

Privacidad en las redes sociales y derechos personales

Dos casos prácticos, las Políticas de Usuarios Facebook y Google

Comunicación presentada para el 8º CIEDI, Guadalajara, México

Autores:

Rodrigo Cetina Presuel
rodrigocetina@ccinf.ucm.es
Colaborador Honorario UCM
Becario en el extranjero CONACYT México.

Loreto Corredoira y Alfonso¹
loretoc@ccinf.ucm.es
Profesora Titular de la Universidad Complutense de Madrid
Directora del Observatorio TICs - Cyberlaw Clinic: cyberlaw.ucm.es

Palabras claves (5): Facebook, Google, habeas data, intimidad, privacidad, redes sociales,

Abstract:

La intimidad en los medios siempre ha sido un tema importante en el Derecho y en la Ética de la Información, tratado por autores y discutido en los tribunales. El Tribunal Constitucional español en 1984 afirmaba que “el reconocimiento explícito en un texto constitucional del derecho a la intimidad es muy reciente y se encuentra en muy pocas Constituciones, entre ellas la española. (...) La inviolabilidad del domicilio y de la correspondencia, que son algunas de esas libertades tradicionales, tienen como finalidad principal el respeto a un ámbito de vida privada, personal y familiar, que debe quedar excluido del conocimiento ajeno y de las intromisiones de los demás, salvo autorización del interesado” (STC 110/1984, de 26 de noviembre, FJ3º).

Antes de la eclosión de las redes sociales y los grandes buscadores como Google, las fotos o grabaciones de particulares publicadas sin consentimiento expreso y/o sin motivo informativo claro, eran las principales intromisiones ilegales denunciadas ante los tribunales, en algunos casos incluso, delito. En los 90 los móviles, las cámaras de fotos o vídeos o, el correo electrónico, abrieron otro flanco débil para la persona. Desde el 2001 con MySpace, comienza el desarrollo de las redes sociales como Tuenti -en España- o Facebook en todo el mundo y compañías como Google, o su servicio *Google maps* entre otros, -que utilizan datos personales e incluso la ubicación física de las personas mediante GPS-, es otra cosa.

Los recientes casos de Facebook y Google, demandados en varios países europeos, España entre otros, por violaciones a la privacidad, son una muestra clara de la necesidad de encontrar un equilibrio entre los intereses de las compañías que gestionan las redes sociales -que tantas aportaciones positivas tienen- y, los de sus clientes. Los usuarios querrían limitar la difusión de sus datos, aunque al mismo tiempo necesitan que las empresas que ofrecen el servicio obtengan dinero con ellos para que los servicios que ofrecen puedan seguir siendo gratuitos.

En este trabajo nos centraremos en dos sitios mundialmente conocidos, uno una red social, Facebook, y otro, Google, originalmente un buscador con aplicaciones de red social (Buzz, chat de Gmail, etc.) y muchas otras herramientas 2.0.

¹ Participa en el Proyecto I+D relacionado con este Congreso: “Las libertades informativas en el contexto de la web 2.0 y las redes sociales: redefinición, garantías y límites”, con referencia DER2009-14519-C05-01.

1) El habeas data. Desafíos de la “autodeterminación informática” en las redes sociales

La primera Ley española de Protección de Datos personales² tuvo seis recursos de inconstitucionalidad por diversos aspectos. Se trataba de la primera regulación de la “intimidad informática”, del conjunto de datos o informaciones recopilados acerca de una persona. Una materia compleja, inédita en el Derecho continental. Los bienes afectados eran y son, la intimidad personal o el derecho también acuñado de “autodeterminación informativa”, derecho del art. 18.4 de la Constitución española de 1978, que como la portuguesa de 1976, fue de las primeras en introducir esta garantía entre los derechos personales.

Como ha analizado DE LUCAS (1999: 36): “La previsión constitucional de la tutela de los derechos frente al uso de la informática se proyecta sobre los datos personales e implica, por un lado, derechos y garantías para los titulares de esos datos de carácter personal. Por el otro, supone para quienes los recogen, tratan, transmiten, ceden o conservan, una serie de obligaciones en lo que se refiere a la calidad y a la seguridad de la información de esa naturaleza que manejan y a las condiciones en que pueden utilizarla, almacenarla, facilitarla o cederla. Además, implica restricciones a la posibilidad de acceder a ella por parte de terceros, así como límites respecto de los datos personales que pueden ser tenidos en consideración y, posteriormente, incorporados a los ficheros automatizados”.

Los datos que se compilan en bases de anunciantes, de las autoridades públicas, de las universidades o ahora de las redes sociales, máquinas buscadoras o gestoras de correo electrónico, son susceptibles de elaborar un perfil personal de cada uno de nosotros. Junto con sus ventajas, ha destacado FERNÁNDEZ-ESTEBAN³, puede causarnos notorios daños.

El derecho al *habeas data*, estudiado también en tesis doctorales, como la de DEL CASTILLO en la Universidad Complutense⁴ tiene aspectos constitucionales y administrativos. Como se ha reconocido en diversos Tribunales, no sólo europeos, “el ámbito de acción o de operatividad del derecho al *habeas data* o derecho a la autodeterminación informática, está dado por el entorno en el cual se desarrollan los procesos de administración de bases de datos personales. De tal forma que integran el contexto material: el objeto o la actividad de las entidades administradoras de bases de datos, las regulaciones internas, los mecanismos técnicos para la recopilación, procesamiento, almacenamiento, seguridad y divulgación de los datos personales y la reglamentación sobre usuarios de los servicios de las administradoras de las bases de datos”⁵.

