DERECHOS FUNDAMENTALES EN LAS REDES SOCIALES

VNiVERSiDAD D SALAMANCA

Eva Garrido Saiz

Con la dirección de:

Mercedes Curto Polo

UNIVERSIDAD DE SALAMANCA

FACULTAD DE TRADUCCIÓN Y DOCUMENTACIÓN

GRADO EN INFORMACIÓN Y DOCUMENTACIÓN

Trabajo de Fin de Grado

DERECHOS FUNDAMENTALES EN LAS REDES SOCIALES

Eva Garrido Saiz

Con la dirección de:

Mercedes Curto Polo

Salamanca, 2016

GARRIDO SAIZ, Eva

Derechos fundamentales en las redes sociales /Eva Garrido Saiz; bajo la dirección de Mercedes Curto Polo – Salamanca: Universidad de Salamanca, Facultad de Traducción y Documentación, 2016,

55 h.

Trabajo de fin de grado – Grado en Información Documentación

1. Derecho privado. 2. Derechos fundamentales. 3. Redes sociales. I. Curto Polo, Mercedes, dir. II. Título.

Lista de abreviaturas

AEPD	Agencia Española de Protección de Datos
BOE	Boletín Oficial del Estado
CE	Comisión Europea
CIS	Centro de Investigaciones Sociológicas
COPPA	Children's Online Privacy Protection Act
INTECO	Instituto Nacional de Tecnologías de la Comunicación
LOPD	La Ley Orgánica de Protección de Datos
RDLOPD	Real Decreto Ley Orgánica de Protección de Datos
TJUE	Tribunal de Justicia de la Unión Europea
UE	Unión Europea

Resumen

En este trabajo se aborda el tema de las redes sociales en relación a los derechos fundamentales de los usuarios destacando que las innegables ventajas de su uso no empañan los riesgos potenciales contra la privacidad. Se hace patente un profundo desconocimiento generalizado de los términos y condiciones legales en el usuario común, así como, un estrato social especialmente delicado como son los menores de edad. Igual de confuso resulta una de las vías de protección de la privacidad, el derecho al olvido tiene diferentes interpretaciones en la legislación dejando una sensación de indefensión de todo usuario que comparte su información en la red.

Palabras clave: Redes sociales, privacidad, motores de búsqueda, derechos fundamentales, derecho al olvido, menores de edad.

Abstract

In this work, it is tackled the social networks matter in relation with the users' fundamental rights, being outlined that the undeniable advantages of their use, don't stain the potential risks against privacy. It is patented a deep widespread ignorance of legal terms and conditions in the common user, as well as a social stratum especially delicate, minors. Similarly confusing is one of the means of privacy protection; the right of forget has different interpretations in the legislation, leaving a feeling of defencelessness in any user who shares his own information on the net.

Keywords: Social networks, privacy, search engines, Fundamental rights, right to oblivion, minor

SUMARIO

1. Introducción

A día de hoy muy pocas personas están exentos del uso de las redes sociales, y por ende de Internet. Cada vez más personas de todas las edades se unen a utilizar lo que ha sido uno de los grandes avances en la comunicación del siglo XXI. El surgimiento de Internet ha modificado radicalmente la vida de las personas, tanto en sus comunicaciones como su vida profesional y comercial, Internet ha globalizado y ha acercado a las personas de todo el planeta.

En un margen muy reducido de tiempo el avance ha sido enorme y tan rápido que toda la regulación concerniente al uso de las Nuevas tecnologías apenas ha tenido tiempo de adaptarse para proteger de una forma segura y capaz a los millones y millones de usuarios de la web. Mientras, la legislación lucha por la protección de las actividades comerciales abusivas donde los datos personales son mera mercancía entre empresas, también tiene a una clase de usuario que generalmente pone poco o ningún cuidado a cuáles son sus derechos y que repercusiones tienen sus actos en Internet.

