PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

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.

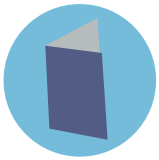
Derechos de Los Interesados

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
62 Britton Street, London EC1M 5UY
United Kingdom

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

UK Registered Charity No. 1147471