las personas también tienen el derecho a “bloquear” o suprimir el tratamiento de datos personales en circunstancias particulares. En dichos casos, será posible conservar los datos personales pero no podrán seguir siendo tratados hasta que se resuelva la controversia.

Otro de los derechos incluidos en muchos marcos de protección de datos, por ejemplo el RGPD, en Nigeria y Sudáfrica, es el derecho a la eliminación. El derecho a la eliminación permite a los interesados, en determinadas circunstancias (es decir, cuando no existe un fundamento legal para el tratamiento), solicitar que el responsable del tratamiento elimine sus datos personales, cese cualquier otra difusión de los mismos y, potencialmente, exija a terceros dejar de tratarlos. Es

importante que, entre otras salvaguardas, se garantice que, al momento de tratar la solicitud, el responsable del tratamiento considere el interés público de los datos que permanezcan disponibles. Es esencial que este tipo de derecho proporcione salvaguardas claras y, en particular, exenciones para la libertad de expresión. Se deben considerar detenidamente la consolidación de este derecho y su funcionamiento en el contexto nacional para garantizar que no sean vulnerables a abusos.

La diferencia que puede marcar la rectificación de datos

Considerando los procesos de toma de decisiones basados en datos que están siendo adoptados tanto por los Gobiernos como por la industria, y dada la naturaleza automatizada del tratamiento de datos (por la que es posible que una persona desconozca que sus datos personales están siendo tratados), resulta más importante que nunca garantizar la exactitud de los datos tratados.

Si se tratan datos médicos inexactos, se podría dar lugar a que las personas no recibieran la asistencia médica que necesitan. Un error en la dirección postal que conserva una agencia de informes crediticios de consumidores podría ser causa de que alguien recibiera una calificación crediticia insatisfactoria (aunque incorrecta) y que, por lo tanto, le rechazaran una solicitud de hipoteca, como ocurrió con Equifax Inc.[8]

El Comité de Derechos Humanos de la ONU, al interpretar el alcance de las obligaciones de las partes estatales en virtud del Pacto Internacional de Derechos Civiles y Políticos (del que India es parte desde 1979), destacó observación general n.º 16 del artículo 17 PIDCP en el año 1989, que:

> **“Para gozar de la protección más efectiva de su vida privada, toda persona debe tener el derecho de verificar si hay datos personales suyos almacenados en archivos automáticos de datos y, en caso afirmativo, de obtener información inteligible sobre cuáles son esos datos y con qué fin se han almacenado. Asimismo, toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar esos archivos. Si esos archivos contienen datos personales incorrectos, o si se han compilado o tratado en contravención de las disposiciones legales, toda persona debe tener derecho a pedir su rectificación o eliminación”.**

Derecho de Objeción

Toda persona tiene el derecho de objetar el tratamiento de sus datos en cualquier momento. Si la persona realiza la objeción, el responsable del tratamiento deberá proporcionar pruebas de la necesidad de continuar el tratamiento de la información de dicha persona, con razones que prevalezcan sobre los intereses, derechos y libertades del interesado. Algunos derechos de objeción deben ser absolutos, por ejemplo en relación con la comercialización directa.

Implementación del derecho de objeción: la exclusión como mecanismo predeterminado

Cuando se trata de la comercialización directa, el mecanismo de exclusión era anteriormente el enfoque estándar. Sin embargo, en países asiáticos se establecieron nuevas restricciones: Hong Kong y Corea del Sur han aprobado requisitos más estrictos de exclusión, con severas penalidades financieras por incumplimiento. Los demás países (excepto Singapur y Filipinas) poseen algunas restricciones para la comercialización directa.[9]

Derecho a la Portabilidad de Datos

Toda persona debe tener el derecho a solicitar que le entreguen, en un formato universalmente legible por máquinas, los datos personales que estén siendo tratados por el responsable del tratamiento. También tiene el derecho a solicitar que dichos datos sean transmitidos a otro servicio con su consentimiento específico. Este derecho contribuye a garantizar que el interesado ocupe la posición central de la legislación y tenga todas las facultades sobre sus datos personales.

Derechos Relacionados con la Elaboración de Perfiles y las Decisiones Automatizadas

La legislación de protección de datos debe proporcionar una protección efectiva y derechos relativos a la elaboración de perfiles y las decisiones automatizadas. Debe incluir, además de todos los derechos antes mencionados, derechos y garantías adicionales que se aplican exclusivamente tanto a la elaboración de perfiles como a las decisiones automatizadas, para abordar inquietudes específicas relacionadas con estas formas de tratamiento.

Estos derechos no deben abordarse en conjunto porque se podría dar lugar a una confusión innecesaria. Sin embargo, es importante que ambos tipos de derechos estén incluidos en el marco de protección de datos.

Elaboración de perfiles

La elaboración de perfiles tiene lugar en diferentes contextos y por diferentes motivos, desde la publicidad dirigida y los exámenes de atención médica, hasta la actuación policial predictiva. La elaboración de perfiles como proceso reconoce el hecho de que es posible derivar, inferir y predecir datos a partir de otros datos. Esto puede usarse para medir, clasificar y evaluar a las personas, y para tomar e informar decisiones sobre ellas que pueden o no ser automatizadas. Mediante la elaboración de perfiles, es posible incluso inferir datos sensibles (es decir, datos que revelan las características particularmente sensibles de una persona como su raza, sus convicciones políticas, religiosas o filosóficas, datos biométricos o médicos, etc.) a partir de datos no sensibles.

La elaboración de perfiles, al igual que cualquier forma de tratamiento de datos, también debe tener un fundamento legal. La legislación debe exigir que las organizaciones que elaboran perfiles sean transparentes en su proceder y que informen a las personas sobre el procedimiento. Las personas también deben conocer las inferencias de preferencias y características sensibles, incluso cuando se derivan de datos que no son sensibles per se. Debido a que la identificación, clasificación y apreciación incorrectas son un riesgo inevitable asociado con la elaboración de perfiles, los responsables del tratamiento también deben notificar al interesado sobre dichos riesgos y los derechos que lo protegen, incluido el derecho al acceso, la rectificación y la eliminación. Se deben aplicar los derechos de una persona a los datos derivados, inferidos y anticipados, en la medida en que se consideran datos personales.

La elaboración de perfiles en la práctica: la publicidad dirigida en línea

En este contexto, las empresas de datos recogen información de personas que no son consumidores. Los datos se recogen de diferentes fuentes públicas y privadas,[10] tanto en representación de clientes como para los fines propios de dichas empresas. Estas empresas elaboran perfiles recopilando, analizando y evaluando la información sobre las personas, y clasificándolas en determinadas categorías y segmentos.

Los perfiles se utilizan para publicidades dirigidas en línea que pueden ser invasivas[11] y manipuladoras, además de tener el potencial de contribuir con la exclusión o discriminación de personas. Un estudio realizado en 2015 por investigadores de la Carnegie Mellon University demostró, por ejemplo, que el sistema de publicidad en línea de Google ofrecía un anuncio de empleos de altos ingresos a los hombres con mucha más frecuencia que a las mujeres.[12] El estudio sugiere que este tipo de discriminación podría ser el resultado de un

> posicionamiento inadecuado de ofertas por parte de los anunciantes, o una consecuencia inesperada del impredecible aprendizaje de máquina a gran escala. Sea intencional o no, este tipo de discriminación es un riesgo inherente a la publicidad dirigida, y es imposible que las personas lo detecten.

Decisiones automatizadas

Como resultado de los avances y las innovaciones tecnológicas, y el significativo aumento de datos generados, existen nuevas maneras de tratamiento de datos personales. Los datos están jugando un papel cada vez más importante en la toma de decisiones.[13]

Cada vez se depende con mayor frecuencia de las decisiones automatizadas, lo que dificulta la interpretación o la auditoría de los procesos de toma de decisiones. Asimismo, este tipo de decisiones pueden ser inexactas, injustas o discriminatorias.

> **Las decisiones automatizadas en la práctica**
>
> Un ejemplo es el uso de puntuaciones de riesgos automatizadas en el sistema de justicia penal. El software patentado, como el sistema de evaluación de riesgos COMPAS, que ha sido sancionado por el Tribunal Supremo de Wisconsin en 2016, calcula una puntuación que indica el grado de probabilidad de que una persona cometa un delito en el futuro.[14] Aunque la decisión final es tomada formalmente por un juez, la decisión automatizada generada por un programa puede ser decisiva, especialmente si los jueces confían exclusivamente en ella o no han recibido advertencias sobre los riesgos de hacerlo o sobre la probabilidad de que el software produzca decisiones inexactas, discriminatorias o injustas.

Debido a los elevados riesgos para los derechos y las libertadas humanas, y los problemas relacionados con la lealtad, transparencia y responsabilidad, los marcos de protección de datos pueden imponer restricciones y salvaguardas para la manera de utilizar los datos en la toma decisiones. Estas salvaguardas deben consolidar el derecho de no ser objeto de determinadas decisiones automatizadas, especialmente si estas decisiones tienen consecuencias para las personas y afectan sus derechos.

Las personas deben tener el derecho a no ser objeto de tomas de decisiones exclusivamente automatizadas. Es importante que la legislación encuadre este derecho como una clara prohibición de decisiones automatizadas, que proteja a las personas de manera predeterminada. La legislación puede contemplar ciertas exenciones, por ejemplo, cuando las decisiones se basan en una ley (por ej. para prevenir fraudes) o cuando la persona ha proporcionado su consentimiento explícitamente. Sin embargo, este tipo de exenciones deben ser limitadas, y estar clara e inequívocamente definidas. La legislación debe ofrecer claridad respecto a qué tipo de decisiones se aplica este derecho. Por ejemplo, en el RGPD, el artículo

22 contempla derechos solamente en relación con decisiones automatizadas que produzcan efectos jurídicos o afecten significativamente de modo similar. El significado de estos conceptos no está totalmente claro en la primera parte de la legislación y ha sido necesaria una orientación que especifica que una decisión con involucramiento humano elaborado también es objeto de salvaguardas y que, entre los efectos jurídicos o que afecten significativamente de modo similar se incluyen: la denegación de subsidios familiares o de vivienda, la denegación a un cruce de frontera, estar sujeto a una mayor cantidad de medidas de seguridad o vigilancia, la desconexión automática del servicio de telefonía móvil por violación de contrato, la denegación automática de una solicitud de crédito en línea y las prácticas de reclutamiento electrónico sin intervención humana.

Derecho a la intervención humana

Incluso en los casos en que las exenciones permiten las decisiones automatizadas, las personas deben tener el derecho a obtener intervención humana.