Lo realmente complejo es encontrar el equilibrio entre la privacidad y la explotación de los datos. Esto es clave para que haya un desarrollo sostenido, ya que el mayor de los servicios que utilizamos se basa en una relación de confianza entre el usuario y quién lo presta.

Lo cierto es que el ciudadano está encantando porque dispone de aplicaciones y servicios gratuitos que le hacen la vida más fácil, mientras que las empresas, cuyo modelo de negocio se basa en la explotación de datos personales, están dando cada vez más herramientas para que el usuario tenga un mejor control de su privacidad.

El nivel de preocupación por la privacidad en los usuarios de Internet es bajo ya que en general confían en demasía, el ciudadano normal desconoce quién o quienes tienen acceso a sus datos, cómo se recolectan, para que se usan o para que se podrían usar y desconoce el valor de sus datos personales.

Sin embargo poco a poco vamos valorando más nuestra privacidad y hay una corriente creciente que empieza a preguntarse sobre donde están los límites. Existe por tanto una responsabilidad de todos de sensibilizar a la sociedad y a sus ciudadanos para que dejen de ser agentes pasivos y que pasen a ser sujetos activos en la gestión de su privacidad.

Para que esto suceda es importante tener herramientas y un marco regulatorio y jurídico que permita conocer entre otras cosas quién, cómo y cuándo se utilizan los datos personales y el valor que se genera con el uso de las redes sociales.

Este trabajo analiza en qué situación se hayan estas tecnologías analizando el marco tanto teórico como jurídico de las redes sociales y los motores de búsqueda.

Precisamente, éstos son los dos actores principales en el conflicto legislativo referente al derecho al olvido.

Le sigue el estudio especializado del derecho al olvido, separando las responsabilidades tanto del motor de búsqueda como de las redes sociales en cuanto a la información divulgada.

De igual forma, se analizará el estrato social más débil ante abusos en la privacidad de datos personales como son los menores y qué condiciones y términos adoptan las redes sociales para su protección así como la legislación que los ampara.

Una vez que tenemos el contexto y hemos delimitado el grado de responsabilidad de cada ente, analizaremos algunos casos prácticos reales donde los protagonistas son el derecho al olvido contra Google y como posteriormente ha afectado a diferentes proveedores de servicios web. Veremos cómo han tenido una disputa referente a la privacidad de sus usuarios y a sus derechos sobre informaciones personales, y sobre qué ente tiene la responsabilidad de la publicidad y difusión de la información lesiva para su persona. Por último, condesaremos que conclusiones son relevantes de este trabajo y que aspectos deberían tener mayor atención.

No puedo desdeñar el hecho de mi gran satisfacción al realizar un estudio referente a un tema realmente interesante para mi persona, con la tutela de Mercedes Curto Polo, quién ha impulsado y potenciado mi interés sobre los temas más “jurídicos” en relación a las Redes Sociales y a su protección normativa.

2. Marco teórico

El ser humano es un ser social por naturaleza, es decir, necesita de los demás para realizarse y desarrollar su vida en sociedad. Esta realidad se refleja en el espectacular crecimiento de las redes sociales a nivel global.

La sociedad española no ha sido ajena a este fenómeno, y se sitúa en Europa como primer país en número de usuarios de redes sociales y segundo del mundo[1]. Este dato lo presenta el Estudio Anual de Redes Sociales, que realiza IBA Spain, cuando revela que un 81% de los internautas accede habitual u ocasionalmente las redes sociales.

Dejando a un lado datos estadísticos, las redes sociales han afectado a nuestra vida cotidiana dándonos nuevas oportunidades como establecer nuevas amistades y relaciones con personas a quienes no conocemos pero que nos une un interés profesional, laboral, personal o de ocio.

En una sociedad dominada por la información, donde el poder se sitúa en el conocimiento, y donde valemos tanto más por nuestras relaciones o contactos como por lo que somos, las redes sociales han venido a configurar e impulsar un nuevo concepto de relación personal y social.

