Privacidad de datos: los límites de Internet y el acceso a la información

Jorge Bossio
Profesor de Ciencias de la Información de la PUCP
Setiembre, 2008

Bossio, Jorge (2008, Setiembre). Privacidad de datos: los límites de Internet y el acceso a la información. *Palestra, Portal de Asuntos Públicos de la PUCP*. En: http://palestra.pucp.edu.pe/?id=393

El artículo fue preparado y publicado originalmente para "Palestra, Portal de Asuntos Públicos de la PUCP", 2008.

Sumilla: El crecimiento de la población que registra datos personales a través de Internet hace relevante el tema de la protección de este tipo de información. El desarrollo del comercio internacional y electrónico hace que los datos personales se transmitan más allá de las fronteras nacionales, donde los derechos podrían no estar garantizados por el Estado. A esto se suma el desarrollo acelerado de la deslocalización de servicios -muchas empresas confían algunas etapas de su proceso de negocio a empresas de otros países-, lo que aumenta la preocupación de los Estados por la protección de los datos personales de sus ciudadanos. Se espera que con la próxima promulgación de una Ley de Protección de Datos Personales, el Perú pueda entrar en la competencia regional por el mercado de deslocalización de servicios (especialmente de "Call Centers").

Las Tecnologías de la Información son alabadas por sus grandes beneficios, y otras veces criticadas por el riesgo que implica el uso de esta herramienta por organizaciones o personas que realizan actividades ilegales -desde las que utilizan información ajena comercialmente, sin derecho de su propietario, hasta organizaciones terroristas, pasando por una amplia gama de criminales que se esconden en el anonimato que les brinda la red para realizar sus actos-. Las redes de pornografía infantil y la seducción en línea han constituido los ejemplos mas difundidos de estas prácticas.

Quienes tienen a su cargo la toma de decisiones y el diseño de políticas públicas deben manejar ese doble escenario: por un lado *promover* el desarrollo de una herramienta que es beneficiosa para la sociedad; y, por otro, *proteger* a los ciudadanos frente al uso indebido de esta herramienta. El tema de la privacidad de datos se sitúa en el centro de la discusión.

La privacidad como derecho fundamental

La privacidad de las personas y, específicamente, de las comunicaciones, es un derecho humano fundamental, como lo señala el artículo 12 de la Declaración Universal de los Derechos Humanos. Los estados tienen la responsabilidad de garantizar este derecho:

> *"Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques."*[1]

Las Tecnologías de la Información plantean retos importantes para los Estados en esta materia, y es por ello que muchos han buscado consagrar este derecho.

En el Perú, el derecho a la autodeterminación informativa está reconocido por la Constitución Política, la cual consagra como derecho fundamental de toda persona que "los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar." [2]

Este derecho es exigible a través de la Acción de Habeas Data. Así lo señala el Código Procesal Constitucional de 2004 en su artículo 61°, mediante el cual se precisa el derecho no solo al acceso a la información, sino al conocimiento, modificación e incluso supresión de la información personal que es registrada en bases de datos públicas o privadas.

> *"En consecuencia, toda persona puede acudir a dicho proceso para:(...) Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales." (Código Procesal Constitucional, art 61°)*

La existencia de mecanismos adecuados para el ejercicio de estos derechos se convierte en una importante necesidad para la sociedad, especialmente en un contexto en el cual cada día un mayor porcentaje de la población interactúa a través de Internet y registra (y muchas veces expone) información personal que podría ser utilizada con fines ajenos a los intereses de las personas.

El uso de Internet en el Perú

En el Perú, la población mayor a seis años de edad que accede a Internet representa el 27% según la Encuesta Nacional de Hogares (INEI 2008). No obstante, dado que sólo el 6,9% de los hogares cuenta con acceso a Internet, las Cabinas Públicas continúan siendo el principal punto de acceso para más del 70% de los usuarios a nivel nacional.

Si bien las cabinas públicas han permitido democratizar el acceso a Internet, el perfil del usuario de Internet en el Perú refleja las notorias condiciones de exclusión social. Es así que, aún cuando la proporción de hombres y mujeres en la población peruana es similar, sólo un 23% de las mujeres sería usuaria de Internet, frente al 31% en el caso de los hombres. Peor aún, solo un 6,2% de la población rural y el 6,6% de la población de lengua nativa en el Perú serían usuarias de Internet según el mismo reporte.

Los principales usos de Internet serían la comunicación (78,5%) y la búsqueda de información (74,7%); lo que coincide (aunque en diferente proporción) con las estimaciones de Apoyo (2007) en Lima, 81% y 54% respectivamente.