Las decisiones automatizadas sin intervención humana deben ser objeto de limitaciones muy estrictas. Esto resulta de particular importancia en el sector de las fuerzas y los cuerpos de seguridad, dado que un potencial error puede perjudicar a una persona e impactar en su bienestar para toda la vida.

Como antes se mencionó en referencia a las orientaciones sobre las decisiones automatizadas y la elaboración de perfiles desarrolladas por el Grupo de trabajo del artículo 29 (es decir, el cuerpo que representa a todas las autoridades nacionales de protección de datos en la Unión Europea, incluida la autoridad británica de protección de datos [Information Commissioner Office, ICO], que lideró la consulta de este documento):

> **“Para calificar como intervención humana, el responsable del tratamiento debe garantizar que cualquier tipo de control de la decisión sea significativo y no únicamente un gesto simbólico. Debe ser llevado a cabo por alguien que tenga la autoridad y la competencia de cambiar la decisión. Como parte del análisis, deberá considerar todos los datos relevantes.”**[15]

Derecho a Recursos Judiciales Efectivos

La legislación debe incluir el derecho de una persona a acceder a recursos judiciales efectivos contra el responsable o el encargado del tratamiento de datos, en el caso de que considere que sus derechos han sido violados como resultado del tratamiento, en incumplimiento con la ley.

El interesado debe tener el derecho a presentar una reclamación ante la autoridad de control independiente. Esto reafirma la necesidad de que la autoridad de control independiente tenga la facultad de recibir reclamaciones por parte de los interesados, investigarlas y sancionar, dentro del alcance propio de sus atribuciones, a quien haya violado los derechos, o remitir el caso a un tribunal. La legislación también debe contemplar la posibilidad de que el interesado emprenda acciones contra la autoridad de control si esta no ha logrado resolver la reclamación.

Además del derecho a presentar una reclamación ante la autoridad de control, las personas también deben tener acceso a recursos jurídicos efectivos a través de órganos jurisdiccionales como los tribunales de justicia.

Se debe empoderar a las personas a iniciar las acciones por sí mismas, y solicitar a terceros (incluidas las ONG) a adoptar medidas en su representación.

Asimismo, las reparaciones colectivas son un mecanismo importante y efectivo para que quienes no cumplen con la ley de protección de datos se responsabilicen de sus acciones. Suele ocurrir que las personas no cuentan con los recursos para investigar y detectar el incumplimiento, bosquejar reclamaciones y tomar medidas legales adicionales. El costo y la complejidad del proceso pueden dar lugar a que sus mecanismos de reparación sean inaccesibles e inefectivos en la práctica. Por lo tanto, un mecanismo de reparación colectiva debe permitir que las ONG con conocimientos sobre la protección de datos persigan las violaciones a dicha ley por iniciativa propia.[16] La disposición específica que establezca que las ONG pueden emprender acciones resulta particularmente importante en el contexto de marcos legales donde es posible que no existan otros mecanismos de reparación colectiva en el campo de la protección de datos (por ejemplo, medidas cautelares).

Debido a desequilibrios de poder y asimetrías de información entre las personas y quienes controlan sus datos personales, sigue siendo poco probable que los interesados persigan casos según las nuevas leyes en el futuro, a pesar de que existan mejores derechos de ejecución. Permitir las reparaciones colectivas sería una manera efectiva de fortalecer el cumplimiento.

Un ejemplo de acceso a recursos judiciales efectivos en acción

La Federación Alemana de Consumidores llevó a Facebook a la justicia debido a una cantidad de violaciones a la actual legislación alemana de protección de datos. El dictamen del tribunal en febrero de 2018 estimó la mayoría de las reclamaciones de la organización de consumidores, incluyendo términos y condiciones ilegales y disposiciones de consentimiento en las configuraciones predeterminadas de privacidad.[17]

Derecho a Indemnización y Responsabilidad

Una persona cuyos derechos han sido violados debe tener el derecho a una indemnización por el daño sufrido, material o no material (por ej. la angustia sufrida). Esto subraya la necesidad de que se establezcan modelos estrictos de ejecución para garantizar que la autoridad relevante pueda investigar cualquier violación ocurrida e iniciar acciones legales.

Excepciones

Es muy común que exista una disposición que contemple excepciones de cumplimiento de determinados principios, obligaciones y derechos. Con frecuencia, las excepciones se relacionarán con el tratamiento de datos personales realizado por autoridades públicas, en particular las agencias de seguridad e inteligencia.

Es esencial garantizar que, si estipula dichas excepciones, la legislación también proporcione detalles precisos sobre las circunstancias específicas en las que los derechos de los interesados pueden verse restringidos. Estas disposiciones deben ser limitadas, necesarias y proporcionales, además de claras y accesibles para los interesados. Asimismo, no deben ser excepciones generales sino que deben referirse a determinados derechos en situaciones muy específicas y limitadas, y estar establecidas claramente por la ley.

Referencias

1 Krishn Kaushik, La aplicación Narendra Modi solicita acceso general: cámara, audio entre 22 datos ingresados, The Indian Express, 26 de marzo de 2016, dis ponible en http://indianexpress.com/article/india/namo-app-asks-for-sweeping-access-camera-audio-among-22-inputs-facebook-data-leak-5111353/

2 Privacy International, Connected Cars: What Happens To Our Data On Rental Cars?, 6 de diciembre de 2018, disponible en: https://privacyinternational.org/report/987/ connected-cars-what-happens-our-data-rental-cars

3 Privacy International, Uncovering the Hidden Data Ecosystem, disponible en: https://privacyinternational.org/campaigns/uncovering-hidden-data-ecosystem

4 Jeremy B White, 'Cambridge Analytica ordered to turn over man's data or face prosecution', The Independent, 5 de mayo de 2018, disponible en: https://www.independent. co.uk/news/uk/home-news/cambridge-analytica-ordered-ico-personal-data-david- carroll-a8338156.html

5 Judith Duportail, 'I asked Tinder for my data. It sent me 800 pages of my deepest, darkest secrets', The Guardian, 26 de septiembre 2017, disponible en: https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold

6 Hilts, A., Parsons, C., and Crete-Nishihata, M., Approaching Access - A look at consumer personal data requests in Canada, CitizenLab, 12 de febrero 2018, dis ponible en: https://citizenlab.ca/2018/02/approaching-access-look-consumer- personal-data-requests-canada/

7 Orientaciones de la OCDE sobre la protección de la vida privada y los flujos de datos transfronterizos de 1980

8 Tims, El error de Equifax, op. cit.

9 Greenleaf, Leyes de privacidad de datos en Asia (OUP, 2014), p. 493.

10 Privacy International, How Do Data Companies Get our Data?, 25 de mayo de 2018, disponible en: https://privacyinternational.org/feature/2048/how-do-data-companies-get-our-data

11 Ej. focalización en jóvenes inseguros - https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens

12 Datta, A., Tschantz, M. C., y Datta, A. Experimentos automatizados en contextos de privacidad en publicidades, Procedimientos en tecnologías para mejorar la privacidad, 2015(1), 92–112. Disponible en https://doi.org/10.1515/popets-2015-0007

13 Privacy International, Los datos son poder: una guía adicional sobre la elaboración de perfiles y las decisiones automatizadas en el RGPD, 2017. Disponible en https://www.privacyinternational.org/report/1718/data-power-profiling-and-automated-decision-making-gdpr

14 Danielle Citron, La (in)justicia de las puntuaciones de riesgo en las sentencias penales, Forbes, 13 de julio de 2016, disponible en https://www.forbes.com/sites/daniellecitron/2016/07/13/unfairness-of-risk-scores-in-criminal-sentencing/#146a7f514ad2

15 http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053

16 Para obtener información sobre el contexto del Reino Unido o la Unión Europa, consulte Anna Fielder, Por qué la reparación colectiva es necesaria para la protección de datos, Privacy International Medium, 9 de enero de 2018, disponible en https://medium.com/@privacyint/why-we-need-collective-redress-for-data-protection-863c6640689c

17 Comunicado de prensa en inglés disponible en https://www.vzbv.de/sites/default/files/downloads/2018/02/14/18-02-12_vzbv_pm_facebook-urteil_en.pdf

PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

PARTE: 5

Fundamentos Para el Tratamiento de Datos Personales

Fundamentos Para el Tratamiento de Datos Personales

El responsable o el encargado del tratamiento de datos deben identificar el fundamento legal que autoriza dicho tratamiento.

Las bases jurídicas para el tratamiento de datos personales deben ser limitadas y estar claramente expresadas en la legislación (es decir, no deben ser fundamentos vagos o amplios, ni una lista abierta de posibles fundamentos de procesamiento). Sin embargo, suele suceder con demasiada frecuencia que las leyes contemplan muchas bases jurídicas.

Entre las bases que pueden aparecer en la legislación se incluyen las siguientes:

- consentimiento del interesado
- garantía de la necesidad del tratamiento para la ejecución de un contrato con el interesado, o para adoptar medidas para celebrar un contrato
- para el cumplimiento de una obligación legal
- para proteger los intereses vitales de un interesado o alguna otra persona;
- para el desempeño de una tarea llevada a cabo en interés público o en el ejercicio de una autoridad oficial, conferida al responsable del tratamiento
- para los fines de intereses legítimos perseguidos por el responsable del tratamiento o terceros, excepto cuando los intereses, los derechos y las libertades del interesado prevalezcan sobre dichos intereses.

A continuación, describimos algunas de estas bases.

Consentimiento

El consentimiento es un principio fundamental de la protección de datos porque permite que el interesado controle cuándo sus datos personales serán sometidos a un tratamiento: se relaciona con el ejercicio de derechos fundamentales de autonomía y autodeterminación.

El consentimiento debe otorgarse de voluntad libre, ser específico, informado y carecer de ambigüedades. Puede ser una declaración por escrito, incluidos medios electrónicos. Debe ser explícito y requerir un proceso activo de la persona, en

lugar de un proceso pasivo de exclusión: como tal, requiere una acción positiva afirmativa. La entidad que trata los datos debe poder demostrar que ha solicitado y recibido el consentimiento.

El consentimiento no es el único fundamento legal para el tratamiento. De hecho, en muchas situaciones de desequilibrio de poder entre la persona y el encargado del tratamiento (por ej. entre un empleado y un empleador), el consentimiento no puede otorgarse de voluntad libre y, por lo tanto, otro fundamento legal debe justificar el tratamiento de los datos personales (por ej. la celebración de un contrato).