Se han cambiado las agendas y libretas de contactos, que representaban nuestra red social por nuevas herramientas de comunicación que facilitan una forma virtual de contacto y relación; así, primero irrumpe el móvil con agenda, y después, las redes sociales digitales, como representación virtual y pública de nuestras relaciones personales, profesionales y laborales.

En torno al 2002 emerge la denominada web 2.0 donde el internauta ya no sólo busca y decide la información que desea obtener sino que también la edita, comenta y comparte. Hasta entonces internet se presentaba estática y el usuario era un mero espectador, posteriormente emerge una internet colaborativa, dinámica y social, donde el usuario no se conforma con ser parte activa de la red y relacionarse con otros internautas, sino que se convierte en protagonista voluntario de una comunidad virtual, desde la que se promueven encuentros, movimientos sociales de apoyo o rechazo y se convocan reuniones o manifestaciones.

Nos hallamos ante una internet social e interrelacional, en la que las redes sociales son su principal herramienta.

[1] ONTSI, Informe sobre el Sector de las tecnologías de la Información en España 2008, 2009.

Este cambio de comportamiento y actitud, en el que se busca compartir entre personas, empresas e instituciones, tanto experiencias, sensaciones, viajes, amistades, como música o conocimientos explica el espectacular crecimiento de las redes sociales. Éxito que sin duda se ha visto favorecido por la generalización del uso de los teléfonos móviles que por su movilidad permiten compartir en breve espacio de tiempo y desde cualquier lugar experiencias, información, vídeos o fotografías.

Con todo esto, las redes sociales han abierto una forma impensable de hacer política, han establecido un espacio de libertad de expresión inimaginable hasta ahora, y han favorecido las relaciones laborales y profesionales en un momento tan crítico como el que actualmente vivimos.

Sin embargo, todos estos cambios no han sido positivos, ya que los usuarios comparten información, datos personales, imágenes, en ocasiones muy sensibles, e incluso de terceras personas, lo que sin duda debe interpretarse como un cambio en la consideración de la intimidad y la privacidad personal por parte del propio usuario, que expone en ocasiones a un riesgo evidente de los derechos fundamentales de la persona.

El propio concepto y el funcionamiento de las redes sociales conllevan cierta renuncia a la intimidad por quienes acceden a las mismas y comparten su vida privada, y se puede decir que se trata de una renuncia voluntaria, aunque no siempre es consciente y reflexiva. Gran parte de los usuarios desconoce la política de privacidad de estas plataformas, que no resulta de fácil comprensión, y de manera mecánica se aceptan todas las condiciones que sean precisas para poder participar en estas comunidades virtuales, especialmente cuando se trata de los más jóvenes.

Lo más recomendable es utilizar la misma prudencia que se emplearían en las actividades fuera de las redes sociales, es decir no actuar de manera inconsciente, impulsiva o imprudente. Debemos medir las consecuencias de nuestros actos, y no actuar de manera irreflexiva y poco cautelosa.

Debemos aclarar que las oportunidades, posibilidades y ventajas que ofrecen las redes sociales no deben quedar en entredicho por las actuaciones imprudentes, abusivas y arriesgas de los usuarios o de terceros malintencionados.

Desde la perspectiva empresarial y económica, las redes sociales han reforzado la presencia de empresas y medios de comunicación en la red, facilitando enormemente la realización de negocios a través de internet. Hoy en día tener un espacio de negocio en las redes sociales más populares es casi una obligación puesto que puede significar un aumento considerable de los beneficios, ya que tal y como demuestran diferentes estudios, los usuarios de Internet reconocen en su mayoría acceder habitualmente a estas comunidades y buscar todo lo que necesitan a través de ellas.

De igual manera, al constituirse en espacio de sociabilización, se convierten en una herramienta incomparable para analizar a posibles competidores, o comunicarse con

potenciales clientes**,** quienes además consultan e indagan dentro de estas plataformas antes de concretar alguna compra o negocio. Por todo ello, no debemos menospreciar la trascendencia comercial, empresarial y económica de las redes sociales, habida cuenta del número de usuarios que pertenecen a estas comunidades virtuales y de las actividades que en ellas se desarrollan.