Citado el marco jurídico general que se aplica en Europa y España veamos cómo son las normas de autorregulación de Facebook y Google en el ámbito de la privacidad y de qué modo cumplen en concreto los preceptos de la Leyes vigentes.

Ambas empresas son estadounidenses, y sus políticas se basan en el Derecho anglosajón, utilizando el método comparativo se analizará lo dispuesto en la Ley norteamericana y en la europea, particularmente la española, señalando las diferencias tanto normativas como conceptuales entre ambos sistemas para después apuntar los vacíos legales y riesgos de

² Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal

³ FERNÁNDEZ-ESTEBAN, M^a Luisa, *Nuevas tecnologías, Internet y derechos fundamentales*, McGraw-Hill, Madrid, 1998, págs. 115 ss.

⁴ DEL CASTILLO, Isabel-Cecilia, El “habeas data”: aspectos constitucionales y administrativos : (“el derecho a saber y la obligación de callar”), Tesis manuscrita, Biblioteca Universidad Complutense, Tesis inédita de la Universidad Complutense de Madrid, Facultad de Derecho, Departamento de Derecho Constitucional, 2007.

⁵ Sentencia de Tutela nº 729/02 de Corte Constitucional, de 05 de Septiembre 2002, Colombia

indefensión para los usuarios españoles.

La Comisión Europea en su decisión del 26 de Julio de 2000⁶ con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo establece qué empresas estadounidenses están adheridas a los principios del “Puerto Seguro” (*safe harbor*), tras comprobar que cuentan con un nivel adecuado de protección. Facebook y Google se encuentran en esta lista como empresa que trata los datos en un ámbito online⁷ por lo cual de acuerdo con los artículos de Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (en adelante la LOPDP) y, su Reglamento de desarrollo contenido en el Real Decreto 1720/2007 de 21 de diciembre (en adelante el Reglamento LOPDP), es lícito realizar el movimiento internacional de los datos.

2) La Política de Privacidad de Facebook

Facebook, como cualquier sitio de Internet, y ahora, como todas las redes sociales que podemos encontrar, se rige con los internautas por unos términos de uso y una política de privacidad⁸.

Téngase en cuenta que por privacidad entiende el diccionario de la Real Academia Española de la Lengua *1. f. Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.*

Estas normas de autorregulación se aplican a la totalidad de la web www.facebook.com, pero no son aplicables a “entidades que no sean propiedad o no se encuentren bajo el control de Facebook, incluidos los sitios web y aplicaciones que utilicen la plataforma”. Esto es, aunque la política de privacidad regule cómo se tratarán nuestros datos dentro de Facebook, tendremos que contrastar la política de privacidad de cada uno de los sitios que interactúen con la red social y averiguar como serán tratados nuestros datos en cada caso.

Recordemos que la principal intención de la red social, tal y como ha declarado en repetidas ocasiones su creador, Mark Zuckerberg, es “compartir información”, en este caso, información personal. Cada uno es **dueño de su propia información** y “cada persona debería poder controlar el grado de privacidad que desea tener y hasta dónde quiere llegar sin que, en modo alguno, sean admisibles injerencias injustificadas”⁹.

Es aquí en donde se identifica el principal problema con esta red social, nuestra información personal es compartida dentro del sitio, bajo ciertas reglas, pero estas reglas permiten que nuestros datos sean compartidos en otros sitios, haciendo en la práctica que un verdadero control sobre nuestros datos sea casi imposible, lo que pone en peligro nuestra privacidad e intimidad.

Recordemos que el Tribunal Constitucional en su Sentencia 292/2000 definió el derecho a la protección de datos como “el derecho fundamental que garantiza a toda persona un poder de control sobre sus datos personales, sobre su **uso y destino**, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado”. La política de privacidad de Facebook, como analizaremos paso a paso a continuación, no permite efectivamente el control sobre este uso y destino de los datos personales. Es un buen comienzo, pero la misma estructura de la red social,

⁶ Disponible en: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/B.12-cp--Decisi-oo-n--sobre-la-adeacuaci-oo-n-conferida-por-los-principios-de-puerto-seguro.pdf

⁷ Dicha lista puede ser consultada en la siguiente dirección URL: <https://www.export.gov/safehrbr/list.aspx>

⁸ Disponibles en: <http://www.facebook.com/terms.php?ref=pf> y en <http://www.facebook.com/privacy/explanation.php#!/policy.php>

⁹ PIÑAR MAÑAS, José Luis: ¿Existe la privacidad? Inauguración del curso académico 2008/2009, Madrid, Publicaciones Fundación Universitaria San Pablo CEU.

y los malos hábitos de los usuarios en su uso cotidiano, hacen insuficiente la protección que puede procurar la política de privacidad.

Es necesario entonces, educar al usuario en un uso responsable y consciente al participar en una red social y analizar con detalle la política de privacidad, contrastándola con la LOPDP y su Reglamento, para señalar sus puntos flacos y proponer los cambios necesarios.