Explícito, de voluntad libre y sin ambigüedades

La definición de consentimiento debe reflejar la elección libre e informada de una persona. Por ejemplo, el RGPD incluye la siguiente definición:

> **“el ‘consentimiento’ del interesado hace referencia a toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.”**

Exenciones para Instituciones Públicas

En algunas jurisdicciones, no se requiere notificación ni consentimiento cuando el tratamiento está a cargo de una institución pública durante el ejercicio de sus funciones legales. Este es el caso de Colombia que, en el artículo 10 (a) de la Ley 1581 de 2012, regula el tratamiento y la gestión de la información personal.

Es fundamental que dicho tratamiento esté sometido a medidas adecuadas y específicas para proteger los derechos y las libertadas de las personas.

Consentimiento implícito

Es posible que algunos textos incluyan el concepto de consentimiento implícito. Este fue el caso en el proyecto de ley propuesto para la enmienda de la legislación de protección de datos en Argentina.

Privacy International no cree que el consentimiento "implícito" cumpla con los estándares de un consentimiento específico, de voluntad libre, informado y sin ambigüedades.

El Grupo de trabajo del artículo 29 (el grupo de autoridades europeas de protección de datos) ha estudiado la temática del consentimiento, y en particular el consentimiento implícito, y concluyó que este último "no era apto según el estándar de consentimiento establecido por el RGPD".[1]

Se debe prestar particular atención a dicha disposición para garantizar que exista una guía y condiciones claras sobre los contextos en los que el consentimiento implícito sería suficiente.

Revocación del consentimiento

Los interesados deben tener el derecho a revocar su consentimiento en cualquier momento. Antes de recoger datos, el responsable del tratamiento debe tener la obligación de informar al interesado (en un momento anterior a obtener el consentimiento) de su derecho a revocar el consentimiento. Esta disposición debe además establecer que cualquier revocación de consentimiento dará lugar a la eliminación de los datos personales. El proceso de revocación debe ser un proceso tan sencillo como su otorgamiento. El responsable del tratamiento debe realizar una acción positiva para confirmar a la persona que su solicitud ha sido procesada, su consentimiento revocado y sus datos eliminados.

El hecho de contar con el consentimiento no debe anular la obligación que tienen los responsables del tratamiento de cumplir con los principios de protección de datos, incluidos el de transparencia, lealtad, limitación de finalidad y minimización de datos. Incluso si se cuenta con el consentimiento, los responsables del tratamiento deben considerar cuidadosamente (por ejemplo, mediante una evaluación de impacto de la protección de los datos) cualquier perjuicio a los derechos de las personas como resultado del tratamiento, y tomar las medidas necesarias para mitigarlos.

Interés Público

Otro fundamento legal que suele reconocerse en la legislación de protección de datos es la necesidad del tratamiento de los datos personales si el responsable lo emprende en interés público.

Una consideración fundamental aquí es que es posible que la legislación de protección de datos no defina qué constituye el "interés público" y, en cambio, delegue esa determinación a quienes traten los datos o a la autoridad a cargo de la protección de los datos. La ausencia de una definición y la falta de claridad en torno a lo que constituye el "interés público", así como su interpretación frecuentemente amplia, generan la inquietud de que este fundamento actúe como un vacío jurídico. El fundamento de interés público debe estar definido claramente para evitar abusos. Por ejemplo, debe ser posible enumerar los fundamentos específicos en interés público (por ej. la administración de justicia) y garantizar que dicha lista sea clara y exhaustiva.

Si existirá una condición que permitirá el tratamiento de datos en situaciones de emergencia, dicha condición debe considerarse y definirse con sumo cuidado y detalle. Todas las bases jurídicas para el tratamiento de datos deben someterse a otras salvaguardas para proteger los derechos y los intereses del interesado, incluyendo la lealtad, la transparencia y una evaluación del impacto de la protección de datos, que claramente tome en cuenta cualquier perjuicio o efecto adverso para las personas.

Por lo tanto, entre las recomendaciones para la autoridad de protección de datos se podrían incluir las siguientes:

- Realizar un mapa de la legislación con disposiciones de "interés público" para clarificar qué se incluiría
- Solicitar que la autoridad de control independiente elabore una guía adicional y realice una prueba del fundamento legal de "interés público"
- Solicitar que las autoridades públicas expliquen claramente qué consideran que constituye el interés público
- Si se aplicará para permitir el tratamiento de datos personales sensibles, la autoridad de control independiente debe definir con antelación el umbral más elevado de "interés público" que debe cumplirse antes de que los datos personales sensibles puedan ser tratados sin consentimiento o algún otro fundamento legal.

Interés legítimo

Con frecuencia, los marcos de protección establecerán que, si el responsable del tratamiento de datos puede demostrar un interés legítimo, entonces dicho interés constituye un fundamento legal para dicho tratamiento. Dado el amplio alcance del término "interés legítimo", es fundamental que se especifique esta condición. Por ejemplo, el responsable del tratamiento debe también demostrar que: el tratamiento es necesario y proporcional para el interés legítimo perseguido y que no invalida los derechos del interesado.

Esta condición puede interpretarse ampliamente y da lugar a abusos. De ser posible, se debe evitar su inclusión en la legislación.

Si se incluye esta disposición y no existen dudas, en el ejercicio de equilibrios, de que existe un perjuicio para la persona, entonces la presunción será que el tratamiento no debe continuarse. Asimismo, es imperativo que los responsables del tratamiento notifiquen claramente a las personas sobre el interés legítimo específico en el que se están basando (es decir, no pueden sencillamente basarse en un interés legítimo genérico o vago), y que realicen una evaluación del perjuicio a las personas caso por caso, incluido un mecanismo de inclusión.

No todas las bases jurídicas están disponibles para todos los responsables del tratamiento. Por ejemplo, la capacidad de recurrir a una justificación de interés legítimo ha sido restringida para las autoridades públicas en el RGPD. Esto significa que las autoridades públicas no pueden basarse en esta justificación cuando el tratamiento se realiza durante el desempeño de sus funciones. Por el contrario, las autoridades deberán identificar el interés público y la función estatutaria o la tarea pública relevante.

Tratamiento de Datos Personales Sensibles

En el caso del tratamiento de datos personales sensibles, se deben cumplir condiciones adicionales. Las situaciones en las que el tratamiento de datos personales sensibles está permitido deben ser limitadas. Si se recurre al consentimiento para justificar el tratamiento de datos personales sensibles, es extremadamente importante que sea explícito y que cumpla con todos los requisitos antes mencionados (es decir, que sea informado, de voluntad libre y específico).

Para fortalecer el principio de limitación de finalidad (estipulado en otra sección de la legislación), la disposición sobre los datos personales sensibles debe reafirmar que dichos datos no pueden recibir un tratamiento adicional para otros fines, o por parte de terceros que no estén identificados en la legislación.

También es importante que se proporcione la protección más elevada a los datos que revelan datos personales sensibles mediante la elaboración de perfiles y el

uso de información proxy (los encargados del tratamiento de los datos pueden inferir, derivar y predecir datos personales sensibles sin que estos hayan sido proporcionados explícitamente).

Las condiciones para el tratamiento de datos personales sensibles deben ser limitadas, y se debe prestar especial atención en el caso de que se propongan condiciones como la de "datos personales que el interesado ha hecho manifiestamente públicos" (artículo 9 del RGPD). Este enfoque da lugar a preguntas como: ¿qué significa "hacer públicos"? ¿Cómo puede verificarse que una persona los ha hecho públicos? Además, es importante destacar que si una persona ha hecho públicos los datos, ¿significa eso que los datos pueden ser utilizados por cualquier otra persona para cualquier finalidad?

Esto resulta particularmente relevante a la luz de los desarrollos recientes: el avance del movimiento de datos abiertos y las leyes de transparencia pública significan que existe una cantidad creciente de bases de datos y otros registros (es decir, registros de propiedad, registros fiscales o bases de datos electorales) que conservan datos personales. El hecho de que dichos datos hayan sido hecho públicos (por motivos de interés público, transparencia y responsabilidad) no significa que los datos conservados puedan ser utilizados para fines distintos de los que se definieron al momento de su recogida.

Asimismo, ha sido una inquietud permanente de Privacy International el uso de la Social Media Intelligence (SOCMINT) como técnica aplicada por parte de las fuerzas, los cuerpos de seguridad y otras agencias, que se está replicando en todo el mundo. Se sostiene que, sin estar sujeto a ninguna reglamentación, autorización judicial o control independiente, el uso de estos datos es legal porque no interfiere con el derecho a la privacidad, y que depende únicamente de los así llamados datos "disponibles públicamente". Nosotros rechazamos este argumento. El tratamiento de datos "públicamente disponibles" en las plataformas de redes sociales tiene consecuencias claras y graves para la privacidad de las personas. El hecho de que los datos estén públicamente disponibles no justifica su recogida, conservación, análisis o cualquier otra forma de tratamiento sin regulación ni control.[2]

El tratamiento de datos personales para fines científicos, históricos o estadísticos

En algunas ocasiones, se suele aclarar en los marcos de protección de datos que el tratamiento de datos personales con fines científicos, históricos o estadísticos podría ser un fundamento legal legítimo.

Para evitar abusos e interpretaciones amplias de este fundamento legal:

- Es necesario aclarar qué constituye la finalidad estadística y científica. Se deben incluir más detalles en la legislación, o se deben elaborar orientaciones para definir mejor este concepto.
- Dicho fundamento legal no debe eximir al responsable o el encargado del tratamiento de todas sus obligaciones, y se deberán proporcionar salvaguardas adecuadas para el tratamiento de datos personales para estos fines.
- Una de las salvaguardas podría garantizar que los datos no se usarán para tomar decisiones sobre las personas, y que el tratamiento se prohibirá si fuera motivo de perjuicios.
- El interesado debe seguir teniendo los derechos sobre sus datos, incluido el derecho a ser informado y el derecho a objetar que sus datos se traten para estos fines.

El tratamiento de datos personales y la libertad de expresión y de acceder a la información

El Estado debe tomar las medidas necesarias para reconciliar el derecho a la protección de datos personales con el derecho a la libertad de expresión y de acceder a la información. Esto puede incluir el tratamiento para fines periodísticos y de derechos humanos, y fines académicos, artísticos o de expresión literaria. Al momento de encontrar un equilibrio de estos dos derechos, es posible que existan exenciones y derogaciones de las obligaciones y los derechos de los interesados.