[1] Declaración Universal de los Derechos Humanos. Disponible en: http://www.un.org/spanish/aboutun/hrights.htm
[2] Constitución Política del Perú de 1993 artículo 2º inciso 6

Los usuarios con mayor antigüedad (y experiencia) en la red son principalmente hombres de mediana edad. Las mujeres y los niños constituyen el grupo en crecimiento pero también el grupo con menor experiencia y en consecuencia los que se encuentran más vulnerables.
Si bien no se cuenta con datos estadísticos aún, es notorio el crecimiento de la participación de los "internautas peruanos" en la llamada web 2.0, a través de los blogs, wikis y software de redes sociales como MySpace, HI5 y Facebook, entre otros.

Las transacciones electrónicas permiten que nuestro accionar quede registrado en bases de datos: cuando cargamos gasolina con la tarjeta de crédito se registra la hora, lugar, cantidad y, hasta hace poco, la placa de nuestro auto; cuando ingresamos a una oficina se registra nuestro nombre y número de DNI, hora de entrada y salida; cuando llegamos a trabajar; cuando nos registramos ("logueamos") a la red; cuando enviamos un correo electrónico; cuando hacemos una búsqueda en Google; cuando hacemos una llamada telefónica; cuando nos prestamos un libro de la biblioteca; cuando vamos al banco, al centro comercial, al cine, es decir: casi toda nuestra vida se registra en bases de datos. ¿Sabemos exactamente quién y con qué objetivo usa esa información? Ciertamente no, y por ello constituye una preocupación que limita el desarrollo del comercio electrónico.

La privacidad y el comercio electrónico

Aún cuando muchos de los usuarios no prestemos atención a la protección de nuestros datos personales, nos damos cuenta que bases de datos con nuestra información personal está siendo comercializada sin nuestra autorización cuando los correos electrónicos no solicitados (conocidos como spam) colman nuestra bandeja de entrada, o cuando recibimos llamadas de entidades financieras, hoteles o clubes para ofrecernos sus servicios y nos damos cuenta que saben mucho sobre nosotros, probablemente mas de lo que quisiéramos.

Para los negocios, el manejo de información sobre el comportamiento de sus clientes es fundamental; no solo para garantizar un buen servicio, sino también para conocer las preferencias del consumidor, adaptarse a los cambios y plantear estrategias innovadoras que le permitan ofrecer mejores productos y servicios. Los consumidores sabemos eso y deliberadamente accedemos a entregar nuestra información en un acto de confianza hacia nuestro proveedor de bienes o servicios.

Sin embargo, el desarrollo acelerado del comercio internacional, y del comercio electrónico en particular, nos obliga a transmitir nuestros datos personales más allá de las fronteras nacionales, donde nuestros derechos podrían no estar garantizados por el Estado, lo cual implica un riesgo mayor.

De hecho, muchas empresas de países desarrollados, en búsqueda de competitividad, confían ciertas etapas de su proceso de negocio a empresas de países en desarrollo. De esta forma, por ejemplo, las llamadas de los clientes o la venta telefónica son actividades que se llevan a cabo en otros países a través de los Call Centers, sector que, por cierto, presenta un alto crecimiento en América Latina por compartir las mismas zonas horarias con Estados Unidos y el Canadá. Es así que los datos personales que los consumidores confían a sus proveedores de bienes o servicios son transferidos a terceras empresas fuera del país.

El proceso anteriormente descrito y conocido como "deslocalización de servicios" constituye un mercado potencial de US$ 330 mil millones que, según los analistas[3], solo estaría aprovechado en un 10% actualmente y que podría llegar a significar más de 110 billones de dólares en el año 2010.

El desarrollo acelerado de la deslocalización de servicios ha elevado la preocupación de los Estados por proteger los datos personales de sus ciudadanos -que son manejados fuera de los límites de las leyes nacionales-. En muchos casos, esta protección implica la imposición de condiciones a las empresas en los países en desarrollo, dónde se brinda el servicio deslocalizado, para que se adecuen a estándares específicos del país de donde provienen los datos.

Para evitar que estas imposiciones se constituyan en barreras para el comercio de servicios, diversos foros internacionales como la OCDE, APEC, la Comunidad Europea, entre otros, buscan desarrollar marcos comunes y armonizados relacionados con los requisitos que deben cumplir las empresas que tratan datos personales de manera transfronteriza.

Marco internacional para la protección de datos

La Organización para la Cooperación y el Desarrollo Económico – OCDE adoptó en 1980 los lineamientos sobre protección de la privacidad y flujos transfronterizos de datos personales con la finalidad de prevenir potenciales limitaciones al flujo de información que podrían afectar el desarrollo económico, específicamente enfocado en servicios financieros. Posteriormente, en 1985, los países miembros de la OCDE reafirmaron, mediante la Declaración sobre flujos de datos transfronterizos, su compromiso con los principios generales establecidos en los lineamientos.

