PRIVACY INTERNATIONAL

Guía para Involucrarse en Políticas Públicas de Protección de Datos

Principios de Protección de Datos

Lealtad, legalidad y transparencia

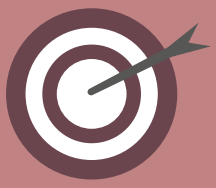
El tratamiento de datos personales debe ser lícito, leal, y efectuado de manera transparente.

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,[10] es esencial que existan limitaciones estrictas a la conservación de datos para mitigar posibles interferencias ilegales con el derecho a la privacidad.

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 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.[11]

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 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.[12]

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
62 Britton Street, London EC1M 5UY
United Kingdom

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

UK Registered Charity No. 1147471