Para fines periodísticos, podría aplicarse una exención en la medida en que sea necesario para 1) proteger el derecho a ejercer el derecho fundamental a la libertad de expresión y opinión para fines periodísticos y 2) para proteger las fuentes. Asimismo, recomendamos que una disposición de este estilo incluya otros ejercicios legítimos del derecho a la libertad de expresión, como es el caso de las investigaciones llevadas a cabo por organizaciones independientes no gubernamentales. [3]

Referencias

1 Grupo de trabajo del artículo 29, Directrices sobre el consentimiento en virtud de la reglamentación 2016/769, adoptada el 28 de noviembre de 2017, según su última revisión y entrada en vigor el 10 de abril de 2018, pp. 30. Disponible en http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

2 Para obtener más información, consulte el documento explicativo de Privacy International, disponible en https://privacyinternational.org/explainer/55/social-media-intelligence

PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

PARTE: 6

Obligaciones de Los Responsables y Los Encargados del Tratamiento de Datos

Obligaciones de Los Responsables del Tratamiento y Procesamiento de Datos Personales

Rendición de cuentas y cumplimiento

Los responsables del tratamiento y procesamiento de datos personales deben demostrar el cumplimiento de sus respectivas obligaciones en materia de protección de datos.

P: ¿Requiere la ley de manera explícita que los responsables del tratamiento y procesamiento de datos personales demuestren su cumplimiento? ☐

Registro del tratamiento de datos

Los responsables del tratamiento y procesamiento de datos personales deberían estar obligados a mantener registros de sus actividades de tratamiento de datos.

P: La ley de protección de datos:

- ¿Contempla esta obligación? ☐
- ¿Especifica qué información debe ser registrada? ☐

Informaciones tales como:

- el nombre y datos de contacto de los responsables del tratamiento y procesamiento de datos personales ☐
- los fines del tratamiento de datos ☐
- el fundamento legal del tratamiento de datos ☐
- una descripción de las categorías de titulares de datos y de las categorías de datos personales ☐
- las terceras partes a quienes se transfieran o vayan a transferir datos personales ☐
- las categorías de terceras partes a quienes se transfieran o vayan a transferir datos personales, incluyendo los resguardos que se hayan adoptado ☐
- tlos plazos de tiempo previstos para el borrado de diferentes categorías de datos ☐
- una descripción de las medidas de seguridad técnicas y organizacionales que se hayan adoptado para asegurar la integridad y confidencialidad de los datos ☐

Resguardando la seguridad, integridad y confidencialidad

Los responsables del tratamiento y procesamiento de datos personales deben tener el deber y la responsabilidad de resguardar su infraestructura y seguridad de los datos.

P: La ley de protección de datos:

- ¿Contempla esta obligación? ☐
- ¿Define con claridad los tipos de medidas organizacionales y de seguridad que los responsables del tratamiento y procesamiento de los datos personales deben adoptar para proteger la seguridad e integridad de los datos?a? ☐

Las obligaciones sugeridas pueden incluir, entre otras:

- pseudonimización de datos personales
- cifrado de datos personales
- garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de procesamiento de datos
- la habilidad de restablecer la disponibilidad y el acceso a los datos personales de manera oportuna en caso de un incidente de seguridad
- implementar procesos de evaluación, monitoreo y auditoria periódica de los resguardos adoptados

Privacidad desde el diseño y por defecto

La protección de datos personales debe ser incorporada en sistemas, proyectos y servicios desde el principio, para asegurar que pordiseño y por omisión se implementen los principios de protección de datos personales y se resguarden los derechos de los titulares de los datos.

P: Al momento de tomar decisiones y durante el tratamiento de datos, ¿Contempla la ley alguno de estos elementos?

- 'Privacidad desde el diseño', que requiere ser implementada mediante medidas técnicas y organizacionales adecuadas ☐
- 'Privacidad por defecto', que requiere la implementación de medidas técnicas y organizacionales adecuadas para asegurar que, por omisión, sólo los datos personales que resulten necesarios para una finalidad específica sean objeto de tratamiento ☐

Evaluaciones de impacto

Los responsables del tratamiento y procesamiento de datos personales deben realizar una evaluación de impacto con anterioridad al tratamiento de datos personales.

P: La ley de protección de datos:

- ¿Contiene esta obligación? ☐
- ¿Detalla qué es lo que tiene que ser evaluado con anterioridad al tratamiento de datos? ☐

Una evaluación de impacto requiere al menos una evaluación de los siguientes puntos:
- la necesidad y proporcionalidad del tratamiento
- los riesgos para los titulares de protección de datos personales y,
- cómo estos riesgos deben ser abordados.

Oficiales de protección de datos personales

Los responsables del tratamiento y procesamiento de datos personales deben designar responsables a cargo de asegurar el cumplimiento de los requerimientos de la ley de protección de datos, incluyendo la supervisión y regulación de la implementación de la ley.

La ley de protección de datos:

- ¿Requiere la designación de un oficial de protección de datos (OPD)? ☐
- ¿Requiere que el OPD tenga el poder, autonomía y recursos suficientes para cumplir con su mandato? ☐

Notificación de violaciones de datos personalesLos responsables del tratamiento y procesamiento de datos personales deben estar obligados a notificar los casos de violación de datos personales a la autoridad supervisora y a los titulares de datos personales dentro de un período razonable de tiempo, definido en la ley.

P: La ley de protección de datos:

- obliga a los responsables del tratamiento y procesamiento de datos personales a notificar a:
  - ¿La autoridad supervisora? ☐
  - ¿Al titular de los datos? ☐
- ¿Detalla la información que debe acompañar a la notificación de violación de datos? ☐

La notificación debe incluir a lo menos:
- la naturaleza de la violación
- quiénes resultaron afectados
- las consecuencias que puede tener la violación de datos
- las medidas adoptadas para enfrentar la violación y las mitigaciones efectuadas para prevenir efectos adversos.

Obligaciones de Los Responsables y Los Encargados del Tratamiento de Datos

Los mecanismos de responsabilidad y ejecución son fundamentales para consolidar con éxito la protección de los datos personales. La legislación debe identificar claramente a las partes responsables del cumplimiento de la ley, además de sus deberes y obligaciones para garantizar el cumplimiento y la protección de los derechos de las personas, y qué medidas deben adoptar en caso contrario.

La ley debe definir claramente quiénes son responsables y encargados del tratamiento de datos, junto con las responsabilidades y obligaciones que correspondan a ambos. La ley también debe cubrir la relación entre responsables y encargados del tratamiento, y especificar qué se espera de cada uno de ellos. Responsables y encargados del tratamiento también deben estar sujetos a obligaciones de registro, seguridad y notificación de fugas de datos.

El principio de responsabilidad representa un importante avance en la legislación debido a que exige a los responsables del tratamiento demostrar su cumplimiento de las obligaciones de protección, incluidos los requisitos de mantener un registro de todo el tratamiento llevado a cabo bajo su autoridad, y de mantener dicho registro actualizado.

Cumplimiento de la Legislación Aplicable

Los responsables y los encargados del tratamiento tienen el deber de garantizar la adopción de todas las medidas necesarias para cumplir con la legislación aplicable. No basta que cumplan con la ley: deben explicar claramente cómo lo hacen, demostrando de esa forma que el procesamiento está siendo efectuado de acuerdo con la ley.

Tanto los responsables como los encargados del tratamiento deben implementar las medidas técnicas y organizativas apropiadas para garantizar y poder demostrar que el tratamiento se lleva a cabo en conformidad con la ley.

Entre dichas medidas se pueden incluir las siguientes::

- realizar una auditoría o mapa actualizado de los datos
- adoptar e implementar políticas y procedimientos integrales de protección de datos
- adoptar un enfoque desde el diseño y por defecto
- designar a un delegado de protección de datos para controlar este proceso

- definir claramente las maneras en las que las personas pueden ejercer sus derechos
- celebrar contratos con quienes tratan los datos en su representación, o en conjunto, para garantizar que las obligaciones sean claras
- llevar a cabo evaluaciones de impacto de la protección de la privacidad y los datos
- mantener registros de las actividades de tratamiento de datos
- capacitar al personal
- implementar medidas estrictas de seguridad
- implementar un procedimiento para dar una respuesta ante los casos de violaciones de datos, y para registrarlas e informarlas
- implementar procedimientos de evaluación para revisar y actualizar estas medidas.

Registro de Actividades de Tratamiento de Datos

Los responsables y los encargados del tratamiento deben tener la obligación de conservar registros de sus actividades de tratamiento y archivar (por escrito) la información que deben proporcionar a los interesados.

Esta información puede incluir:

- el nombre y los detalles de contacto del/de los responsable/s y encargado/s del tratamiento
- la finalidad del tratamiento
- una descripción de las categorías de interesados y de las categorías de datos personales
- las terceras partes con quienes se compartieron o se compartirán los datos personales
- los terceros a quienes se transfirieron o se transferirán los datos personales, incluidos los detalles de las salvaguardas adoptadas
- los límites de tiempo previstos para la eliminación de las diferentes categorías de datos
- una descripción de las medidas de seguridad técnicas y organizativas adoptadas para garantizar la integridad y confidencialidad de los datos.

Integridad y Confidencialidad

Tanto el responsable como el encargado del tratamiento deben tener la obligación y la responsabilidad de salvaguardar la seguridad de los datos y la infraestructura. Asimismo, sus obligaciones deben exigirles informar e investigar las violaciones de datos, además de brindar información a la autoridad de control relevante y a los interesados afectados.

La legislación debe estipular no solo salvaguardas de seguridad para proteger los datos sino también la obligación de proteger también los dispositivos y la infraestructura utilizados en cada etapa del tratamiento, incluidas la generación, la recogida, la retención y el intercambio de datos (es decir, tanto los datos almacenados como los datos en tránsito).

La legislación debe incluir obligaciones específicas para los responsables y los encargados del tratamiento en relación con la seguridad, incluyendo, entre otras, las siguientes:

- la seudonimización de datos personales
- la encriptación de datos personales;
- la garantía de confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y los servicios de tratamiento
- la capacidad de restablecer la disponibilidad y el acceso a los datos personales de manera oportuna en el caso de incidentes físicos o técnicos
- un proceso de seguimiento y evaluación periódico, al igual que la auditoría de la efectividad de las medidas organizativas y técnicas para garantizar la seguridad del tratamiento, incluida la privacidad desde el diseño y la efectividad de las evaluaciones de impacto de la protección de datos (DPIA, por sus siglas en inglés).

Es posible también someter a las organizaciones de tratamiento de datos a otros marcos legales, incluidos los relacionados con la ciberseguridad, que exigen la protección de los datos.

Seudonimización: no es una fórmula milagrosa para cumplir con la protección de datos

La seudonimización se presentó como una técnica para mejorar la privacidad porque reduce el riesgo y respalda los esfuerzos de los responsables del tratamiento para cumplir con sus obligaciones. Implica reemplazar cualquier característica identificatoria de los datos con un pseudónimo o, en otras palabras, un valor que no permita la identificación directa del interesado sin tener acceso a información adicional. El objetivo es reducir la vinculabilidad de un conjunto de datos con la identidad original de una persona.