Para comprender y analizar el desarrollo de las redes sociales debemos establecer previamente su concepto y caracteres y así poder explicar el éxito de su crecimiento y de su popularidad. De acuerdo con la definición ofrecida en el Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes online del Instituto Nacional de Tecnologías de la Comunicación (INTECO) y la Agencia Española de Protección de Datos (AEPD), las redes sociales se definen como:

"Servicios prestados a través de internet que permiten a los usuarios generar un perfil, desde el que hacer públicos datos e información personal y que proporcionan herramientas que permiten interactuar con otros usuarios y localizarlos en función de las características publicadas en sus perfiles". [2]

La mayoría de los ingresos que generan las redes sociales son a través de la publicidad que difunden en las páginas Web, a las que los usuarios crean y acceden. De esta manera los usuarios que publican en sus perfiles mucha información sobre sus intereses ofrecen un mercado depurado a los publicitarios que desean difundir publicidad específica y basada en la información.

Por ello es importante que funcionen respetando los derechos y libertades de los usuarios, que tienen la esperanza de que los datos personales que revelan sean tratados de acuerdo con la legislación europea y nacional relativa a la protección de datos y la intimidad.

Las redes sociales pueden clasificarse en base a diferentes criterios pero el tema que nos atañe, la finalidad, es el atributo que utilizamos para clasificarlas:

- Redes sociales de comunicación, como Facebook, Twitter o Instagram. En estas plataformas el usuario se puede dar de alta en el servicio libremente, o a través de invitación y encontrar conocidos o invitarles a formar parte de su comunidad. Este tipo de redes permiten la vinculación entre los usuarios con contactos de segundo o tercer grado o gente que pertenece a los mismos grupos, como pueden ser miembros de colegios, universidades, etc. En estas redes se suelen publicar fotografías, videos, reflexiones, aficiones y preferencias de todo tipo.

[2] INTECO y AEPD, Estudio sobre privacidad de los datos y la seguridad de la información en las redes online, 2009.

- Redes sociales especializadas, cuya finalidad suele unir a colectivos con unos mismos intereses; virtualtourism.com para viajeros, flickr.com para compartir fotografías o para encontrar pareja como Meetic o Ashley Madison.

- Redes sociales profesionales, como LinkedIn, Xing o JobToday, que permiten a los individuos de todo el mundo buscar oportunidades de empleo, hacer networking con compañeros de trabajo, con gente del ámbito profesional. Estas tienen un público más especializado, y su modelo de financiación está basado en venta de servicios Premium o en la realización de campañas de publicidad personalizada.

3. Marco jurídico

Desde el ámbito jurídico se entiende por red social, a tenor de lo preceptuado por el Grupo de Trabajo sobre Protección de Datos del artículo 29 el 12 de junio de 2009, en su Dictamen 5/2009 sobre redes sociales: como *plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes.*[3]

De este modo, las redes sociales se convierten en lugares virtuales de relación personal, en los que no solo gestionamos nuestra identidad sino que podemos limitar nuestros intereses y restringirlos según nuestras preferencias.

Todos los sujetos que participan de forma directa o indirecta en las redes sociales deberían conocer sus derechos y obligaciones, así como los riesgos que derivan de su uso. El hecho de participar en las redes sociales supone la implicación de diferentes sujetos y riesgos.

Los principales sujetos implicados son, las redes sociales y plataformas colaborativas, los proveedores de servicios, los desarrolladores de software, empresas de marketing y publicidad, la propia Administración Pública, y los usuarios.[4]

[3] GRUPO DE TRABAJO SOBRE PROTECCIÓN DE DATOS DEL ARTÍCULO 29, Dictamen 5/2009 sobre redes sociales en línea, 2009. Disponible es: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_es.pdf

[4] INTECO y AEPD, Estudio sobre privacidad de los datos y la seguridad de la información en las redes online, 2009.

