Introducción a la privacidad en Internet

Informe de la Internet Society

La privacidad ayuda a reforzar la confianza de los usuarios en los servicios en línea. Sin embargo, la privacidad en línea está constantemente bajo presión de ser quebrantada. Promover leyes de privacidad de datos que sean fuertes e independientes de la tecnología, principios de privacidad por diseño y principios éticos en la recolección y tratamiento de los datos es un enfoque clave para proteger y fomentar la privacidad en línea.

Introducción

La privacidad es un derecho importante[1] y un facilitador fundamental de la autonomía personal, la dignidad y la libertad de expresión. Aunque no existe una definición de privacidad universalmente aceptada, en el contexto de Internet en general se conviene que privacidad *es el derecho de determinar cuándo, cómo y en qué medida los datos personales pueden ser compartidos con terceros*.

En la era digital de hoy, la información se puede recopilar de forma más rápida, fácil y económica que nunca. Los avances en diferentes frentes tecnológicos han contribuido a este nuevo escenario. Por ejemplo:

- El almacenamiento de datos es barato, por lo que los datos están accesibles en línea por largos periodos de tiempo.
- Los datos se pueden intercambiar de forma rápida y distribuida, lo que permite su fácil proliferación.
- Las herramientas de búsqueda en Internet pueden reconocer imágenes, rostros, sonidos, voces y movimientos, por lo que resulta fácil rastrear dispositivos y personas en línea a lo largo del tiempo y en diferentes lugares.
- Se están desarrollando sofisticadas herramientas para vincular, correlacionar y agregar a gran escala datos que aparentemente no tienen ninguna relación entre sí.
- Es cada vez más fácil identificar individuos —y clases de individuos— a partir de datos supuestamente anonimizados o desprovistos de identificación.
- Hay cada vez más sensores en objetos y dispositivos móviles conectados a Internet.

Los datos personales se han convertido en una mercancía rentable. Día a día, los usuarios de Internet comparten cada vez más datos personales, a menudo sin saberlo, y la Internet de las Cosas solo

[1] Ver la *Declaración Universal de Derechos Humanos de la ONU,* http://www.un.org/en/documents/udhr/ ; el *Pacto Internacional de Derechos Civiles y Políticos,* http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx ; y la *Convención Europea sobre Derechos Humanos,* http://www.echr.coe.int/Documents/Convention_ENG.pdf

aumentará este fenómeno. Estos factores tienen el potencial de exponer los datos personales de los usuarios y crean desafíos de privacidad a una escala mayor que nunca...

Con esto en mente, es importante fomentar el desarrollo y la aplicación de marcos de privacidad que adopten un enfoque ético para la recolección y el tratamiento de los datos. Marcos que incorporen, entre otras cosas, los conceptos de justicia, transparencia, participación, responsabilidad y legitimidad.

Consideraciones clave

Aunque no existe una ley universal de privacidad o protección de datos que se aplique en toda la Internet, sí existe una serie de marcos de privacidad internacionales y nacionales que han convergido para conformar un conjunto de principios de privacidad esenciales que sirvan de línea de base. Los siguientes principios se derivan de las Directrices de la Organización para la Cooperación y el Desarrollo Económico (OCDE) sobre Privacidad (2013) y se reconoce ampliamente que proporcionan una buena base para el desarrollo de políticas y prácticas de privacidad en línea:

- **Limitaciones a la recolección.** Deben existir límites a la recolección de datos personales. Tales datos se deben obtener por medios legítimos y justos y, cuando corresponda, con el conocimiento o consentimiento del sujeto de los datos.
- **Calidad de los datos.** Los datos personales deben ser pertinentes a los fines para los que se van a utilizar y, en la medida necesaria para tales fines, deben ser precisos, completos y estar al día.
- **Especificación de los fines.** Se deben especificar los fines para los que se recogen los datos personales. Su uso se debe limitar a estos fines o a otros que no sean incompatibles.
- **Limitación del uso.** Los datos personales no se deben divulgar, poner a disposición de terceros ni utilizar para otros fines, excepto con el consentimiento de la persona o cuando lo autorice la ley.
- **Garantías de seguridad.** Los datos personales deben estar protegidos por garantías de seguridad razonables.
- **Apertura.** Debe existir una política general de apertura que se aplique a los desarrollos, prácticas y políticas relacionados con los datos personales.
- **Participación individual.** Las personas deben tener el derecho de obtener información sobre los datos personales en poder de los demás y de que estos datos se borren, rectifiquen, completen o modifiquen, según corresponda.
- **Responsabilidad.** Quienes recogen datos personales deben ser responsables de cumplir con los principios.