Ejemplos de disposiciones de seudonimización:

Como se propone en el proyecto de reforma a la Ley 25.326 que regula la protección de datos en Argentina:

> **“Todo tratamiento de datos personales de modo que cualquier información obtenida no pueda ser asociada con una persona identificada o identificable.”**

Según el RGPD:

> **“El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.”**

Es importante que la seudonimización se considere apenas una entre otras medidas que pueden adoptar el responsable y el encargado del tratamiento de datos: es posible que como única medida no sea suficiente, dado que el mismo concepto depende de la capacidad de reidentificación y, por lo tanto, es posible que se requieran medidas adicionales para garantizar el cumplimiento de las obligaciones de protección de datos, dependiendo de las circunstancias.

Los datos seudonimizados siguen siendo datos personales y no deben usarse para evadir los derechos de las personas, negándoles por ejemplo el acceso a sus datos porque carecen de un identificador (cuando una organización ha asignado a una persona un identificador único que la persona desconoce y, por lo tanto, se le deniega el acceso a los datos asociados con éste). Asimismo, los estudios han demostrado que la seudonimización y la supresión de toda señal de identificación estándar por sí mismas no son medidas suficientes para evitar que los usuarios puedan ser reidentificados, y que todavía existen riesgos de reidentificación.

Como lo destaca el Data Science Institute del Imperial College en Londres:

> **Esta combinación de seudonimización y supresión de toda señal de identificación funcionó bastante bien durante 15 o 20 años. Sin embargo, los conjuntos de datos modernos, y especialmente los conjuntos de datos utilizados por la inteligencia artificial, son muy diferentes a los usados a mediados de la década del año 1990. Los conjuntos de datos de hoy en día, provenientes de teléfonos, navegadores, la Internet de las cosas o ciudades inteligentes, son de una dimensión elevada: contienen cientos o miles de datos de cada persona y de su manera de comportarse.**
>
> **Esto cambia fundamentalmente la capacidad de los métodos de anonimato para proteger efectivamente la privacidad de las personas mientras se permite el uso de los datos.[1] Un estudio basado en metadatos de teléfonos móviles demostró que con solamente cuatro puntos (horas y sitios aproximados) es posible identificar inequívocamente al 95% de personas en un conjunto de datos de 1,5 millones de personas. Esto significa que si se sabe dónde y cuándo estuvo una persona apenas cuatro veces en el transcurso de 15 meses, en promedio, es posible reidentificarla en un conjunto de datos de teléfonos móviles anonimizado sencillamente, revelando todo su historial de localizaciones.[2]**

Privacidad Desde el Diseño y por Defecto

Además de la ejecución mediante las reglamentaciones y los órganos jurisdiccionales, las decisiones técnicas tomadas en la etapa de diseño de los sistemas pueden tener un papel importante en la puesta en práctica de las normas de protección de datos. A través de medios tecnológicos, y considerando la privacidad en el diseño de los sistemas, es posible limitar la recogida de datos, restringir el tratamiento adicional y evitar accesos innecesarios, entre otras medidas de privacidad. La legislación puede influir, y de ser necesario obligar a cumplir, dichos desarrollos mediante un requisito de protección de datos/la privacidad desde el diseño y por defecto.

Privacidad desde el diseño

La privacidad desde el diseño implica que la protección de datos debe integrarse desde el momento en que se empieza a diseñar un sistema, de modo que las salvaguardas antes mencionadas se contemplen también desde el principio. La obligación de cumplir recae tanto en el responsable como en el encargado del tratamiento.

Este enfoque reduce la dependencia de las salvaguardas políticas. En cambio, regula el tratamiento de datos personales mediante la tecnología propiamente dicha. Es necesario destacar que la adopción ha sido lenta, dado que las empresas y los Gobiernos se resisten a restringir capacidades y aspiraciones futuras de explotación de datos personales, incluso si legalmente deberían limitar la desviación de uso.

En algunas jurisdicciones, la "privacidad desde el diseño" se ha convertido en un requisito legal. En la 32.a Conferencia Internacional de Comisarios de Protección de Datos y Privacidad de 2010, se aprobó por unanimidad una resolución que reconocía la privacidad desde el diseño como componente esencial de la protección fundamental de la privacidad.[3]

Privacidad por defecto

Un segundo componente es la "privacidad por defecto", que requiere que un producto, servicio o sistema aplique una estricta protección de la privacidad y de los datos de manera predeterminada. Esto incluye configuraciones que protegen la privacidad por defecto, es decir, sin que el usuario final deba realizar manualmente ningún tipo de configuración.

Esta medida es esencial, dada la engorrosa y compleja naturaleza técnica de muchas políticas de protección de la privacidad y los datos. La carga no debe recaer en las personas: no debe esperarse que tengan los conocimientos y la experiencia necesarios para comprender la complejidad de los servicios y dispositivos que usan. Siempre que sea posible, deberán gozar del más elevado nivel de protección de forma predeterminada.

Evaluaciones de Impacto

Otro requisito que ha sido integrado en los marcos nacionales de protección de datos es que las evaluaciones de impacto se lleven a cabo antes del tratamiento de los datos personales. Esto resulta particularmente importante en los casos en que existe un riesgo para los derechos y las libertades de las personas, incluso cuando el tratamiento implica datos personales sensibles, decisiones automatizadas, elaboración de perfiles o seguimiento de espacios públicos.

Una evaluación de impactos requiere, como mínimo:

- la evaluación de la necesidad y proporcionalidad del tratamiento
- los riesgos para las personas
- la manera en que se abordarán dichos riesgos.

Delegados de Protección de Datos

El control es un elemento clave de cualquier tipo de mecanismo de responsabilidad. Es importante que los responsables y los encargados del tratamiento designen responsabilidades claramente para garantizar el cumplimiento de los requisitos de protección de datos. Esto puede incluir la designación de delegados de protección de datos que se responsabilicen de controlar y regular la implementación de la ley.

Los responsables y los encargados del tratamiento deben garantizar que el delegado goce de las facultades, la autonomía y los recursos adecuados para llevar a cabo su función.

Notificación de Violaciones

En el caso de que ocurran violaciones de datos, los responsables del tratamiento deben tener la obligación de notificarlas a la autoridad de control y al interesado.

Esta obligación debe estar estipulada con precisión en la ley y establecer:

- Claramente el periodo de tiempo, que debe requerir que la notificación se lleve a cabo lo antes posible después de que el responsable o el encargado del tratamiento haya detectado la

violación
- Un requisito de notificación siempre que exista algún riesgo para los derechos de las personas involucradas
- Qué información debe acompañar la notificación de violación, por ejemplo la naturaleza de la violación, quiénes se ven afectados, las posibles consecuencias y las medidas tomadas para abordar la violación y mitigar los efectos adversos.

Definiciones de "violaciones de datos":

RGPD: "'violación de datos personales' significa toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos (Artículo 4 [12])".

Convenio 108: "Cada parte garantizará que el responsable del tratamiento notifique sin demora, al menos a la autoridad de control competente, según lo dispuesto por el artículo 15 del presente convenio, sobre cualquier violación de los datos que pudiera interferir gravemente con los derechos y las libertades fundamentales del interesado".

El RGPD dispone que es obligatorio notificar a la autoridad de control si una violación de datos puede "dar lugar a riesgos para los derechos y las libertadas de las personas" (artículo 33). De igual modo, es obligatorio informar al interesado si la violación de datos personales puede provocar un elevado riesgo a los derechos y las libertades de personas físicas (artículo 34).

La notificación a la autoridad de control debe realizarse dentro de las 72 horas posteriores al momento en que se tomó conocimiento de la violación por primera vez. La notificación al interesado debe realizarse sin dilaciones indebidas. Los responsables del tratamiento también deberán notificar a sus clientes, los encargados del tratamiento, sin dilaciones indebidas, una vez que hayan tomado conocimiento por primera vez de la violación de datos. (Artículo 33, sección 2).

Ejemplo de Protocolos Para Responder Ante Casos de Violaciones de Datos

En Colombia, cuando existen violaciones de la seguridad y surgen riesgos para la gestión de los datos personales, se debe informar a la autoridad de protección de datos (el informe debe ser realizado tanto por el responsable como por el encargado del tratamiento)[4]. Existe una Guía de responsabilidad,[5] que estipula

que la notificación debe incluir el tipo de incidente, la fecha en que ocurrió, la causa, el tipo de datos personales comprometidos y la cantidad de personas cuyos datos se ven afectados. La guía también estipula que se debe informar a quienes se vean afectados y proporcionarles las herramientas necesarias para minimizar los daños causados por la violación.

Transferencias Internacionales de Datos

El enfoque general es que cualquier transferencia de datos personales a otro país (y cualquier transferencia posterior) no debe disminuir el nivel de protección de los derechos que tienen las personas sobre sus datos personales.

Existen varios modelos adoptados para reglamentar y gestionar la transferencia de datos entre fronteras.

Algunas jurisdicciones, como México, recurren a una notificación de privacidad que debe ser acordada entre el responsable del tratamiento y el interesado, y que estipulará si la persona está o no de acuerdo con la transferencia de sus datos. En este caso, el destinatario de los datos deberá cumplir con las mismas obligaciones que tienen los responsables originales del tratamiento. En nuestra opinión, este modelo no es satisfactorio.

Uno de los mecanismos comunes para la regulación y el control de transferencias internacionales de datos es la evaluación de la adecuación del posible destinatario de los datos. Este es el modelo adoptado en Europa y Argentina, por ejemplo.

Según este modelo, está permitido cualquier tipo de intercambio o transferencia de datos personales a entidades de otros países, siempre que el destinatario ofrezca un nivel de protección de datos personales que sea, como mínimo, equivalente al nivel establecido en la ley nacional del emisor. La evaluación puede ser llevada a cabo por una autoridad de control o una autoridad de protección de datos independiente, seguida de una consulta pública y una cuidadosa investigación.

La evaluación del nivel de protección de datos personales realizada en el tercer país debe incluir explícitamente:

- Respeto por los derechos humanos y las libertades fundamentales, legislación relevante, incluida la relativa a seguridad pública, defensa, seguridad nacional y legislación penal, y el acceso de las autoridades públicas a los datos personales
- Reconocimiento de los derechos de los ciudadanos y extranjeros dentro del territorio, sin discriminación por su condición de inmigrante
- Estado de derecho, incluida la legislación nacional vigente y la normativa regulatoria/profesional
- Existencia y funcionamiento efectivo de autoridades de control independientes para garantizar el cumplimiento de la ley y
- Los compromisos internacionales que haya celebrado el tercer país o la organización internacional involucrada, así como cualquier otro tipo de obligaciones que surjan de convenios o instrumentos legalmente vinculantes y de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de datos personales.

