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

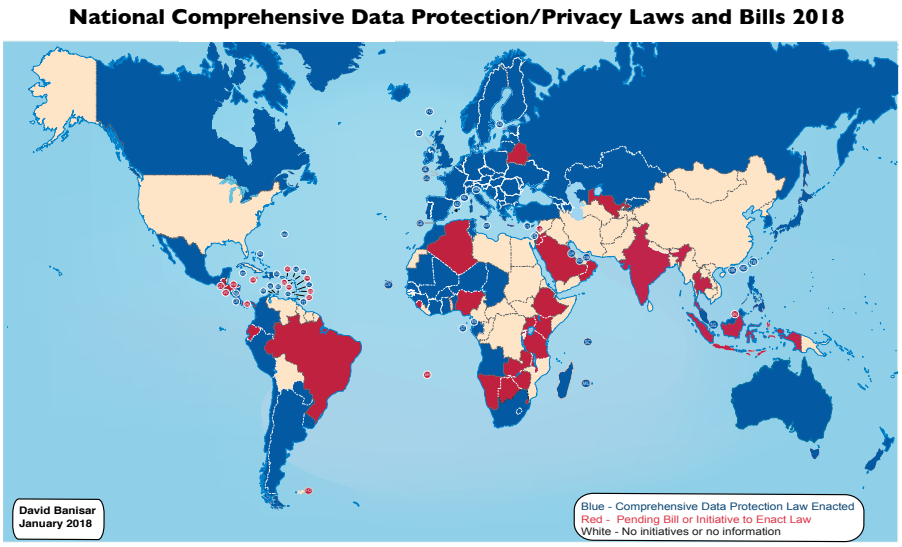
La responsabilidad debe ser el aspecto central de cualquier legislación que regule el tratamiento de datos personales y la protección de los derechos de las personas. Por lo tanto, un ente o autoridad reguladora debe estar a cargo de la ejecución de las normas de protección de datos. El alcance de las 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 https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=0900001680089ff4e

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
62 Britton Street, London EC1M 5UY
United Kingdom

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

UK Registered Charity No. 1147471