Cabe señalar que muchos de estos principios implican transparencia con respecto a quién está recopilando los datos y para qué se están utilizando.

Desafíos

Al determinar acciones relacionadas con la privacidad en línea, los formuladores de políticas deben considerar una serie de desafíos clave. Algunos desafíos son ampliamente reconocidos e incluyen los siguientes:

1. **Determinar cuáles datos deben ser protegidos.** Por lo general, las leyes de privacidad y protección de datos se aplican a los datos personales, en algunas jurisdicciones también conocidos como *información*

personal. Una definición habitual indica que datos personales son “cualquier información sobre una persona física identificada o identificable”.[2] Pero no todas las definiciones son iguales. Además, puede ser difícil determinar qué tipos específicos de datos se consideran información personal en un contexto particular. Por otra parte, la rápida evolución de los servicios y la tecnología utilizada para procesar los datos implica que determinar qué es lo que hay que proteger es un desafío permanente.

2 **Diferentes requisitos legales relativos a la protección de datos.** Las leyes de privacidad no son iguales en todos los países. Esto significa que algunos datos pueden estar legalmente protegidos en un país pero no en otro. Además, incluso cuando los datos estén cubiertos por las leyes de ambos países, las protecciones ofrecidas pueden ser diferentes (por ejemplo, la recolección de datos puede ser por inclusión o exclusión voluntaria, también llamados sistemas *opt-in* u *opt-out*). Para complicar todavía más las cosas, más de un país puede querer hacer valer sus leyes. Por ejemplo, un país puede afirmar que se aplica su derecho de protección de datos porque los datos personales se refieren a sus ciudadanos, mientras que otro puede afirmar que se aplica el suyo porque la empresa que recoge los datos tiene su sede en su territorio nacional. Poner en práctica los derechos y expectativas de privacidad individuales puede ser especialmente problemático cuando las leyes de los países están en conflicto directo o son de alguna forma incompatibles. En particular, las recientes controversias relativas a la vigilancia masiva han planteado la cuestión de si las cláusulas que hablan del principio de “necesidad y proporcionalidad” ofrecen suficiente protección a los ciudadanos. Los debates globales en torno al tema de la vigilancia ponen de relieve lo difícil que resulta para los estados nacionales ponerse de acuerdo y llegar a interpretaciones coherentes de las convenciones internacionales en la esfera de la privacidad, como por ejemplo en materia de derechos humanos o derechos civiles y políticos.

3 **Protección de la privacidad cuando los datos atraviesan fronteras.** Internet se extiende más allá de las fronteras nacionales, pero las leyes de privacidad y protección de datos se basan en la soberanía nacional. Es por ello que se necesitan disposiciones especiales para proteger los datos personales que abandonan un país e ingresan en otro de manera de asegurarle a los usuarios la continuidad de la protección de sus datos. Los enfoques varían, pero tienden a tener en cuenta si el país receptor tiene una protección “adecuada”. En este sentido, han surgido diferentes marcos para facilitar los flujos de datos transfronterizos dentro de una misma región o entre diferentes regiones.[3]

4 **Consentimiento real y significativo.** En general, las leyes de privacidad y protección de los datos personales permiten cierto grado de recopilación y uso de los datos personales si el individuo otorga su consentimiento. En teoría, este enfoque empodera a los usuarios de Internet de modo que tengan un cierto nivel de control o elección en relación con la manera en que otros recogen y utilizan sus datos. Sin embargo, en la práctica los usuarios de los servicios en línea podrían no leer o no comprender qué es lo que están aceptando (por ejemplo, porque los términos de servicio son extensos y están escritos en un lenguaje jurídico complejo). Incluso si comprenden los términos, los usuarios pueden no ser capaces de negociarlos. El uso generalizado de dispositivos móviles con sensores y pantallas pequeñas donde se muestran las opciones de privacidad y los usos secundarios frecuentes de los datos personales (por

[2] Las siguientes publicaciones contienen definiciones de datos personales: Directrices de la OCDE *sobre Privacidad (2013)*; Convención *108 del Consejo de Europa*; Directiva de la UE *sobre Protección de los Datos (1995)* y Convención *de la Unión Africana sobre Ciberseguridad y Protección de los Datos Personales.*

[3] Entre los marcos transfronterizos se pueden mencionar los siguientes: el *Sistema de Reglas de Privacidad Transfronteriza de APEC (CBPR)*, el *Marco de “Safe Harbor” EE.UU.-UE*, las *Reglas Corporativas Vinculantes de la UE.*

ejemplo, para entregar publicidad dirigida) generan problemas adicionales a la hora de que los usuarios ejerzan control sobre sus datos personales. Un enfoque técnico podría consistir en fomentar el desarrollo de sistemas que hagan más fácil que el usuario comprenda y gestione la información que recogen los dispositivos inteligentes y conectados que los rodean.