2.1. Datos que Facebook solicita a sus usuarios

Facebook, como la práctica totalidad de los sitios de Internet para usuarios registrados pide una serie de datos a quien pretende abrir una cuenta en el sitio. Los datos básicos que esta red social solicita son: el nombre completo, señalando en sus términos de usuario que éste y todos los datos deben de ser verdaderos; la edad, para comprobar la edad mínima del usuario, que es de 13 años a nivel internacional y de 14 en España; una dirección de correo electrónico y, el sexo. Los datos son públicos, salvo estos dos últimos que podrán ser ocultados por el usuario. Además, la red social también nos alentará a subir una fotografía que se asociará con nuestro perfil

Estos datos –de acuerdo con el artículo 3 de la LOPDP- son datos de carácter personal, pues se trata de información concerniente a personas físicas identificadas o identificables y, en su conjunto, constituyen un fichero cuyo responsable es la empresa *Facebook, Inc.*

Facebook también avisa a los usuarios que al aceptar la política de privacidad, lo cual se considera hecho con el simple hecho de registrarse o acceder al sitio, se otorga el consentimiento para la recopilación y procesamiento de los datos en Estados Unidos. Esta transferencia está regulada por los artículos 33 y 34 de la LOPDP y en el Título VI del Reglamento LOPDP y al igual que ocurre en Google, especialmente en Gmail, tiene enorme trascendencia pues es el usuario quien hace esa transferencia de sus contactos.

Según el apartado 3 de la Política de Privacidad de Facebook, tanto nuestro nombre como fotografía de perfil, que como ya dijimos están asociados, carecen de una configuración de privacidad por lo cual cualquier persona podrá verlas, incluso a través de motores de búsqueda de terceros, como Google o Yahoo, opción que viene activada por defecto, salvo que optemos por impedir la indexación en estos buscadores. Esto permite que terceros distintos, ajenos a nuestros “amigos” o contactos relacionados e incluso a la red social puedan tener acceso a nuestro perfil e incluso identificarnos con facilidad. Esta situación es especialmente delicada en cuanto a los menores cuya intimidad y datos merecen especial protección.

Una vez creada la cuenta, que se hace sencillamente desde su página principal, nos pedirá nuestro acceso a los contactos de nuestra cuenta de correo electrónico para sugerirnos amigos de Facebook, avisándonos que la contraseña no será guardada. Sin embargo informa de que, por defecto, almacenará la información de nuestros contactos para un uso específico salvo que optemos por lo contrario. Esta información de contactos puede ser después eliminada en cualquier momento, si así lo elige el usuario, aunque no es fácil dar con estos controles.

Acto seguido, Facebook nos invita a proporcionarle información más detallada sobre nosotros, como, por ejemplo, la Universidad en la que estudiamos o nuestro sitio de trabajo. Además Facebook, a discreción del usuario, solicita datos más personales como nuestro lugar de nacimiento o ubicación actual y datos como la ideología política, la orientación religiosa e incluso, de manera implícita, la orientación sexual.

Aunque estos datos son opcionales, si el usuario decide proporcionarlos, se debe de recordar que la red social configura por defecto el mayor grado de visibilidad del perfil de usuario, es decir,

que si el usuario no decide ocultar esta información después de introducida, dichos datos podrían obtenerse haciendo una simple búsqueda dentro de Facebook o incluso podrían llegar a ser encontrados a través de un buscador convencional.

Esto es especialmente grave puesto que se trata de datos especialmente protegidos pues se encuentran dentro de la esfera del derecho fundamental recogido en el apartado 2 del artículo 16 de la Constitución Española que declara que “nadie podrá ser obligado a declarar sobre su ideología, religión o creencias”.

En el apartado 2 artículo 7 de la LOPDP se dice que datos especialmente protegidos como la ideología, afiliación sindical, religión y creencias sólo pueden ser tratados mediante el consentimiento expreso y por escrito del interesado.

Facebook es ciertamente transgresora porque no sólo pregunta al usuario por su sexo sino que, en otro apartado interroga sobre *si le gustan* los hombres o las mujeres y si busca entre otras cosas una *relación*. En el art. 7.3 se dice que los datos relativos a la vida sexual o bien también a la salud y al origen racial sólo pueden ser recabados, tratados y cedidos cuando por razones de interés general así lo disponga una ley o el afectado lo consienta expresamente. En Europa esa autorización expresa debe ser por escrito (en una consulta médica, en una encuesta, etc) no se puede omitir esto.

Sobre tan delicados datos como la orientación religiosa, política o sexual, Facebook sólo hace una tibia referencia en el apartado 3 de su política de privacidad y recomienda que estos datos únicamente se hagan visibles **a amigos de amigos**. Recordemos que por defecto la información personal estará disponible **para todos** en la red.

Estas Políticas son tan endebles con respecto a información sensible que aumentan el riesgo de agresiones a la privacidad, intimidad y honor de los usuarios.

Es necesario que quienes diseñan los términos de usuario de esta red social tomen medidas para o bien que estos datos dejen de ser requeridos, puesto que su relevancia es cuestionable o bien, instauren las medidas tecnológicas para que datos tan delicados estén siempre ocultos por defecto.

Las forma de decidir sobre la política de privacidad por los dirigentes de la red social “genera, a veces, arbitrariedades en la forma de imponer sus criterios particulares con una objetividad discutible para el resto de los usuarios, que, al fin y al cabo... son los que proveen los contenidos¹⁰”.

El usuario debe ser consciente de qué datos suyos son verdaderamente esenciales para la red social, o cuáles lo son para la finalidad comercial que permite a Facebook prestar servicios gratuitos al usuario. Identificados estos datos, y en colaboración con las autoridades responsables de la protección de datos de carácter personal, consideramos que se debe presionar a los responsables del servicio a que solo exijan los datos mínimos, dotándolos además de máxima protección.

