PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

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 personale
- 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 volumen 3, número de artículo: 1376 (2013), disponible en https://rdcu.be/WBtA

3 Resolución de privacidad desde el diseño, 32.a Conferencia Internacional de Comisarios de Protección de Datos y Privacidad, Jerusalén, Israel, 27-29 de octubre, 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 responsabilidad 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
62 Britton Street, London EC1M 5UY
United Kingdom

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

UK Registered Charity No. 1147471