Principios rectores

Dado que los datos personales tienen valor monetario y estratégico para los demás, es un desafío asegurar que estos datos solo se recopilen y utilicen apropiadamente. Los siguientes principios rectores promueven el logro de este resultado:

- **Interoperabilidad global.** Alentar la adopción de estándares de privacidad (tanto técnicos como reglamentarios) desarrollados de forma abierta, que sean interoperables a nivel global y que faciliten los flujos de datos transfronterizos y a la vez protejan la privacidad.
- **Colaboración.** Promover la colaboración de múltiples partes interesadas y un enfoque holístico que asegure valor para todas las partes.
- **Ética.** Promover marcos de privacidad que apliquen un enfoque ético en la recolección y tratamiento de datos. Entre otras cosas, los enfoques éticos incorporan los conceptos de equidad, transparencia, participación, responsabilidad y legitimidad en la recolección y tratamiento de los datos.
- **Impacto sobre la privacidad.** Comprender el impacto que tiene la recolección y utilización de datos personales sobre la privacidad. Considerar las implicancias de los metadatos para la privacidad. Reconocer que incluso la mera posibilidad de la recolección de datos personales podría interferir con el derecho a la privacidad. Además, comprender que la privacidad de una persona puede verse afectada incluso si dicha persona no es identificable pero sí puede ser 'marcada'.
- **Anonimato y seudoanonimato.** Las personas deben poder comunicarse a través de Internet de forma confidencial y anónima.
- **Minimización de los datos.** Fomentar prácticas de minimización de los datos. Insistir en la recolección selectiva de datos y el uso exclusivamente de los datos necesarios y solo por el tiempo que sea necesario.
- **Posibilidad de elección.** Empoderar a los usuarios para que puedan negociar términos de recolección y tratamiento de datos justos, en pie de igualdad con quienes los recogen, y también para que puedan otorgar un consentimiento significativo.
- **Entorno legal.** Promover leyes fuertes y que no dependan de ninguna tecnología específica, su cumplimiento y aplicación eficaz. Estas leyes deben concentrarse en los resultados de privacidad deseados, no en especificar determinados medios tecnológicos para dirigir las prácticas de privacidad.
- **Entorno técnico.** Promover entornos abiertos que apoyen el desarrollo voluntario y basado en el consenso de protocolos y estándares que soporten soluciones para mejorar la privacidad.
- **Entorno de negocios.** Ayudar a que las empresas reconozcan que los enfoques que respetan la privacidad pueden ofrecer ventajas competitivas y reducir su exposición a riesgos legales.
- **Principios de privacidad por diseño.** Promover la privacidad por diseño de todo el ciclo de desarrollo, implementación y despliegue. Los principios de privacidad por diseño también se deben aplicar al desarrollo de estándares, aplicaciones, servicios y procesos de negocio.

- **Herramientas.** Promover el desarrollo de herramientas útiles que permitan a los usuarios expresar sus preferencias de privacidad y comunicarse de forma confidencial (por ejemplo, el cifrado) y anónima o seudoanónima y que además permitan a los proveedores de servicios ofrecer opciones y la posibilidad de visualizar lo que está ocurriendo con los datos del usuario.

Recursos adicionales

La Internet Society ha publicado una serie de documentos y contenido adicional relacionado con este tema. Se puede acceder libremente a estos materiales en nuestro sitio web.

- Página de recursos de la Internet Society sobre privacidad, http://www.internetsociety.org/our-work-privacy
- Página de recursos de la Internet Society sobre huella digital, http://www.internetsociety.org/your-digital-footprint
- Identidad en línea: ¿Qué es la identidad?, http://www.internetsociety.org/understanding-your-online-identity-overview-identity
- Identidad en línea: Protección de la privacidad, http://www.internetsociety.org/understanding-your-online-identity-protecting-your-privacy
- Identidad en línea: Cómo proteger nuestra identidad en línea, http://www.internetsociety.org/understanding-your-online-identity-learning-protect-your-identity

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva, Switzerland
Tel: +41 22 807 1444 • Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave., Suite 201
Reston, VA 20190 USA
Tel: +1 703 439 2120 • Fax: +1 703 326 9881
Correo electrónico: info@isoc.org

bp-privacy-20151030-es