2.1. Información que Facebook recaba sobre sus usuarios

¹⁰ JIMÉNEZ LÓPEZ, David. “La Protección de datos de carácter personal en el ámbito de las redes sociales electrónicas: el valor de la autorregulación”. En *Anuario Facultad de Derecho*, Universidad de Alcalá, II, 2009. Páginas 237-274.

Además de la información personal que compone nuestro perfil de Facebook, la red social nos avisa de que recaba otros tipos de datos sobre nosotros por el uso cotidiano que se hace de su servicio. Un ejemplo de esto es cuando el usuario sube al servicio un vídeo o un álbum de fotos, una de las funciones más populares de la plataforma. Esta información que Facebook llama *contenido* ofrece también opciones de privacidad, pero de nuevo, por defecto es de lo más accesible posible incluso para terceros.

Facebook informa a sus usuarios que recoge información sobre el tipo de navegador, ubicación y dirección IP del usuario, todo esto con fines de prospección comercial, lo que el usuario autoriza al adherirse a los términos de usuario y política de privacidad de la red social en el momento que decide activar su cuenta de usuario.

La red social recopila además datos del usuario mediante la interacción con otros usuarios, obteniendo así datos adicionales sobre nosotros que son revelados por nuestros contactos. Además se avisa al usuario de la utilización de *cookies* para recabar este tipo de información y da, mediante las medidas técnicas de seguridad de su navegador, la opción de bloquearlas. Con todo ello, es fácil concluir que se configura una auténtica identidad on line, a la que tenemos derecho.

La LOPDP hace referencia a este tipo de datos en el artículo 3, c) cuando define al tratamiento de datos “como las operaciones y procedimientos técnicos de carácter automatizado... que permitan la recogida, grabación, conservación, elaboración, modificación... así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”.

2.3. Acerca de cómo utiliza Facebook la información de los usuarios

La política de privacidad establece en su apartado 1 que se entiende aceptada por el usuario por el simple hecho de acceder o utilizar el servicio. Es decir, se consiente el tratamiento y comunicación de datos en las formas que la misma política define, lo cual haría referencia al artículo 45.1 b) del Reglamento *LOPDP* que establece que con finalidades comerciales se podrán usar datos “facilitados por los propios interesados u obtenidos con su consentimiento”.

El artículo 6 de la *LOPDP* establece que es necesario el “consentimiento inequívoco” del interesado para el tratamiento de sus datos. El que por el simple uso de la red social se entienda que el usuario ha aceptado y comprendido exactamente como se tratarán sus datos personales se antoja improbable. Si tenemos en cuenta que la mayoría de los usuarios no lee ni siquiera la política de privacidad antes de utilizar el servicio, es bastante discutible que se pueda hablar de un “consentimiento inequívoco” para el tratamiento de los datos.

El mencionado artículo impone la obligación para quien trata los datos de que los utilice sólo para “finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial”. Facebook establece ocho formas de utilización de la información privada de sus usuarios. Cuatro de ellas son relacionadas con el perfil del usuario y su conexión con otros usuarios, es decir se refieren a la gestión del sistema e incluyen el contacto directo a través del correo electrónico con el usuario, el complementar el perfil con datos obtenidos de otros, sugerir contactos o permitir a otros usuarios el usar datos personales que posean de uno para poder encontrarle. Esto puede incluir el correo electrónico, y como ya dijimos si este dato personal está disponible en una configuración demasiado abierta puede revelar nuestra dirección incluso en motores de búsqueda y exponernos a correos no deseados y al *spam*.

Tres formas de tratamiento de datos están relacionadas con los fines publicitarios. Cuando

Facebook comparte la información personal con anunciantes, los datos si son transmitidos de manera disociada no requieren el consentimiento previo del usuario.

Y, finalmente, la octava es para contactar directamente al usuario a través del correo electrónico y darle a conocer otros servicios ofrecidos por la misma plataforma.

Sin embargo, creemos que existe un cierto peligro de permitir una “asociación no consentida” por parte de los usuarios en lo que Facebook llama “anuncios sociales”, definida en el apartado 5 de la política de privacidad y que consiste en emparejar “los anuncios que ofrecemos con información pertinente que poseemos sobre ti y sobre tus amigos para que los anuncios resulten más interesantes y se adapten mejor a ti y a tus amigos”. Esto quiere decir que junto a una página publicitaria de por ejemplo, una marca de refresco, podría aparecer la foto del perfil de un usuario para que también lo vean sus contactos.

2.4. De cómo comparte Facebook con terceros la información privada

La política de Privacidad de Facebook establece los supuestos en que se efectúan cesiones de datos con terceros, que de acuerdo con el artículo 10.1 del Reglamento LOPDP sólo podrá hacerse con consentimiento del interesado. En línea con lo dispuesto con el artículo 12.2 del mismo Real Decreto español, Facebook debe informar al usuario de manera inequívoca la finalidad a la que se destinarán los datos pues de lo contrario este consentimiento sería nulo. Para esto, se enumeran una serie de supuestos en los que los datos son comunicados a terceros.

Un primer rubro hace referencia a compartir datos como el nombre o la foto de perfil con posibles contactos o amigos para que éstos puedan ponerse en contacto con el usuario y también cuando éste invita a alguien a unirse a Facebook. Todo esto está enmarcado en las funciones normales que implican la prestación del servicio. Recordemos que si el usuario tiene su perfil en la configuración de visibilidad máxima estos datos aparecerán en los resultados de búsqueda tanto de Facebook como de otros motores de búsqueda externos.

