Competencia comunicativa para profesionales de las TIC

Protección de la privacidad en Internet

José Luis Rodríguez Gómez

0. Introducción

El avance de la Sociedad de la información y de las nuevas tecnologías han puesto en un primer plano el debate sobre la privacidad. El problema no comienza en la era internet, sino que tiene antecedentes muy lejanos: la historia de la cultura escrita está llena de libelos y pasquines de contenido difamatorio contra la privacidad del individuo. Pero es cierto, que las intromisiones en la intimidad se han multiplicado y han adoptado en esta nueva era múltiples modalidades. De hecho, el fenómeno o instituto jurídico de la protección de datos cuenta con una trayectoria relativamente reciente.

Entendida, en general, como "ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión" (RAE 1980, *s.v.* privacidad), este derecho básico se ve amenazado por la facilidad de acceso y circulación de los datos personales contenidos en las bases de datos y ficheros de la administración y de las empresas, en las redes sociales, e, incluso, en discos locales de uso pretendidamente personal. El tema es amplio y en él se ven implicadas entidades tan dispares como el individuo, el estado, el sistema educativo, la empresa, etc.

Para delimitar el tema, centrándome exclusivamente en la privacidad en internet, una vez constatado el auge imparable de las tecnologías de la información, trataré, en primer lugar, los aspectos técnicos -en particular los procesos invisibles para el usuario-, y jurídicos de la privacidad. En segundo lugar, abordaré, dada su actualidad, la privacidad en las redes sociales y en la blogosfera, entornos ambos de sumo riesgo para la intimidad. El tema de la privacidad en ese ámbito es de máxima relevancia, y así lo indica, por ejemplo, la naciente *Diaspora*, red social que significativamente utiliza el slogan "cuida tu privacidad", como su mayor reclamo frente a su gran competidor, *Facebook*[1].

1. El avance de la Sociedad de la Información

Es la Sociedad de la Infomación el contexto en que se plantea mayoritariamente el problema de la privacidad. La expansión de este nuevo paradigma social parece imparable al menos en el mundo desarrollado. Es significativo a este respecto el caso español: pese a la recesión económica, el año 2009 conoció un incremento importante en el número de internautas y en volumen de comercio electrónico:

> El volumen de negocio generado por el comercio electrónico B2C en 2009 se sitúa en 7.760 millones de euros, lo que supone un incremento del 15,9% respecto a 2008. Este incremento en el volumen de negocio está relacionado con el aumento del porcentaje de internautas (que pasa del 58,3% a 64% de la población de 15 años y más) y del porcentaje de aquellos internautas que realizan comercio electrónico / compras (pasando del 40,3% al 41,5%), dando lugar a un incremento en número absoluto de compradores on-line de 1.481.292 individuos (ONTSI 2010).

Esta expansión pone en manos de cualquier ciudadano o colectivo las herramientas necesarias para erosionar la intimidad individual, y todo ello se ve beneficiado por la tecnología y por los intereses que se mueven en torno a este nuevo modelo de organización social. Por una parte, las tecnologías propias de la sociedad de la información permiten trazar la biografía de cualquier usuario en todos sus detalles; y por otra, las empresas, cuya finalidad es el beneficio, están ávidas de información sobre los gustos y aspiraciones de sus potenciales clientes. Finalmente, los gobiernos, por motivos fiscales o de seguridad, tratan también de

[1] En https://joindiaspora.com se ofrece información suficiente sobre esta naciente plataforma de red social. Una lectura rápida de su página de inicio nos permite constatar el énfasis que esta iniciativa pone en la privacidad: "tus fotos, historias y bromas sean compartidas sólo con la gente que tu quieras... Tú mantienes la propiedad sobre todo lo que compartas en *Diaspora*... *Diaspora* hace que compartir sea transparente y fácil - y esto va por privacidad también..."