Los mecanismos de toma de decisiones deben ser transparentes, claros y prescriptivos, además de requerir consultas con los actores relevantes, incluida la sociedad civil. Asimismo, esta evaluación debe revisarse con frecuencia para establecer un mecanismo de revisión periódico del proceso de toma de decisiones.

Si no es posible emprender una evaluación de adecuación, el responsable o el encargado del tratamiento deben tomar medidas para compensar la ausencia de protección de los datos, garantizando que existan y se ejecuten las salvaguardas apropiadas para proteger al interesado. Las salvaguardas apropiadas pueden adoptar diversas formas: entre los ejemplos de la Unión Europea se incluyen el desarrollo de normas corporativas vinculantes para las transferencias entre empresas y cláusulas de protección de datos estándar dentro de las cláusulas contractuales, según sea permitido por una autoridad de control.

Ejemplos de Mecanismos de Adecuación

Según el artículo 45 del Reglamento (UE) 2016/679 (RGPD), la Comisión Europea estipula un mecanismo mediante el cual es posible determinar si un país fuera de la Unión Europea ofrece un nivel adecuado de protección de datos y, de ser aceptado, si se permite la transferencia de los datos desde la Unión Europea a dicho tercer país sin necesidad de ninguna salvaguarda adicional.

La adopción de una decisión de adecuación implica 1) una propuesta por parte de la Comisión Europea, 2) una opinión del Comité Europeo de Protección de Datos, 3) una aprobación por parte de los representantes de los países de la Unión Europea y finalmente 4) la adopción de la decisión por parte de los Comisarios europeos.[6]

Si bien la sección 12 de la Ley de Protección de Datos de Argentina n.o 25 326 del año 2000 ('la ley'), prohíbe la transferencia a países que no proporcionan niveles adecuados de protección, la adopción de un reglamento en 2016 introduce dos contratos modelo para las transferencias internacionales de datos a este tipo de países. El primer modelo aplica a las transferencias de un responsable del tratamiento a otro, mientras que el segundo debe utilizarse para transferencias a encargados del tratamiento que proporcionan los servicios.[7]

En Sudáfrica, la legislación estipula un conjunto de condiciones que una "parte responsable" (la parte emisora) debe cumplir para transferir datos personales de un interesado a un tercero en un país extranjero. Entre estas condiciones se incluyen que (i) el interesado debe expresar su consentimiento para dicha transferencia; (ii) la transferencia sea necesaria para la celebración de un contrato y (iii) la transferencia sea para el beneficio del interesado, y que no sea viable para la parte responsable obtener el consentimiento del interesado para la transferencia.

Exenciones

Existen varios motivos para que se realicen transferencias de datos que pueden considerarse exentos de cumplir con la protección de datos:

- Cuando la transferencia es necesaria para una cooperación legal internacional entre entidades de investigación e inteligencia públicas, en conformidad con instrumentos de legislación internacional y con respeto a los principios de legalidad, necesidad y proporcionalidad
- Cuando la transferencia es necesaria para la protección de la vida o la seguridad física del interesado o un tercero
- Cuando el cuerpo competente autoriza la transferencia según los términos del reglamento
- Cuando la transferencia es el resultado de un compromiso asumido en un acuerdo internacional de cooperación
- Cuando la transferencia es necesaria para la ejecución de políticas públicas, o es parte del mandato legal de una autoridad pública

Independientemente de las exenciones implementadas, estas deben ser reguladas estrictamente y requerirán una guía adicional para garantizar que no se interpreten de manera amplia ni sean vulnerables a abusos, además de que cumplan con los estándares de derechos humanos. Estas excepciones deben enmarcarse e interpretarse inequívocamente para garantizar que dichos acuerdos no provoquen el debilitamiento de la protección de datos ofrecida por la ley.

Referencias

1 Yves-Alexandre de Montjoye et al, La resolución del problema de privacidad de la inteligencia artificial, Data Science Institute del Imperial College, Londres, febrero de 2018, PDF disponible en https://www.imperial.ac.uk/media/imperial-college/data-science-institute/WhitePaper_SolvingALPrivacyIssues.pdf

2 Yves-Alexandrew de Montjoye et al, Único en la multitud: los límites de la privacidad de la movilidad de las personas, 3, 1376., Informes científicos volu men 3, número de artículo: 1376 (2013), disponible en https://rdcu.be/WBtA

3 Resolución de privacidad desde el diseño, 32.a Conferencia Internacional de Co misarios de Protección de Datos y Privacidad, Jerusalén, Israel, 27-29 de octu bre, 2010, disponible en https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

4 Artículos 17(n) y 18 (k) de la Ley 1581/2012 disponibles en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

5 Industria y Comercio, Guía para la implementación del principio de responsabi lidad demostrada (Accountability), p20, PDF en español disponible en https://iapp.org/media/pdf/resource_center/Colombian_Accountability_Guidelines.pdf

6 Comisión Europea, Adecuación de la protección de datos personales en países que no son miembro de la Unión Europea, disponible en https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

7 8 de noviembre de 2016, Reglamentación 60 – E/2016 sobre transferencias internacionales de datos personales.

PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

PARTE: 7

Autoridad Control Independiente

Autoridad Control Independiente

Si bien los acuerdos internacionales de protección de datos siguen siendo en gran parte no prescriptivos en cuanto a la ejecución, para dar efecto al derecho fundamental de protección de datos y sus principios y garantizar el cumplimiento de las obligaciones, la legislación debe estipular el establecimiento de una autoridad de control independiente. La autoridad de control requiere esta base legislativa para establecer claramente su mandato, facultades e independencia.

Modelos y Estructuras

Se han considerado dos modelos de ejecución: la creación de una autoridad de control independiente y un modelo de ministerio.

De los siete acuerdos y estándares internacionales relevantes para la privacidad de los datos, cinco requieren el establecimiento de una autoridad de control independiente. Si bien los principios de la OCDE no requerían una autoridad de control independiente, el modelo de la Unión Europea, tanto el RGPD (antes conocido como Directiva 95-46) y el Convenio 108 del Consejo de Europa, sí lo requerían (el 90 % de los países con legislación de protección de datos han optado por este modelo).[1] Contar con una autoridad de control independiente también resulta directamente relevante para la evaluación de adecuación, ya que es esencial para ejercer el control y la ejecución.

Sin embargo, es importante destacar que en muchas jurisdicciones, como México y el Reino Unido, se ha establecido una sola institución para actuar tanto de regulador como de agente de ejecución de leyes relativas al acceso a la información y la protección de datos. Esta combinación de funciones no debe contradecir el mandato, las funciones y las facultades de la autoridad de ejecución, o la independencia del Ejecutivo.

Asimismo, algunos países han optado por tener múltiples autoridades de control independientes. En Alemania, la reglamentación de la protección de datos en relación con entidades públicas y privadas aplica a nivel estatal, y luego existe un Comisario Federal de Protección de Datos que hace un seguimiento de las autoridades federales y otras entidades públicas bajo el control del gobierno federal.

Estructura, Mandato y Facultades

El mero establecimiento de esta autoridad independiente no es suficiente. La ley debe garantizar:

Estructura

- Proceso para el establecimiento y la designación: la ley debe contemplar un proceso y un cronograma de tiempo para el establecimiento de la autoridad y la designación de su director y sus miembros.[2]
- Composición y estructura: la legislación debe establecer la composición de esta autoridad, incluidas las habilidades y la experiencia requeridas.
- Recursos: la legislación debe estipular que la autoridad recibirá los recursos suficientes, ya sean financieros, técnicos o humanos.
- Estatus independiente: la legislación debe estipular que la autoridad independiente de protección de datos mantenga su autonomía, para cumplir efectiva y adecuadamente su misión de ejecutar el marco de protección de datos. La autoridad no debe recibir influencias externas y se debe abstener de llevar a cabo acciones incompatibles con sus obligaciones.
- Seguimiento y ejecución: se debe dar a la autoridad la tarea de hacer un seguimiento de la aplicación de la ley, así como de ejecutarla. Esto también requeriría revisiones periódicas de las actividades de quienes son sujetos de derecho.

Mandato

- Mandato de investigar: la autoridad debe recibir el mandato de llevar a cabo investigaciones y accionar ante reclamaciones, emitiendo pedidos vinculantes e imponiendo penalidades cuando toma conocimiento de que una institución o algún otro organismo ha quebrantado la ley. Este mandato incluye ser capaz de: exigir información al responsable o el encargado del tratamiento, realizar auditorías, obtener acceso a toda la información que se requiera para la finalidad de la investigación, incluido el acceso físico a las instalaciones o el equipo utilizado para el tratamiento, si fuera necesario.
- Mandato de recibir reclamaciones y ofrecer una respuesta: tanto las personas como las asociaciones de protección de

la privacidad o interés público deben gozar del derecho de presentar reclamaciones ante esta autoridad independiente. La autoridad independiente también debe poder recibir reclamaciones de organizaciones competentes, basadas en evidencias que demuestren prácticas inadecuadas antes de que haya ocurrido un quebrantamiento de la ley.

- Mandato de ofrecer asesoramiento: la autoridad debe asesorar a los cuerpos gubernamentales relevantes (dependiendo del sistema político), al igual que a otros cuerpos públicos en materia de medidas legislativas y administrativas para la protección de los derechos y las libertades de las personas físicas, en relación con el tratamiento de sus datos personales.
- Provisión de información: el trabajo de la autoridad debe incluir la provisión de información a los interesados en relación con el ejercicio de sus derechos según la legislación de su país o de algún otro lugar; en este último caso, es posible que se requiera establecer contacto con las autoridades de control extranjeras.
- Mandato de promover la conciencia pública: parte del rol de la autoridad es promover la conciencia pública y el entendimiento de los derechos, los riesgos, las normas y las salvaguardas de los interesados. Esto incluye la toma de conciencia de los recursos disponibles para exigir y gozar de dichos derechos, y de los riesgos asociados con la protección de datos personales.

Facultades

- Facultad de imponer sanciones: la autoridad independiente debe tener la facultad de imponer penalidades apropiadas, incluidas multas, notificaciones de ejecución, obligaciones y enjuiciamiento. Este proceso de sanción no debe depender de que la persona presente una reclamación, sino que puede ser impuesto de manera proactiva por la autoridad independiente de protección de datos.
- Emisión de recomendaciones y directrices: en virtud de su facultad de investigar e imponer sanciones, la autoridad independiente también debe ser capaz de emitir recomendaciones y directrices, explicando su interpretación de algunas disposiciones o aspectos de la legislación de protección de datos, ya sea de manera general o dirigida a un sector específico. Dado el ritmo vertiginoso de los avances tecnológicos, esta es también una manera de evitar que la legislación de protección de datos se desactualice y se vuelva obsoleta.