Otros supuestos son en relación con la cesión de información a comerciantes así como la prestación y publicidad de servicios. La cesión a terceros queda a la entera discreción del usuario y no se hará sin su consentimiento. Los datos pueden ser usados para anunciar la misma plataforma de Facebook a terceros pero sin la identificación específica de ningún usuario.

En lo que sí es transparente Facebook es en que pone a disposición del usuario y de sus potenciales clientes una página explicativa de cómo ve el anunciante la información de los usuarios.¹¹

Cuando Facebook presta un servicio junto con otra empresa, se compromete a identificarla y a ofrecer al usuario su respectiva Política de privacidad para que el usuario lo autorice o, garantizando así el cumplimiento de lo dispuesto en los artículos 10 y 12 del Reglamento antes mencionados.

Los datos también son cedidos a gente que presta *servicios necesarios* para Facebook, como por ejemplo el alojamiento del sitio web en servidores, caso en el que se designa un encargado del tratamiento, lo cual se ajusta con lo dispuesto en el capítulo III del Reglamento LOPDP. De acuerdo con la Ley y Directiva Europea¹² esto no puede ser considerado como una comunicación

¹¹ Que puede visitarse aquí: <http://www.facebook.com/advertising/>

¹² DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

de datos.

También se hace referencia al supuesto especial del artículo 19 del Reglamento LOPDP sobre la transferencia de datos debido a unas operaciones societarias de venta o cambio de control de la empresa en cuyo caso la ley establece que no existe cesión de datos. Facebook hace mención a que la información personal seguirá estando sujeta a la política de privacidad en vigor.

Por último se establece que los datos pueden ser cedidos para responder a requerimientos legales y evitar daños, fraudes o actividades ilegales de acuerdo con el artículo 11.d de la Reglamento LOPDP que no exige el consentimiento del usuario para los datos a las autoridades judiciales en el ejercicio de sus funciones, principalmente autoridades jurisdiccionales de los Estados Unidos, supeditándolo a que las otras jurisdicciones se acojan a la buena fe y a los “estándares internacionales generalmente aceptados”.

Cuando los administradores de Facebook consideran que un usuario puede incurrir en alguna actividad ilegal como el fraude, pueda cumplir amenazas, pudiendo causar un daño físico inminente o se juzgue que alguna actividad infringe los términos de usuario, la plataforma se reserva el derecho de compartir la información personal con otras empresas, abogados, tribunales u otras entidades gubernamentales. En este caso, y dado que la administración principal del servicio se encuentra en EEUU tal procedimiento seguirá la legislación de ese país y no necesariamente el de residencia del afectado.

4. La Política de Privacidad de Google

En términos generales Google tiene una política algo más simple que la de Facebook, aunque la complejidad de este “conglomerado” de Internet que asocia buscador, aplicaciones, Gmail, biblioteca on line, etc genera más riesgos o dificultades en el control de la información personal.

Google ha publicado y revisado en varias ocasiones su Política, debido a diversas denuncias por aplicaciones que afectan a la intimidad, imagen o privacidad como *Street View*¹³ o *Google Maps*, ante la difusión de fotos de las casas, de las matrículas de los coches, o del interior de una propiedad. También son numerosísimas las quejas de usuarios sobre los resultados del buscador, así como siguen en pie varias investigaciones oficiales de organismos como la Unión Europea, las Agencias de Protección de Datos europeas, entre ellas la española y la UK Information Commissioner (ICO) con centenares de denuncias de sus ciudadanos acerca de las fotos del o, el propio Gobierno norteamericano.

El Parlamento Europeo está estudiando la cuestión de la “retención de datos” y ha promovido una posición común de los países miembros de la Unión¹⁴.

Su política es simple, y se fundamenta en estos cinco principios (ver cuadro 1), en nuestra opinión demasiado genéricos y bienintencionados. Los detalles sobre qué hace con los datos, cómo se ven desde fuera por otros o cómo eliminarlos no están todos en castellano, por lo que debemos contrastar algunos matices en el “Privacy Center” disponible on line.

¹³ Con resultados diversos: Street View salió indemne del *U.S. District Court for Western Pennsylvania* en el caso de dos ciudadanos Aaron and Christine Boring v. Google Inc, 2008; en Alemania y en el Reino Unido, se presenta algo más difícil para Google. Ver casos en Findlaw: <http://writ.news.findlaw.com/ramasastry/>

¹⁴ Más información: Report to EU Forum on Data Retention en el URL: [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-61845](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-61845)

Principios de privacidad (Cuadro 1)

En Google buscamos ideas y productos que superen los límites de la tecnología existente. Como empresa que actúa de forma responsable, Google trabaja para garantizar que cualquier innovación se realice garantizando a los usuarios un nivel adecuado de seguridad y de privacidad. Nuestros Principios de privacidad nos ayudan en la toma de decisiones en todos los niveles empresariales, lo que nos permite proteger a los usuarios y ofrecerles lo que necesitan a la vez que desarrollamos nuestra continua [labor](#) de organización de la información mundial.

1. **Uso de información para ofrecer a los usuarios productos y servicios valiosos**
2. **Desarrollo de productos que reflejen prácticas y estándares de publicidad firmes**
3. **Recopilación de información personal de forma transparente**
4. **Oferta de alternativas significativas a los usuarios para proteger su privacidad**
5. **Supervisión responsable de la información almacenada**

4.1. Qué datos solicita al usuario registrado

El uso simple de Google como buscador no requiere mayor identificación personal. El buscador sí instala “cookies” que rastrean nuestra navegación a partir de la IP del ordenador o computer que usemos –sea propio o ajeno–.