capturar todo ese volumen de datos. Garton Ash (2010) describe así el constante atropello al derecho a la intimidad que sufre el ciudadano en el entramado del ciberespacio:

> … existen imágenes detalladas de nuestras casas en Google Earth y Google Street View... Nuestros *smartphones* permiten localizarnos. Nuestra búsqueda en Google es la historia íntima de nuestra vida. Los bancos y las contructoras tienen acceso sin problemas a nuestro historial de crédito. Y los Gobiernos británico y estadounidense se han arrogado -en nombre de la "seguridad"- el poder de supervisar todo, incluidos nuestros correos electrónicos y nuestras llamadas de móvil.

En definitiva, cómo avanzar en el desarrollo y democratización de la Sociedad de la Información y, al mismo tiempo, respetar el inalienable derecho a la intimidad, es el reto al que se enfrenta la nueva sociedad del siglo XXI y, más en concreto, su medio de mayor actividad y que, en múltiples aspectos, contribuye a mejorar la calidad de vida, el ciberespacio[2].

2. Transgresión invisible

Una vez automatizados, los datos están listos para circular por la red y los riesgos que amenazan cualquier política de protección son prácticamente imprevisibles. No se trata tan solo de proteger enormes bancos de datos o sistemas de ficheros, sino y sobre todo el rastro que los datos dejan en la red. Determinadas informaciones que constituyen un atentado sobre la intimidad y la reputación del individuo permanecen en Internet sin posibilidad alguna de eliminarlas[3]. Recientemente, Gómez (2010: 24) planteaba el alcance del problema ofreciendo datos que ponen de manifiesto su creciente dimensión y el menoscabo que conlleva en la reputación de los afectados:

> Las solicitudes de tutela de derechos para cancelar datos de páginas *web* o impedir que sean difundidos por buscadores de Internet aumentaron el 200% … La mayoría afecta a recuperación por buscadores de datos en boletines oficiales o medios de cumunicación digitales sobre sanciones administrativas ya cumplidas, edictos de deudas vencidas o datos de víctimas de violencia doméstica.

Para reducir riesgos, en la medida de lo posible, es conveniente tener en cuenta los distintos mecanismos que violan la protección de datos y que actúan de forma invisible o inconsciente para el usuario, en concreto las *cookies* y el *spyware*.

Las *cookies* constituyen uno de los principales agentes de vulnerabilidad y tal vez el más eficaz. Definidas como "fragmento de información que se almacena en el disco duro del visitante de una página web a través de su navegador, a petición del servidor de la página. Esta información puede ser luego recuperada por el servidor en posteriores visitas" (Wikipedia, *s.v.* Cookies), son un mecanismo fundamental para identificar al usuario, conocer sus tendencias, y, de este modo, personalizar la comunicación que se le va a transmitir. Desde el punto de vista legal de la protección de datos constituyen un cauce ilegítimo, y así lo pone de manifiesto uno de los mejores tratadistas de la privacidad electrónica:

> La facilidad con la que dichos archivos logran grabarse en el ordenador visitante al margen del conocimiento del internauta, contrasta con su alto grado de lesividad, máxime cuando son habituales los tratamientos comerciales derivados de estos rastros electrónicos o de cliqueo, cuando no otras aplicaciones más espurias (Ballesteros Moffa 2005: 168).

---

[2] La amplísima bibliografía que se ofrece en uno de los mejores tratados jurídicos sobre el tema (Ballesteros Moffa (2006: 316-345)) nos da idea cabal del interés que este problema ha suscitado entre profesionales de ámbitos tan dispares como el derecho, el periodismo, la economía, la política o la informática.

[3] Dadas estas dificultades, han surgido empresas en línea que tienen como objetivo atender la petición de borrado de datos y rastro de sus clientes. Un ejemplo es http://salirdeinternet.com, que se define como el primer despacho en eliminar datos del buscador Google y de los Boletines Oficiales con el objetivo de recuperar el anonimato en Internet.