- Facultades regulatorias especiales: asimismo, en algunos casos, la legislación de protección de datos puede otorgar a la autoridad facultades para regular determinados aspectos de la ley, por ejemplo para actualizar definiciones o requisitos de seguridad y aprobar el flujo transfronterizo de datos.

Sanciones frente a violaciones de la ley

Los tipos de sanciones o penalidades que se pueden imponer varían, aunque podrían incluir:

- Multas administrativas, por ejemplo, el RGPD fija multas en €20 millones, o el 4 % de los ingresos anuales; en Corea del Sur, es el 3% de los ingresos anuales.
- Delitos penales (responsabilidad individual) para determinadas acciones, por ejemplo obtener o divulgar datos personales a sabiendas o descuidadamente, sin el consentimiento del responsable del tratamiento.
- Responsabilidad directa para los directores de empresas.

Referencias

1 Consulte: sección 4: 4. Estándares para mecanismos de ejecución, y “regulación de respuesta”, capítulo 3: Estándares con los que evaluar las leyes de privacidad de datos de un país, en Greenleaf, G. (2014), Leyes de privacidad de datos en Asia: Perspectivas comerciales y de derechos humanos, Oxford University Press.

2 Esto es debido a que en muchos casos ha transcurrido tiempo entre la adopción de la ley y la designación de la autoridad de control independiente.

PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

PARTE: 8

Documentos de Referencia

Documentos de Referencia

Privacy International

Documentos explicativos

Video: ¿Qué es la protección de datos? Video:
https://www.privacyinternational.org/video/1623/video-what-data-protection

Documento explicativo: ¿Qué es la protección de datos?:
https://www.privacyinternational.org/explainer/41/101-data-protection

¿Qué es el RGPD?:
https://privacyinternational.org/topics/general-data-protection-regulation-gdpr

Recursos educativos

Curso en línea: Derecho de objeción: Introducción y principios:
https://advocacyassembly.org/en/courses/28/#/chapter/1/lesson/1

Curso en línea: Derecho de objeción: Datos y vigilancia:
https://advocacyassembly.org/en/courses/22/#/chapter/1/lesson/1

Curso en línea: Los riegos de los sistemas de uso intensivo de datos:
https://advocacyassembly.org/en/courses/41/#/chapter/1/lesson/1

Análisis de la propugnación y las políticas

Nuestro trabajo: La modernización de la legislación de protección de datos:
https://privacyinternational.org/what-we-do/modernise-data-protection-law

Temáticas: Protección de datos:
https://privacyinternational.org/topics/data-protection Análisis legal y político a nivel nacional e internacionalhttps://privacyinternational.org/how-we-fight/advocacy-and-policy

Investigación

Estado de privacidad: https://privacyinternational.org/type-resource/state-privacy

Manipulación invisible: 10 maneras en que se utilizan nuestros datos en nuestra contra: https://privacyinternational.org/feature/1064/invisible-manipulation-10-ways-our-data-being-used-against-us

Organizaciones y redes especializadas

Derechos Digitales Europeos (EDRi, por sus siglas en inglés): https://edri.org

Diálogo Transatlántico de Consumidores: http://tacd.org

Consumer International: https://www.consumersinternational.org

Asociación Internacional de Profesionales de la Privacidad (IAPP, por sus siglas en inglés): https://iapp.org/resources/IEEE https://www.ieee.org/publications/index.html

Agencia de Derechos Fundamentales de la Unión Europea

Tema: Sociedad de la información, privacidad y protección de datos: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection

Manual sobre legislación europea para la protección de datos, junio de 2018: http://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law

Naciones Unidas

Consejo Económico y Social, Desarrollos de Derechos Humanos y Científicos y Tecnológicos, nota del Secretario General, E/CN.4/1233, 16 de diciembre de 1976: https://digitallibrary.un.org/record/559884/files/E_CN.4_1233-EN.pdf

Asamblea General de la ONU Principios Rectores para la Reglamentación de Archivos Computarizados de Datos Personales: http://www.un.org/documents/ga/res/45/a45r095.htm

El derecho a la privacidad en la Era Digital: https://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx

Análisis legal

DLA Piper, Comparación de la legislación de protección de datos en todo el mundo y Manual: https://www.dlapiperdataprotection.com

Organismos reguladores nacionales, regionales e internacionales

Consejo Europeo: http://www.coe.int/en/web/data-protection/home

La protección de datos en la Unión Europea:
http://ec.europa.eu/justice/data-protection/

Grupo de trabajo del artículo 29 (ahora disuelto y sustituido por el Comité Europeo de Protección de Datos):
http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358

Organizaciones de Estados Americanos:
http://www.oas.org/dil/data_protection.htm

Asociación francophone des autorités de protection des données personnelles (AFAPDP, por sus siglas en francés): https://www.afapdp.org/documents

Conferencia Internacional de Comisarios de Protección de Datos y Privacidad:
https://icdppc.org/document-archive/

Red Iberoamericana de Protección de Datos (RIPD):
http://www.redipd.es/documentacion/index-ides-idphp.php

Autoridades de privacidad de Asia-Pacífico (APPA, por sus siglas en inglés):
http://www.appaforum.org/resources/

Academia

Brussels Privacy Hub, Vrije Universiteit Brussels:
https://www.brusselsprivacyhub.eu/index.html

Legislación Internacional para la Privacidad de Datos (DIPL, por sus siglas en inglés), Oxford University Press: https://academic.oup.com/idpl

Graham Greenleaf, Universidad de Nueva Gales del Sur, Facultad de Derecho, Australia: https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=57970

Posibilidades para el Compromiso

Existen diversas oportunidades de colaboración para las organizaciones de la sociedad civil interesadas en comprometerse con la promoción y la protección del derecho a la privacidad de las personas y de la protección de sus datos. A continuación, presentamos una lista que no es exhaustiva. Sin embargo, se ofrecen varias posibilidades de compromiso a nivel nacional e internacional, que esperamos alentarán a más organizaciones de la sociedad civil de todas las disciplinas a involucrarse en el desarrollo de políticas y en los procesos jurídicos de la protección de datos.

A nivel nacional

Organizaciones de la sociedad civil

Las organizaciones de la sociedad civil deben participar para garantizar que los procesos de elaboración de políticas sean abiertos, inclusivos y transparentes. Es importante que más organizaciones diversas se unan a la campaña para la protección de la privacidad y la protección de datos. Las organizaciones de la sociedad civil cuyo mandato es promover y defender la protección de los derechos fundamentales tienen un rol fundamental en el emprendimiento de investigaciones independientes, al igual que en el análisis legal y político de las prácticas y las políticas actuales y las propuestas para la protección de datos. Estos esfuerzos colaborativos tienen un rol esencial en informar y educar a los actores relevantes para garantizar que se adopten y se ejecuten los estándares y las medidas de seguridad y privacidad más elevadas, y para que las instituciones públicas y privadas cumplan con sus obligaciones nacionales y de derechos humanos.

Mediante nuestro trabajo con nuestra red, hemos promovido durante más de una década la adopción de leyes de protección de datos en todo el mundo. Obtenga más información sobre la red: https://privacyinternational.org/partners

Autoridades de control independientes

En el caso de que ya existan, las autoridades de control independientes, generalmente conocidas como autoridades nacionales para la protección de datos y la privacidad, tienen el mandato y la responsabilidad de dar efecto y garantizar la ejecución de la legislación de protección de datos. A medida que avanza el debate con estas autoridades en torno al compromiso con la protección de datos, es esencial garantizar el entendimiento de los nuevos desafíos que presentan las recientes tecnologías y sistemas, al igual que las implicancias para la protección y la promoción de los derechos fundamentales. Las consultas públicas organizadas por la autoridad a medida que desarrolla nuevas políticas, directrices y estándares constituyen oportunidades para que las organizaciones de la sociedad civil compartan sus inquietudes y recomendaciones.

Comunidad jurídica, poder judicial e instituciones judiciales

Una posibilidad de compromiso es el trabajo de generación de conciencia y capacitación en la comunidad jurídica, tanto con abogados como con jueces. Esto resulta esencial para garantizar que el poder judicial esté bien informado y capacitado, lo que constituye una necesidad cada vez más imperante al momento de considerar casos de violaciones a la privacidad y situaciones que implican tecnologías e innovaciones más avanzadas. En segundo lugar, el litigio estratégico proporciona una oportunidad única para poner en tela de juicio la legislación y las prácticas existentes, y para solicitar una reforma que garantice que las leyes sean coherentes y se interpreten según los estándares nacionales, regionales e internacionales de derechos humanos. Las normas establecidas y fortalecidas por los órganos jurisdiccionales proporcionan sólidas oportunidades de propugnación porque garantizan su implementación por parte de los actores relevantes, en conformidad con la ley y también como medio de generación de conciencia entre la sociedad en cuanto a sus derecho

Instituciones nacionales de derechos humanos

En los países en los que los Gobiernos y los órganos jurisdiccionales no respetan el Estado de derecho, las instituciones de derechos humanos tienen un rol importante como protectoras y vigilantes de los derechos humanos. Como destacamos en nuestra guía, la protección de datos está estrechamente vinculada con la promoción y la protección del derecho a la privacidad. Si bien comprende diversas facetas, uno de los aspectos fundamentales que componen este derecho, que resulta cada vez más relevante en la vida de las personas, es la protección de los datos de las personas. Por lo tanto, el compromiso con las instituciones de derechos humanos es esencial para garantizar que las interferencias y las violaciones a la protección de datos y el derecho a la privacidad se investiguen, documenten y den lugar a acciones reparadoras. Esto requiere la generación de conciencia sobre los desafíos que implican el desarrollo y el uso de nuevas tecnologías, si se implementan en un vacío legal, con escasos o ningún mecanismo regulatorio y sin consideración de los derechos humanos. Las organizaciones de la sociedad civil proporcionan una fuente importante de información para estas instituciones porque contribuyen a guiar las investigaciones, hacer un seguimiento de las estrategias y establecer prioridades.

Organismos reguladores sectoriales

Muchos países cuentan con una variedad de organismos reguladores que supervisan la efectiva implementación de leyes o políticas sectoriales, que pueden incluir (o no) disposiciones de protección de la privacidad y de los datos (or ejemplo, los reguladores de las telecomunicaciones, que tienen un papel cada vez más importante en áreas relacionadas con la vigilancia de las comunicaciones y la gestión del espectro de las técnicas de vigilancia táctica). Cada vez con mayor frecuencia, las comisiones electorales y las agencias de cuestiones sociales y de bienestar se están convirtiendo en partidarias de la ampliación de las bases de datos y la invasión de los sistemas de identidad. Las organizaciones de la sociedad

civil pueden adoptar un rol útil contribuyendo a que estas instituciones comprendan mejor los nuevos desafíos propuestos por las tecnologías y los sistemas más recientes.