La compañía declara “Por qué almacenamos datos personales” aunque ciertamente no dice cuáles: para mejorar y facilitar la navegación y la búsqueda o, para evitar el *phishing*, *scripting attacks*, el *spam* en todas sus formas. Por ejemplo, explica de modo educativo si uno escribe una búsqueda un término de modo incorrecto, Google nos sugiere: **Quizás quiso decir:** [guadalajara méxico](#)

Si damos “clic” en el primer resultado, los ingenieros de Google entienden que estaba bien sugerida la lista de enlaces, y eso sumado a cientos de clic de usuarios similares, le da más credibilidad al buscador. Sin duda hay algunas razones más: su utilización publicitaria en los anuncios contextuales algo omnipresente en Gmail, en Google Libros, etc.

4.2. Cómo utiliza Google los datos que compila y cómo la comparte con terceros

A los usuarios que quieren registrarse -lo que requiere una cuenta Gmail para utilizar de modo personal iGoogle, Google Analytics, Google Docs o cualquier otro servicio-, Google les pide datos personales (nombre, dirección de correo electrónico y contraseña de la cuenta). Para determinados servicios, como nuestros programas publicitarios, solicita también información sobre la tarjeta de crédito u otra información bancaria, que –afirma- “guarda en formato encriptado en nuestros servidores seguros”.

Google se compromete a que si va a “combinar” datos de una cuenta con la información procedente de otros servicios de Google o de terceros preguntar “si desea o no que realicemos dicha combinación de datos”.

Esta autorización expresa se cumple –aunque el usuario debe estar muy atento a la pregunta on

line- que es paso previo a utilizar algún recurso; por ejemplo, abrir un documento adjunto, como se muestra en el Cuadro 2.

En los litigios abiertos en el Reino Unido ésta es una cuestión clave, y de difícil solución, pues la *UK Data Protection Act (DPA)* requiere que el consentimiento de los usuarios sea previo a la recolección de los datos, algo complejo en Street View o Google Maps.

Además Google avisa al usuario de que *“puede optar por utilizar funciones adicionales de Gmail como, por ejemplo, el chat, que se conecta a la red de Google Talk, o Google Buzz. El servicio Google Talk cuenta con su propio aviso de privacidad, al igual que Google Buzz, cuyo aviso puede consultarse en esta página”*. Esto nos merece una opinión negativa porque multiplica la información, la dispersa generando inseguridad.



CUADRO 2

5. Derechos de acceso, rectificación, cancelación y oposición en Facebook y Google

La legislación europea citada –que se aplica en cada país miembro de la Unión mediante la incorporación de la correspondiente Directiva, en este caso la DIRECTIVA 95/46/CE citada– obliga a los Estados a desarrollar los derechos de acceso, rectificación, cancelación y oposición, temas básicos en el ejercicio del nominado derecho de autodeterminación informática aludido al principio.

En España, en particular es el Reglamento LOPDP que hemos venido analizando el que establece en el artículo 24.2 que “deberá concederse al interesado un medio sencillo y gratuito” para el ejercicio de estos derechos.

De acuerdo con lo establecido la posibilidad del ejercicio de estos derechos dada en el artículo 24.4¹⁵, Facebook ha fijado un servicio valiéndose de una herramienta tecnológica dentro de su

¹⁵ Artículo 24.4: “Cuando el responsable del fichero o tratamiento disponga de servicios de cualquier índole para la

misma plataforma que permite el ejercicio de estos derechos; también Google remite a una web para eliminar enlaces, aunque el seguimiento de su eficacia que hemos experimentado en nuestra investigación es baja.

Con respecto al derecho de acceso: Facebook informa al usuario de la forma en que sus datos están siendo tratados, tema que ya hemos tratado anteriormente y, Google ofrece al *“usuario cambiar la configuración de la cuenta de Gmail en la sección “Configuración” de Gmail. Puede organizar o suprimir los mensajes a través de la cuenta de Gmail o cancelar esta última en la sección “Cuenta de Google” de la configuración de Gmail. Dichas supresiones o cancelaciones tendrán efecto inmediato en la vista de la cuenta. Aunque, “las copias residuales de mensajes y cuentas suprimidos pueden tardar hasta 60 días en eliminarse de nuestros servidores activos y podrían permanecer en nuestros sistemas de copia de seguridad sin conexión.*

Los derechos de rectificación y cancelación pueden ejercerse también de forma on line, por lo que no constaría fehacientemente una solicitud como ésta, lo que es importante si se desea ir a los tribunales o a una autoridad administrativa.

En Facebook mediante la herramienta de edición de perfil la rectificación se puede hacer accediendo en cualquier momento, modificando los datos que son actualizados en tiempo real. También se puede eliminar algún aspecto concreto de la base de datos procediendo al borrado de éste en el campo correspondiente.

En Google cabe rectificar y anular una cuenta personal en Gmail, aunque los datos se conservan durante 60 días. Los principales problemas vienen por la falta de registro de datos recopilados en servicios de “escaneado” de calles, edificios o tierras que lleva a término en los servicios de “geolocalización”.