Por otro lado los principales riesgos que conllevan están relacionados con los derechos vinculados con los datos personales; la intimidad, honor y propia imagen; la propiedad intelectual e industrial.

Los riesgos mencionados anteriormente comienzan cuando el usuario inicia el proceso de registro en la red social. En este momento, la Administración ofrece un marco jurídico de protección al usuario en relación a sus derechos, en muchas ocasiones este servicio no es suficiente en relación de la contratación con la red social ni respecto a los derechos de intimidad, intelectuales ni industriales.

Son numerosos y significativos los datos personales que en ocasiones voluntariamente, y en otras inconscientemente, los usuarios transfieren a las plataformas para su tratamiento. Es por ello, que cada red social debe tener una serie de pautas y principios específicos que permitan a los usuarios, antes de registrarse, identificar su política de privacidad y sobre todo contar con la normativa vigente de protección de datos personales.

Los datos personales se entienden en La Ley de Protección de Datos[5], en su Art. 3 como cualquier información referente a personas físicas con posibilidad de identificarlas. El R.D. 1720/2007 (RLOPD), en su Art. 5.1, especifica además que puede tratarse de información numérica, alfabética, grafica, acústica, etc. La persona o entidad que posea nuestros datos (y por tanto es el "responsable de los ficheros"), tiene el deber de pedir el consentimiento de la persona afectada. Y salvo que la ley disponga otra cosa al respecto, este consentimiento debe ser específico e informado, es decir, se presta para una finalidad concreta; y no se hace extensivo a otros usos para los que no se haya dado expresamente dicho consentimiento

La LOPD, en su Art. 16.1, establece que "el responsable del tratamiento de los datos tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días". Mientras que, en el Art. 16.3, deja claro que "la cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas".

El Art. 44.3 de esta misma ley hace referencia a las infracciones graves, y en su apartado h) destaca como tal la de "mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen".

En España, la regulación sobre protección de datos de carácter personal en el sector privado se conforma a partir de dos normas principalmente: la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), y el Real

[5] LEY ORGÁNICA 15/1999, Protección de Datos de Carácter Personal. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (RDLOPD).

A nivel sectorial se encuentran La Ley 34/2002 , de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (BOE 166 de 12-07-2002), la Ley 32/2003, General de Telecomunicaciones (Arts 33-35) y la Ley 59/2003, de 19 de diciembre, de Firma Electrónica (BOE 304 de 20-12-2003).

En el ámbito de la Unión Europea, el derecho a la protección de datos se contempla en el artículo 8 de la Carta Europea de Derechos Fundamentales, en el cual se establece un tratamiento leal de los datos para fines concretos que se sustenta en el consentimiento. En cuanto a la regulación legal a la que están sometidas las redes sociales, a pesar de las diferencias entre las distintas redes y su singular configuración en el ámbito de la UE, todas ellas están sometidas con el mismo marco jurídico general recogido en la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, de protección de las personas frente al tratamiento de sus datos personales y de su libre circulación.

Debido al amplio alcance que el tratamiento de datos personales en Internet puede llegar a tener y su incidencia en los derechos fundamentales, las instituciones europeas llevaron a cabo un proceso de unificación y modernización de las normas jurídicas. Es por ello que el 25 de enero de 2012 la Comisión Europea publicó el Borrador de la Propuesta de Reglamento General de Protección de Datos de la Unión Europea. Esta Propuesta pretende modernizar la legislación europea de protección de datos estableciendo una normativa que se adapte con mayor rigor a las transformaciones, nuevas circunstancias y presupuestos de hecho que realmente genera el mundo de las TIC en el ámbito de la protección de los datos de las personas, queriendo establecer un marco más sólido y coherente en materia de protección de datos en la UE. Asimismo la Propuesta pretende homogeneizar las distintas legislaciones nacionales de los estados miembros, que adaptaron de forma diferente la Directiva.