Luego de 30 años de adoptados los lineamientos, prácticamente todos los países miembros de la OCDE cuentan con marcos legales desarrollados y autoridades establecidas con facultades específicas para garantizar la protección de los datos personales en el ámbito nacional.

El esfuerzo de la OCDE por establecer un marco internacional fue seguido por la Unión Europea, la Organización de las Naciones Unidas (ONU) y el Foro Asia-Pacífico de Cooperación (APEC) han desarrollado también marcos internacionales para la protección de datos personales.

Por lo general, la protección que se desea garantizar mediante estos marcos internacionales se refiere a que la información personal debe ser: (i) obtenida legalmente, (ii) usada solo para el propósito para el cual fue entregado; (iii) solicitada solo si es relevante; (iv) actualizada, (iv) accesible; (v) mantenida en reserva y (vi) destruida luego de ser usada. (EPIC 2007)

En 2006 la OCDE realizó un estudio[4] que tenía como objetivo evaluar la efectividad de las leyes y las instituciones encargadas de su cumplimiento, prestando atención principalmente a la capacidad para resolver problemas relacionados con el flujo transfronterizo de datos personales, encontrando que existe una brecha entre la ley y la práctica en muchos de los

[3] India's outsourcing valued at $60 billion by 2010 / By John Ribeiro, IDG News Service. December 12, 2005
[4] Disponible en http://www.oecd.org/dataoecd/17/43/37558845.pdf

países. Estos resultados motivaron la renovación del compromiso de los países de la OCDE en la cooperación mutua para atender la problemática en conjunto.

Las recomendaciones para la cooperación transfronteriza para la protección de datos se emitieron en junio de 2007[5] y buscan promover el mejoramiento de los marcos legales domésticos para que faciliten la cooperación y el desarrollo de mecanismos internacionales de supervisión y control que a su vez garanticen el cumplimiento de las leyes y principios generalmente aceptados.

Para los países miembros de la Unión Europea, la Directiva 95/46/CE[6] es el texto de referencia en materia de protección de datos personales. La Directiva se elaboró con el objetivo de establecer un equilibrio entre el objetivo de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión. De esta forma, la Directiva establece requisitos estrictos para las empresas e instituciones que manejen bases de datos y señala la creación de un organismo nacional independiente en cada país miembro encargado de la protección de datos personales.

Dentro del Foro de Cooperación Asia Pacífico (APEC) también se viene discutiendo la necesidad de implementar marcos de cooperación internacional para asegurar la protección de datos y para ello se ha iniciado un proceso de implementación en el seno del Grupo de Trabajo de Comercio Electrónico con la finalidad de implementar la Reglas Transfronterizas de Privacidad.

El Marco fue desarrollado sobre las bases de los principios de protección de la Privacidad y el flujo transfronterizo de datos del 23 de septiembre de 1980 en el marco de la Organización para la Cooperación Económica y el Desarrollo (OCDE) y tomando en cuenta la Directiva Europea 95/46/CE.

El Marco de Privacidad de Datos del APEC busca establecer un conjunto de principios y normas comunes que sean adecuadas para los países de la región y que cumplan con el doble objetivo de promover el flujo transfronterizo de datos y proteger a la vez los derechos de los ciudadanos. Por ello establece los siguientes objetivos: (i) Proteger la información personal; (ii) Prevenir la creación de barreras innecesarias al flujo transfronterizo de datos, (iii) Fomentar la uniformidad por parte de empresas multinacionales en los métodos utilizados para la recolección, uso y procesamiento de datos personales y (iv) Fomentar los esfuerzos nacionales e internacionales para promover y hacer cumplir las disposiciones legales de protección de Datos Personales.

El modelo de APEC tiende a establecer líneas generales que orienten a las economías miembro hacia la protección de datos personales sin que ello implique el establecimiento de cláusulas de cumplimiento obligatorio, es un modelo que fomenta la autorregulación, el fortalecimiento de las capacidades de los agentes (empresas, consumidores y reguladores) y la cooperación entre los Estados para la solución de problemas en el flujo transfronterizo de datos.