La Agencia de Protección de Datos española ¹⁶ha solicitado en julio de 2010 a Google España copia de los discos duros donde almacena las fotografías y panorámicas de Street View. Con eso los ciudadanos pueden también dirigirse a la APD y cancelar la información personal ante la respuesta no satisfactoria de Google. Además de que pueda haber sanciones, lo que interesa ahora para los residentes y usuarios de España es que los datos se conservarán en el Registro de la Agencia, ante el que se puede ejercitar “el derecho de consulta, regulado en el artículo 14 de la LOPD habilita a cualquier persona para conocer, de forma pública y gratuita, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del fichero”.

La compañía Google *“se adhiere a los principios de privacidad de garantía de seguridad estadounidenses. Para obtener más información sobre el marco de las disposiciones de seguridad o nuestro registro, visite el sitio web del Departamento de Comercio”.*

Tal web nos remite al acuerdo citado sobre “Puerto Seguro” el Ministerio de Comercio o Department of Commerce del Gobierno USA¹⁷ dice en su introducción que: *“The European Commission’s Directive on Data Protection went into effect in October of 1998, and would prohibit the transfer of personal data to non-European Union nations that do not meet the European “adequacy” standard for privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different ap-*

atención a su público o el ejercicio reclamaciones... podrá concederse la posibilidad al afectado de ejercer sus derechos de acceso, rectificación, cancelación y oposición a través de dichos servicios”.

¹⁶ URL y formularios de denuncia o reclamación en <https://www.agpd.es>

¹⁷ URL: <http://www.export.gov/safeharbor/>

proach to privacy from that taken by the European Union". Esta declaración reconoce la diversidad legislativa entre Europa y EEUU, aunque -por su propio interés- Google y otras empresas estadounidenses han implementado normas básicas sobre la transferencia de ficheros a países no-comunitarios.

En sucesivos trabajos similares a éstos abordaremos qué ocurre con la cancelación de datos y con la definitiva eliminación de sus copias caché o "rastros" en la web. Sin duda se trata de otro problema propio de estas redes o servicios 2.0.

¿Cabe volver o recuperar los datos?

Google sí permite la *vuelta a casa* de un usuario que cancela su cuenta, aunque para ello ha debido ordenar una copia de seguridad. Se ofrece al usuario la opción de desactivar la cuenta haciéndola invisible para cualquier usuario sin que los datos sean eliminados, pudiendo este, si así lo desea, reactivar su cuenta en cualquier momento con los mismos datos que se conservan a menos que el usuario solicite la eliminación definitiva de la cuenta.

En Facebook da en un período de 14 días de acuerdo a lo establecido en los términos de usuario de Facebook, añadiéndose un período máximo de 90 días en que la información permanecerá en copias de seguridad pero sin que esta esté disponible a terceros.

La misma Política de privacidad de Facebook hace referencia a que aunque la información se elimine, sus copias pueden permanecer visibles en otros lugares, por ejemplo en otros perfiles con los que se ha compartido.

Facebook se compromete a que dicha información, siempre y cuando esté dentro de su plataforma, no podrá ser asociada con el usuario que se dio de baja, sustituyendo el nombre de su perfil por el de un "usuario anónimo".

Sin embargo, el verdadero problema, es que el derecho de cancelación no queda garantizado en los supuestos en que algún otro usuario haya copiado o almacenado nuestra información y la ha distribuido posteriormente por la red o bien cuando la configuración de privacidad está en el nivel que permite el máximo acceso, pues aunque Facebook eliminará la información en su plataforma, no podrá hacer nada por los datos que se han distribuido en buscadores y sitios externos que cuentan con su propia política de privacidad.

En Google como hemos dicho *"las copias residuales de mensajes y cuentas suprimidos pueden tardar hasta 60 días en eliminarse de nuestros servidores activos y podrían permanecer en nuestros sistemas de copia de seguridad sin conexión.*

En la práctica, si la información personal ya ha sido expandida en buscadores como Google, y se han hecho copias "caché" será muy difícil que esa información sea efectivamente cancelada, pero eso no imposibilita el pleno ejercicio del derecho de cancelación, incluso el de rectificación, aunque requiere dirigirse a varias instancias en diversos países:

- Al del que edita la web para que lo elimine
- al que la enlaza
- al que hace seguimiento de fuentes RSS
- al que almacena internamente los resultados de sus búsquedas

5. Conclusiones

Los riesgos siguen en paralelo a las grandes ventajas de las redes sociales. Un usuario debe elegir estar o no en ese tipo de “conversaciones públicas”, lo que dependerá de sus intereses personales o profesionales.

Consideramos que, a veces, la información que se solicita del usuario para acceder a una red social puede resultar desproporcionada, como es el caso de Facebook; en otros servicios como Google o Gmail, y sus aplicaciones como Buzz o Picasa, lo que resulta insólito es el conjunto de cosas que éstas hacen por uno mismo, suplantándole la voluntad.

En Facebook es peligroso el tratamiento que se hace de datos de especial protección como las orientaciones religiosas, políticas o incluso sexuales. Aunque no es intención de la red social revelar estos datos, la complicada mecánica de este tipo de plataformas, y de Internet en general, agrede la intimidad y vida privada.

Hemos identificado problemas y deficiencias en la Política de Privacidad de Facebook pues a veces esta es confusa. Ciertas aplicaciones, como el referido caso de los “anuncios sociales” pueden terminar por vulnerar la privacidad del usuario aunque esta no sea la intención.

De Google destacaríamos como punto débil la complejidad de las aplicaciones que están totalmente enlazadas con el registro de usuario, y la escasez de medios on line para hacer efectivos los derechos de rectificación y cancelación.