Pero no siempre esta tecnología tiene finalidad delictiva. En ocasiones se programan para ofrecer de forma más eficiente un mejor servicio al usuario. En este caso, el proveedor del servicio debería infomar al usuario cuándo esa cookie se va a almacenar y el periodo durante el que va a permanecer en el disco. Asimismo, debe comunicar de forma clara qué finalidad tiene, qué tipo de información va a recoger, y los derechos de cancelación que asisten al usuario (COM 2000: 385).

Junto a las *cookies* y con finalidad muy semejante existen otros medios de transgresión de la intimidad, tales como los mencionados programas espía (*spyware*), que se instalan en el disco duro, a menudo a través de un virus troyano, y recaban información sobre el usuario: correo electrónico, lista de contactos, datos sobre su conexión a internet, tarjeta de crédito, cuentas bancarias, etc. Estos datos son destinados en la mayoría de los casos a empresas de publicidad, aunque frecuentemente sirven también a fines delectivos.

Finalmente, dado el alto interés comercial de los datos, los sitios web que exigen el registro de usuario para ofrecer determinados servicios suelen gestionar la información introducida de forma nada transparente, al margen de lo que prescribe la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos (LOPD). En efecto, un estudio norteamericano constataba que “de los 1400 *websites* analizados un 85 por ciento recogía y almacenaba datos presonales de los visitantes, de los que solo un 14 por ciento atendían a la privacidad de la información recogida” (Ballesteros Moffa 2005: 168). Ante esta situación, se impone la intervención de los organismos públicos competentes que vigile el cumplimiento de leyes vigentes, como la mencionada LOPD. Con este motivo, a modo de incentivo, tal como nos recuerda Ballesteros Moffa (2005: 302), el Real Decreto 292/2004 crea un distintivo público de confianza cuya concesión exige por parte de las empresas el cumplimiento de una serie de requisitos encaminados a garantizar la seguridad y la protección de los usuarios.

3. Privacidad en las redes sociales

3.1. Falta de control sobre los datos

La privacidad es una de las cuestiones de mayor actualidad entre el público en general y, en particular, entre los profesionales de la información. En este sentido, Sola-Martínez (2009) resume el debate sobre la privacidad en las redes sociales que tuvo lugar en Iwetel, lista de distribución de bibliotecarios y documentalistas del ámbito español e iberoamericano. La discusión toma como referente *Facebook* y en menor medida ese otro fenómeno de la web 2, la bolgosfera y las wikis, es decir, iniciativas que, al amparo de estas tecnologías, tienen como finalidad compartir conocimiento y que se engloban en la tecnología que se ha dado en denominar *cloud computing*.

Los participantes en el debate son, en general, profesionales expertos en el mundo de la documentación y de la sociedad de la información, en contacto con los usuarios de a pie y con la responsabilidad de ofrecer soluciones no solo a los problemas técnicos o de selección de información, sino también a los problemas de privacidad. El punto de partida del debate fue el cambio en una cláusula de la licencia de uso de *Facebook* relativa a la privacidad y de la que se han hecho eco todos los medios de comunicación. Esa "inocente" modificación se resume así:

> Al parecer, *Facebook* ha cambiado una de sus cláusulas de contratación o licencia de uso. Antes, si un usuario se borraba de Facebook, con él se borraban todos sus datos, imágenes, vídeos, y demás, sin embargo, ahora se especifica que esa información ¡será 'eternamente' de Facebook! y que debemos fiarnos de su buena fe..." (Sola-Martínez 2009: 470).

La diferencia respecto a la situación anterior es que la baja de Facebook no conlleva la

eliminación de todos los materiales de ese usuario, sino que siguen estando disponibles. Es decir, no es posible la gestión absoluta de la privacidad por parte de los usuarios. Ante esta restricción de los derechos básicos, los profesionales implicados en el debate abogan por la formación. Del mismo modo que existe una formación para la circulación vial y para cualquier comportamiento social, parece lógico implantarla para el uso de la red. En efecto, el alcance social de los servicios que ofrece la red es lo suficientemente amplio como para advertir de sus peligros y riesgos desde las instituciones públicas e impulsar planes de formación.