El debate internacional sobre el Marcos Legales de protección de datos

La publicación de la Directiva Europea 95/46/CE desató un debate sobre los marcos nacionales para la protección de datos y su potencial limitante del comercio mundial de

[5] Disponible en http://www.oecd.org/dataoecd/43/28/38770483.pdf
[6] Disponible en http://derecho.eui.upm.es/DPDPF.pdf

servicios debido principalmente a lo establecido por el artículo 25° de la Directiva que establece la prohibición para la transferencia de datos personales hacia Estados que no ofrezcan un nivel "adecuado" de protección. La evaluación sobre la adecuación de los marcos de protección de datos es llevada a cabo por un Grupo de Trabajo especial y evalúa todas las circunstancias que concurren en una transferencia tomando en cuenta la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, los marcos legales vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

El debate surgió dado que esta disposición impedía el flujo de datos con los Estados Unidos, economía con una política muy distinta a la Europea en la materia. Luego de un extenso proceso de negociación que culminó en el año 2000, Estados Unidos se "adecuó" a la norma Europea mediante un convenio llamado Safe Harbor (Puerto Seguro), consistente en un conjunto de principios de privacidad de adopción voluntaria por las empresas que deseen ser consideradas adecuadas para procesar datos de origen europeo. De esta forma, los Estados Unidos establecieron una política de protección de datos adecuada para el modelo europeo sin que ello implique la adopción del modelo europeo en el marco legal doméstico.

Por lo general, los países de América Latina han adoptado el modelo europeo (específicamente de la red iberoamericana de protección de datos) que implica, entre otras características la creación de un marco legal doméstico, la creación de una autoridad independiente, el consentimiento previo y expreso del consumidor para cualquier uso de sus datos y el establecimiento de un registro de bases de datos. Argentina obtuvo la adecuación mediante el Dictamen 4/2002 del Grupo de Trabajo sobre Protección de Datos en el año 2002[7]. Otros países como Chile y Uruguay estarían buscando obtener dictámenes similares para competir en igualdad de condiciones por el mercado europeo a través de la oferta de servicios de Call Centers.

Retos y oportunidades para el Perú

Del mismo modo que otros países de la región, el Perú está buscando desarrollar sus capacidades para competir en el mercado de la deslocalización. Es así que la Agencia de Promoción de la Inversión Privada implementó en el año 2007 un programa a fin de convertir al Perú en un Hub de Negocios para Call Centers.
Según los estimados de Proinversión, el programa permitió el ingreso de 7 empresas de Call Centers en dicho año esperándose una inversión aproximada de US$ 26 millones y la generación de 20,000 puestos de trabajo constituyéndose en una importante alternativa de empleo juvenil.

Se espera que con la promulgación de la Ley de protección de Datos Personales anunciada recientemente (Andina, 13 de agosto de 2008) por la Ministra de Justicia Rosario Fernández, el Perú pueda obtener la adecuación europea para el flujo transfronterizo de datos y entrar en la competencia regional por este importante mercado.
Más aún, el Perú cuenta con la oportunidad histórica de participar en diversos foros de integración con Europa y con las economías del APEC y de servir, durante el año 2008, como anfitrión y facilitador para las discusiones de dichos foros. Esta participación le

[7] Dictamen disponible en https://www.agpd.es/portalweb/canaldocumentacion/docu_grupo_trabajo/wp29/common/B.2.59-cp--wp63--Dictamen-4.2002.-Protecci-oo--Datos-Argentina.pdf

permitiría aprender y aprovechar lo mejor de ambos escenarios y desarrollar un modelo que sea competitivo para la oferta de servicios a nivel global.

Bibliografía

Apoyo (2007) Usos y Actitudes hacia Internet. Lima, Apoyo Opinión y Mercado

Bossio, Jorge (2007) Privacidad y flujo de datos transfronterizos: oportunidades para la promoción de nuevos mercados en la era digital EN: Latintel Año 3 No. 10 (Noviembre 2007).

Delpiazzo, Carlos E. A la búsqueda del equilibrio entre privacidad y acceso. [Documento electrónico] Consultado por última vez el 18 de agosto de 2008 en http://www.fder.edu.uy/contenido/pdf/9jornadas_idi.pdf

EPIC (2007). Privacy and human rigths 2006.

INEI (2008) Las Tecnologías de Información y Comunicación en los Hogares: Enero-marzo 2008.

OECD (2006) Report on the cross-border enforcement of privacy laws.

OECD (2007) OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy.
Proinversión. PERÚ: Hub de Negocios en Call Centers. [Recurso electrónico] Disponible en: http://www.proinversion.gob.pe/0/0/modulos/JER/PlantillaStandard.aspx?ARE=0&PFL=0&JER=3286

UNESCO (2007) Informe de Análisis y Propuestas en Materia de Acceso a la Información y Privacidad en América Latina. Disponible en: http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/374d0ee90831e4ebaa1def162fa50747/Informe_de_Propuestas.pdf

UNESCO (2007). Informe Situacional de Privacidad y Acceso a la Información en América Latina. Disponible en: http://www.alfa-redi.com/apc-aa-alfaredi/img_upload/374d0ee90831e4ebaa1def162fa50747/Informe_Situacional.pdf