Los derechos de acceso, rectificación y cancelación de datos personales no siempre están plenamente garantizados. No porque las políticas de privacidad analizadas sean malintencionadas o estén mal redactadas, si no porque a veces la misma naturaleza de las redes sociales complica su efectiva tutela a posteriori, ante ataques informáticos del llamado malware, etc. La reacción de Google ante los procedimientos administrativos o judiciales es correcta, pero eso pone la garantía de los derechos en el nivel del litigio, lo que es inadecuado.

Ciertas actitudes del usuario, como el no informarse adecuadamente, pueden contribuir a este resultado. Es importante que el usuario aprenda el uso responsable de las redes sociales. Se deben conocer las implicaciones en la privacidad, la intimidad y la protección de datos personales que conlleva una red social. Es necesario conocer cómo es el tratamiento de sus datos y lo que esto implica en cuanto a la protección de su privacidad.

Es necesario encontrar un equilibrio entre los intereses de las compañías que ofrecen plataformas de redes sociales y los de sus clientes; es decir, entre la información requerida, para que ésta no atente contra la intimidad y el honor de las personas y la utilizada por las redes sociales para la consecución de sus fines comerciales, siempre implementando las políticas y medios técnicos más correctos posibles.

Es responsabilidad del ciudadano hacer un uso inteligente y con cabeza de las redes sociales que por otro lado le aportan evidentes beneficios. Que un servicio sea gratuito no hace que nos exima de ser cautelosos en la cesión de datos, en la aceptación por un simple “clic” de condiciones que tienen consecuencias en nuestras familias, en la empresa o en otras organizaciones.

Es parte de tal responsabilidad de los ciudadanos, junto con las autoridades de protección de datos personales y organizaciones civiles, ejercer presión y exigir que las redes sociales depuren sus políticas y técnicas de protección de la información.

Esto sólo se puede lograr si las mismas redes sociales son las que mantienen abierto el canal de

diálogo y escuchan las inquietudes de los usuarios y organizaciones, buscando el balance entre el ejercicio de su actividad con fines de lucro y la adecuada protección de los datos personales y los derechos fundamentales al honor, la intimidad y la propia imagen. La red web 2.0 es una red de escucha, interactividad y acción, por parte de todos.

Bibliografía:

FERNÁNDEZ-ESTEBAN, M^a Luisa, *Nuevas tecnologías, Internet y derechos fundamentales*, McGraw-Hill, Madrid, 1998, Páginas 115 ss.

C BARRIOUSO RUIZ, “La Protección de datos de carácter personal en el ámbito de las redes sociales electrónicas. el valor de la autorregulación”, en *Anuario de la Facultad de Derecho*, Universidad de Alcalá II, Madrid, 2009.

I.C. DEL CASTILLO: El "habeas data": aspectos constitucionales y administrativos: ("el derecho a saber y la obligación de callar"), Tesis manuscrita, Biblioteca Universidad Complutense, Tesis inédita de la Universidad Complutense de Madrid, Facultad de Derecho, Departamento de Derecho Constitucional, 2007.

D. JIMÉNEZ LÓPEZ, David. “La Protección de datos de carácter personal en el ámbito de las redes sociales electrónicas: el valor de la autorregulación”. En *Anuario Facultad de Derecho*, Universidad de Alcalá, II, 2009. Páginas 237-274.

P. LUCAS MURILLO DE LA CUEVA: *El derecho a la autodeterminación informativa*, Tecnos, Madrid, 1990.

P. LUCAS MURILLO DE LA CUEVA: "LA CONSTRUCCIÓN DEL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA" en *Revista de Estudios Políticos (Nueva Época)*, Núm. 104. Abril-Junio 1999, pp. 35 a 60.

J. PIÑAR MAÑAS, *¿Existe la privacidad? Inauguración del curso académico 2008/2009*, Publicaciones de la Fundación Universitaria San Pablo CEU, Madrid, 2009 cita indirecta de: D. JIMENEZ LÓPEZ, «La Protección de datos de carácter personal en el ámbito de las redes sociales electrónicas. el valor de la autorregulación » en *Anuario de la Facultad de Derecho*, Universidad de Alcalá II, Madrid, 2009

Legislación:

Constitución Española de 1978, art. 18

DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos

Ley Orgánica 15/1999 de 13 de diciembre de Protección de datos de carácter personal

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

Jurisprudencia y textos legales:

Sentencia del Tribunal Constitucional 110/1984 de 26 de noviembre.

Sentencia del Tribunal Constitucional 292/2000 del 30 de noviembre

Sentencia de Tutela nº 729/02 de Corte Constitucional, de 05 de Septiembre 2002, Colombia

Decisiones de la Comisión Europea:

Decisión de la Comisión de 26 de Julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

Normativa sobre “Puerto Seguro” o Safe Harbor Framework, Department of Commerce del Gobierno USA, <http://www.export.gov/safeharbor/>

Lista de empresas incluidas en el *safe harbor* de EEUU;
<https://www.export.gov/safehrbr/list.aspx> visitado el 14-VII-2010

Links a páginas web:

Términos de Usuario de Facebook: visitado el 14-VII-2010
<http://www.facebook.com/terms.php?ref=pf>

Principios de Privacidad de Google, visitado el 20-VII-2010
http://www.google.com.uy/intl/es/corporate/privacy_principles.html

Política de Privacidad de Facebook: visitado el 14-VII-2010
<http://www.facebook.com/privacy/explanation.php#!/policy.php>

Información para anunciantes de Facebook: visitado el 14-VII-2010
<http://www.facebook.com/advertising/>

Madrid, Julio 2010