Al problema descrito -permanencia de los datos y falta de control sobre ellos por parte del interesado- se une la extraña benevolencia con la que este medio cuenta por parte de sus usuarios, siempre dispuestos a volcar sus datos más personales. Lohr (2010) plantea, a este respecto, una pregunta muy inteligente: "If a stranger come up to you on the street, woud you give him your name, Social Security number and e-mail address?", y responde "Probabily not", con la mínima probabilidad de error.

3.2. Más allá del control del individuo

El problema no termina en la posesión por parte de una determinada entidad de esos tres o cuatro datos individuales que, aisladamente, parecen inofensivos, sino que, tal como sostienen algunos expertos informáticos, esos pocos bits recolectados de diversos sitios y redes, basándose en correlaciones estadísticas sofisticadas, premiten crear un retrato fidedigno de la identidad personal del usuario en concreto. El ejemplo que nos propone es el siguiente:

> In a class project at the Massachusetts Institute of Technology that received some attention las year, Carter Jernigan and Behram Mistree analyzedd more than 4,000 Facebook profiles of students, including links to friends who said the were gay. The pair was able to predict, with 78 percent accuracy, whether a profile belonged to a gay male. (Lohr 2010)

Es decir, aun en el mejor de los casos aplicando los controles que garantizan la privacidad de nuestros datos, no estamos a salvo de que nuestra información personal se difunda por la red. La privacidad a causa de las redes sociales ha dejado de ser una cuestión individual: "your online friends and colleagues may do it for you, referring to your school or employer, gender, location and interest" (Lohr 2010). Un estudio reciente llevado a cabo por las Universidades de Texas y Stanford revela que, examinando las correlaciones entre varias cuentas en línea es posible identificar a más del 30 por ciento de los usuarios de ambos servicios de Twitter -el servicio de microblogging y Flickr- aun prescindiendo del nombre de la cuenta y del correo electrónico (Lohr 2010).

Así pues, el control de acceso y los mecanismos básicos que el software ofrece para proteger la privacidad no son suficientes, ya que no se trata de un acceso controlado sino del conocimiento del contexto social en el que nuestra información va a circular. Boyd (2010) toma del mundo real un ejemplo ilustrativo. Sostiene, en primer lugar, que la privacidad no es lo opuesto a hablar en público:

> Sitting in a restaurant, we have intimate conversations knowing that the waitress may overhear. We count on what Erveng Goffman called "civil inattention": peopel will politely ignore us, and even if they listen they won't join in, because doing so violates social norms. Of course, if a close friend sits at the neighboring table, everything changes. Whether an enviorement is public or not is beside the point. It's the situation that matters.

El individuo debe aplicar su sentido común para gestionar correctamente su privacidad; debe ser consciente de la situación comunicativa, del interlocutor y del contexto en el que se desarrolla el acto de la comunicación. Y esta precaución que se presupone en el ámbito de la vida real debe trasladarse a sus relaciones en el ciberespacio y en concreto en las

redes sociales, teniendo en cuenta que en este medio los riesgos son mayores: "Before we can communicate appropriately in a social environment like Facebook or Twitter, we must develop a sence for what people share" (Boyd 2010).

Pero el problema de la privacidad ni tan siquiera se termina con la muerte del individuo, sino que a menudo puede sobrevirle, ya que la web es cada vez más un espacio vital donde se toman decisiones trascendentes y se realizan actividades primordiales. En este sentido, podemos hablar de "vidas en línea" y de la necesidad de regular su muerte. Esa "muerte en línea" debe ser gestionada de forma semejante a la herencia material y a las últimas voluntades. El problema ha reclamado ya la atención de algunos estados; así, por ejemplo, "Canadian government officials asked Facebook to outline in tis privacy police that families can ask to have the profiles of their deceased relative deleted" (Dow Jones & Company 2009).