Finalmente el 8 de abril de 2016, el Consejo adoptó su posición en primera lectura. A continuación, el Parlamento Europeo adoptó el proyecto de Reglamento el 14 de abril de 2016. Aprobando así el Reglamento General de Protección de Datos de la Unión Europea por el cual recogen los derechos de las personas y se establecen las obligaciones de los encargados y responsables del tratamiento de los datos.

El incremento de los tratamientos de datos personales con ciencias como la videovigilancia, la biometría, la nanotecnología, la historia clínica electrónica en la nube, la identificación por radiofrecuencia, etc. incrementan el nivel de riesgo para la privacidad, por lo que este proceso debe ir acompañado de una mejora de las garantías de la privacidad de las personas.

Este cambio era necesario ante avance tecnológico, dando a las personas más instrumentos para el control sobre su información personal. En esta misma línea está la aprobación del Tratado de Lisboa, que refuerza la base jurídica en la Unión Europea para aprobar una normativa para el reconocimiento de un derecho fundamental a la protección de datos personales. Y es que, la protección de datos personales es un elemento esencial para la construcción de la Unión Europea y para hacer viable la libre circulación de personas y que los países europeos tengan un modelo de protección de datos personales homogéneo que permita el intercambio de información.

Sin embargo, las divergencias en la protección de los datos personales en los Estados miembros son aún demasiado grandes, consecuencia, por una parte, por la Directiva 95/46/CE y por otra, del margen de maniobra que dejaba la propia directiva como derecho institucional y que contenía abundantes cláusulas abiertas a distintas aplicaciones en cada país. Estas diferencias en la protección de los datos personales entre los Estados miembros han obstaculizado el mercado interior, han dificultado el ejercicio de actividades económicas a escala comunitaria y han falseado la competencia; y más importante, esta ausencia de una protección equivalente afecta a la protección de datos personales de todos los ciudadanos europeos.

4. Derecho al olvido y servicios de la sociedad de la información: motores de búsqueda y redes sociales.

Según la Agencia Española de Protección de datos el derecho al olvido es:

El denominado 'derecho al olvido' es la manifestación de los tradicionales derechos de cancelación y oposición aplicados a los buscadores de internet. El 'derecho al olvido' hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información).

El derecho al olvido es un derecho relacionado con el Habeas Data y la protección de datos personales. Se puede definir como el derecho que tiene el titular de un dato personal a borrar, bloquear o suprimir información personal que se considera obsoleta por el transcurso del tiempo o que de alguna manera afecta el libre desarrollo de alguno de sus derechos fundamentales.

Los servicios de la sociedad de la información integrados por los motores de búsqueda y las redes sociales constituyen un ámbito en el que el derecho al olvido tiene una importancia significativa.

En el caso de los buscadores, la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 ha afirmado que este tipo de servicios se deben al cumplimiento de la normativa de protección de datos y, en particular, la obligación de éstos de eliminar de la lista de resultados los vínculos a páginas web que contengan datos personales inadecuados, no pertinentes o excesivos.

Este reconocimiento del derecho al olvido frente a los motores de búsqueda constituye un avance en conseguir una protección plena y eficaz de los derechos de las personas en el entorno digital cuya implementación efectiva requerirá la colaboración de los gestores de los motores de búsqueda y las autoridades de protección de datos con el fin de establecer un marco claro y seguro para dar solución a los conflictos entre intereses privados e interés público.

En el caso de las redes sociales, se ha de poner especial atención en el valor del consentimiento del particular como elemento clave para aclarar los supuestos en que se quiere ejercitar el derecho al olvido.

4.1 Motores de búsqueda

Los motores de búsqueda constituyen la puerta de acceso a Internet. Desarrollan una función esencial de organización de la información disponible en la red y facilitan el acceso a ella. Sin estas herramientas la tarea de buscar la información que nos interesa en el universo de páginas web existentes (cerca de mil millones de páginas web, actualmente, de acuerdo con los datos de www.internetlivestats.com) sería imposible.