Ministerios y órganos legislativos

Diversos ministerios y órganos legislativos están elaborando leyes y políticas sobre tecnología a diario, lo que tiene significativa implicancia para la gobernanza de los datos personales y la protección de los derechos fundamentales. Sin embargo, suelen carecer de leyes apropiadas para proteger la privacidad y, por lo tanto, tampoco cuentan con un marco de gobernanza para considerar. En muchos países, este vacío legal significa que no existen (o existen pocas) garantías para la protección, y las oportunidades de reparación son ineficientes o tampoco existen. La sociedad civil ha realizado sus propias investigaciones, está capacitada y ha adquirido experiencia en las implicancias prácticas que las políticas actuales tienen en los derechos humanos. Esto la convierte en un actor fundamental para presentar y consolidar sus conocimientos y experiencia ante los ministerios y las agencias gubernamentales, las comisiones parlamentarias y los organismos responsables de diseñar y reformar las leyes.

A nivel regional e internacional

Órganos de las Naciones Unidas

Algunos órganos de las Naciones Unidas tienen el mandato y la capacidad de controlar y proporcionar recomendaciones y reparaciones. Brindando principalmente sus enfoques abiertos y consultivos, estos órganos proporcionan un espacio importante para que la sociedad civil se comprometa y transmita sus preocupaciones y los desafíos que enfrentan a nivel nacional, como resultado de las políticas y prácticas nacionales, regionales e internacionales implementadas, así como para que promuevan un cambio en sus respectivos países. Existen varias oportunidades para presentar problemáticas relacionadas con la protección de los datos y la privacidad en algunos de los órganos de tratados de la ONU, al igual que mecanismos de seguimiento e informe de derechos humanos, según lo descrito en la guía “¿Cómo hablar sobre privacidad en la ONU?” de Privacy International Para obtener más información consulte:
https://privacyinternational.org/feature/1030/brief-guide-how-talk-about-privacy-un.

Comité Consultivo (T-PD) del Convenio 108 del Consejo de Europa

Establecido por el Convenio 108, el Comité Consultivo (T-PD) consiste en representantes de las partes del convenio modernizado para la protección de personas en relación con el tratamiento de datos personales, complementado por observadores de otros Estados (miembros o no miembros) y organizaciones internacionales. Asimismo, es responsable de interpretar las disposiciones y mejorar la implementación del convenio. El Comité Consultivo del Convenio 108 también es responsable de diseñar informes, directrices y principios guía sobre

tópicos como, por ejemplo, las cláusulas contractuales que rigen la protección de datos durante la transferencia de datos personales a terceros que no están obligados a un nivel adecuado de protección de datos, o la protección de datos en relación con la biométrica. Para obtener más información consulte: https://www.coe.int/en/web/data-protection/consultative-committee-tpd.

Conferencia Internacional de Comisarios de Protección de Datos y Privacidad (ICDPPC, por sus siglas en inglés)

La Conferencia Internacional de Comisarios de Protección de Datos y Privacidad (ICDPPC, por sus siglas en inglés) fue establecida en 1979 con la visión de un entorno en el que las autoridades de protección de datos y privacidad en todo el mundo son capaces de cumplir efectivamente con su mandato, ya sea individualmente o en conjunto, mediante la difusión de conocimientos y conexiones de respaldo. Organizada anualmente, la Conferencia ha establecido cuatro prioridades de alto nivel para que las acciones resulten focalizadas y más efectivas: 1) fortalecimiento de conexiones; 2) trabajo con socios; 3) el avance de la privacidad global en la era digital y 4) completar la consolidación de capacidades de la conferencia y evaluar la efectividad. Como segundo plan estratégico, estas prioridades tienen el objetivo de mejorar la capacidad de acción de la conferencia. La conferencia adopta diversas resoluciones y emite declaraciones que presentan sus resultados clave, además de describir los próximos proyectos que serán llevados a cabo por la Secretaría y las autoridades nacionales de protección de datos. Para obtener más información consulte: https://icdppc.org

Association francophone des autorités de protection des données personnelles (AFAPDP, por sus siglas en francés)

La AFAPDP se estableció en 2007. Reúne a las autoridades independientes de protección de datos de 19 Estados que comparten un idioma, un legado legal y valores. La visión de la ADAPDP es promover la adopción de medidas para salvaguardar efectiva y eficientemente el derecho de las personas a la protección de sus datos. Tiene el objetivo de contribuir con la garantía de los derechos fundamentales de las personas que promueven un espacio digital francófono basado en la confianza adecuada para el desarrollo económico. Trabaja en el fortalecimiento de la capacidad de los miembros de la AFAPDP para alentar la investigación y compartir las mejores prácticas, actuar como centro de experiencia, recoger y divulgar información sobre sus miembros y cooperar con otras organizaciones para promover la protección de los datos y la democracia. La AFAPDP se reúne anualmente para su asamblea general y también organiza una conferencia anual. Se realizan visitas de campo en los países miembro para explorar el territorio o las temáticas específicas. Para obtener más información consulte: https://www.afapdp.org

Red Iberoamericana de Protección de Datos (RIPD)

La Red Iberoamericana de Protección de Datos (RIPD) fue establecida en 2003. El objetivo de la RIPD es promocionar la colaboración y el diálogo, así como

compartir información, promover políticas y metodologías para garantizar una avanzada regulación del derecho a la protección de datos personales.

Actualmente consiste en 22 autoridades de protección de datos de España, Portugal, México y otros países de América Central y América del Sur y el Caribe. Durante la última década, la organización ha promovido el desarrollo de una legislación integral de protección de datos y la introducción de autoridades de protección de datos en toda Latinoamérica. La RIPD promueve el diálogo e impulsa iniciativas de establecimiento de agenda mediante la organización de encuentros anuales, seminarios y talleres, así como la elaboración de estándares y principios para respaldar a las autoridades de protección de datos y a otros actores involucrados en la protección de datos. Para obtener más información consulte: http://www.redipd.es/index-ides-idphp.php

Autoridades de privacidad de Asia-Pacífico (APPA, por sus siglas en inglés) http://www.appaforum.org/resources/

Se trata de un foro para las autoridades de protección de datos y privacidad en la región de Asia-Pacífico. Otorga a las autoridades de la región la oportunidad de crear asociaciones, debatir sobre mejores prácticas y compartir información sobre la tecnología emergente, las tendencias y los cambios a la regulación de la privacidad. Los miembros de APPA se reúnen dos veces al año, debaten temas permanentes en su agenda, como los informes jurisdiccionales de cada delegación, y realizan mesas redondas de intercambio de iniciativas. En cada foro, los miembros debaten y se concentran en diferentes temáticas. Para obtener más información consulte: http://www.appaforum.org

El Comité Europeo de Protección de Datos

El Comité Europeo de Protección de datos (CEPD, antes Grupo de trabajo del artículo 29) es un organismo europeo independiente que contribuye con la aplicación coherente de la normativa sobre protección de datos en toda la Unión Europea. Además, promociona la cooperación entre las autoridades de protección de datos de la Unión. El CEPD está establecido por el Reglamento General de Protección de Datos (RGPD), y tiene base en Bruselas. Está compuesto por representantes de las autoridades nacionales de protección de datos y el Supervisor Europeo de Protección de Datos. Tiene como objetivo garantizar la aplicación coherente en la Unión Europea del Reglamento General de Protección de Datos y de la Directiva Europea para el Cumplimiento de la Ley. Puede adoptar guías generales para clarificar los términos de las leyes europeas de protección de datos, otorgando a los interesados una interpretación coherente de sus derechos y obligaciones. El RGPD también los empodera para tomar decisiones vinculantes hacia las autoridades nacionales de control y garantizar la aplicación coherente. Para obtener más información consulte: https://edpb.europa.eu/edpb_en

Autoridad de Protección de Datos de Europa Central y del Este

Fundada en 2001, la Autoridad de Protección de Datos de Europa Central y del

Este vincula a las instituciones nacionales responsables de la política de protección de datos en 17 estados de Europa Central y del Este. Realiza un encuentro anual y publica recomendaciones y posiciones sobre la implementación de la legislación de protección de datos. Su plataforma en línea está diseñada para respaldar las actividades que apuntan a una cooperación estrecha y una ayuda mutua entre estas autoridades. Para obtener más información consulte: http://www.ceecprivacy.org/main.php

Otros Actores Relevantes

Industria

Los actores económicos han resultado ser influyentes y poderosos en la economía global. En muchos otros sectores comerciales, incluida la minería y la industria de extracción, estos actores han sido objeto de un mayor escrutinio, y se les ha obligado a realizar e implementar evaluaciones de derechos humanos. Sin embargo, esto todavía debe convertirse en la norma en el sector de la industria.

Si bien los Gobiernos tienen la responsabilidad final de garantizar que los ciudadanos gocen de sus derechos fundamentales, que incluyen recibir protección ante la acción de terceros, algunas de las responsabilidades recaen en la industria. La sociedad civil puede asumir un rol en la generación de conciencia sobre el derecho a la privacidad y los riesgos que surgen a partir de actividades comerciales de la industria, ya sea directamente o coludiendo con otros.

La industria está en una posición de poder y, si se logra involucrarla efectivamente, podría convertirse en un aliado para garantizar la protección de los derechos, logrando que no coluda con terceros y que no reciba presiones para llevar a cabo prácticas que violan los derechos humanos.

Comunidad tecnológica

Esta comunidad incluye a los individuos y los grupos que diseñan nuevas tecnologías, e investigadores de seguridad y hackers. Si bien una gran parte del debate se desarrolla en torno a la gobernanza y la regulación insatisfactorias de estas tecnologías más que en la tecnología en sí misma, este grupo es un posible aliado con el que nuestra comunidad debe involucrarse más. Al trabajar con la comunidad tecnológica, las organizaciones de la sociedad civil pueden identificar y prescribir estándares para la promoción de enfoques de privacidad desde el diseño hasta la innovación, en particular para habilitar la gobernanza de la información.

Media

Los medios tienen un rol fundamental en el control, la investigación y el intercambio de la información. También suelen ser una gran fuerza como protectores de la democracia y la buena gobernanza. Las formas tradicionales de medios siguen siendo una fuente importante de información para el público, en particular en países donde Internet no es tan fácilmente accesible y no es tan confiable.

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471