4. Conclusión

Los mecanismos desarrollados al amparo de las nuevas tecnologías y de la Sociedad de la Información para atentar contra la privacidad en beneficio de distintos intereses, no siempre legítimos, adoptan formas cada vez más sofisticadas, dejando en total indefensión al usuario. Por otra parte, las redes sociales, que cuentan con millones de usuarios y están en constante crecimiento, no han hecho más, en lo que concierne a la privacidad, que agravar el problema.

Dada su complejidad, como usuarios tenemos la obligación de adoptar todas las medidas a nuestro alcance para proteger nuestra intimidad, siendo conscientes de que la vía jurídica rara vez resuelve la situación. Los propios juristas advierten de esa incapacidad y apelan a la autorregulación y a la implantación de buenas prácticas. Así pues, una buena iniciativa como usuarios sería la prestar mayor atención a las garantías institucionales, es decir, a los distintivos de confianza que los organismos competentes conceden a las empresas en virtud de su buen hacer este ámbito y el respeto a la privacidad.

Recurriendo a la autoprotección o a la ley, exigiendo fiabilidad y autorregulación a los sitios web en los que participamos, en ningún caso debemos resignarnos a que la transgresión de nuestra intimidad sea la regla general. Sus consecuencias pueden ser irreparables, como así lo demuestra, por mencionar un hecho extremo que debe hacernos reflexionar, el caso de Tyler Clementi, estudiante de 18 años de la Rutgers University, cuyos actos íntimos fueron grabados en secreto por un compañero y difundidos a través de una red social. Su reacción fue el suicidio, arrojándose desde el puento George Washington al río Hudson, y despidiéndose, a través de Facebook -¿acaso su verdugo?-, con un escueto mensaje: "Jumping off the gw bridge sorry".

Bibliografía

Ballesteros Moffa, L.A. (2005). *La privacidad electrónica. Internet en el centro de protección*. Valencia : Tirant lo Blanch; Madrid: Agencia Española de Protección de Datos.

Boyd, Danah (2010). "Why Privacy is not Dead". T*echnology Review*. [en línea]. http://www.technologyreview.com]. September/October. [fecha de consulta: 31 de diciembre de 2010]

COM 2000 = Parlamento Europeo. *Directiva relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas*.

Dow Jones & Company (9 de octubre de 2009). "Web Privacy for the Dead". *The Wall Street Journal*. [en línea]. http://blogs.wsj.com/digits/2009/10/09/web-privacy-the-dead]. [fecha de consulta: 23 de diciembre de 2010]

Garton Ash, Timothy (11 de octubre de 2010). "Facebook: restablecer la privacidad". *El País*. [en línea: http://www.elpais.com/articulo/opinion/Facebook/]. [fecha de consulta: 21 de diciembre de 2010]

Gómez, Rosario G. (7 de enero de 2011). "Quiero que Internet se olvide de mí". *El País*, págs. 24-25

Lohr, Steve (16 de marzo de 2010). "How Privacy Vanishes Online". *The New York Times*. [en línea: http://www.nytimes.com/2010/03/17/technology/]. [fecha de consulta: 16 de diciembre de 2010]

Observatorio Nacional de las Telecomunicaciones y de la SI (ONTSI) (2010). *Estudio de comercio electrónico B2C 2010.* [en línea: http://www.ontsi.red.es/hogares-ciudadanos/articles/id/4877/estudio-b2c-2010.html] [Fecha de consulta: 12 de diciembre de 2010]

Sola-Martínez, María José (2009). "Redes sociales: más allá de la privacidad". *El profesional de la información*. vol. 18, n. 4, julio-agosto, págs. 470-474.