Los motores de búsqueda han reclamado para sí el papel de "intermediarios neutrales"[6] entre los editores de las páginas web y los usuarios de la red, realizando únicamente una actividad técnica que favorece la accesibilidad y el hallazgo de los contenidos que publican unos y buscan otros.

Según este principio de neutralidad, defendido sobre todo por Google, la responsabilidad por los contenidos a los que enlaza su página de resultados es exclusivamente del editor de la página. De este modo, en relación con el grado de responsabilidad que le corresponde a los buscadores a la hora de garantizar el derecho al olvido es de la página fuente de la información y no del buscador.

[6] MIERES, Mieres Mieres, Luis Javier. *El derecho al olvido digital*. 2014

"La propuesta de Reglamento general de protección de datos realizada por la Comisión en el caso Google parece asumir que el sujeto obligado a dar cumplimiento al derecho al olvido es la persona que ha divulgado los datos y no los terceros que albergan copias o enlaces a ellos."[7]

De acuerdo con el artículo 17 de la propuesta del Reglamento, ante el ejercicio del derecho de cancelación o de oposición, corresponde a la página que inicialmente trató los datos poner fin al tratamiento y adoptar las medidas razonables precisas para informar a un tercero que posteriormente esté tratando los datos que el interesado está solicitando la supresión del dato o la copia o réplica.

En contra a esta tesis que podemos llamar del "intermediario neutral" y la no sujeción a la normativa de protección de datos de los motores de búsqueda, ha cogido peso la posición de la Agencia Española de Protección de Datos que ha sostenido que los buscadores al presentar los enlaces a distintas páginas web en su página de resultado realizan un tratamiento de datos del que son responsables y están obligados a respetar y garantizar los derechos de cancelación y oposición de los particulares afectados.

Esta posibilidad de que los motores de búsqueda sean destinatarios del derecho al olvido ha sido acogida por el Parlamento Europeo en el texto del artículo 17 de la propuesta de Reglamento en el sentido de incluir expresamente el derecho "a obtener de los terceros la supresión de cualquier enlace, copia o réplica de esos datos personales".

De este modo, del texto del Reglamento general de protección de datos aprobado por el Parlamento Europeo se deduce claramente que el titular de los datos podrá dirigirse tanto al responsable del tratamiento como al motor de búsqueda para que cese la difusión de los datos personales que considera obsoletos, excesivos o impertinentes.

Este es el panorama normativo en el que debe situarse la sentencia del Tribunal de Justicia de 13 de mayo de 2014, C-131/12, dictada en relación con la cuestión prejudicial formulada por la Audiencia Nacional, en el asunto Google España.

El reconocimiento del derecho al olvido frente a los motores de búsqueda está basada en la afirmación de cuatro tesis, que hasta la sentencia, eran especialmente problemáticas.

En primer lugar, la actividad de los motores de búsqueda debe calificarse como tratamiento de datos. Las funciones que realizan los buscadores de extraer los datos de las páginas web existentes, registrarlos, organizarlos en el marco de sus programas de

[7] Troncoso Reigada, A. (2012), El derecho al olvido en Internet a la luz de la propuesta de Reglamento General de Protección de Datos Personales, Datospersonales.org: Revista de la Agencia de Protección de Datos de la Comunidad de Madrid, núm. 59.

indexación, conservarlos en sus servidores y facilitar el acceso a los usuarios a través de la página de resultados constituyen operaciones de tratamiento.

En segundo lugar, el motor de búsqueda establece los fines y los medios de esa actividad y, por tanto, es el responsable de que el tratamiento de datos personales cumpla con las exigencias de la Directiva 95/46. Esta responsabilidad es propia y autónoma respecto de la de los editores de las páginas web. El que éstos no hayan utilizado protocolos de exclusión o códigos no significa que el motor de búsqueda quede liberado de su responsabilidad respecto de las operaciones de tratamiento de datos personales que realiza. De este modo, el motor de búsqueda debe garantizar *"una protección eficaz y completa de los interesados, en particular, de su derecho al respeto de la vida privada en el marco de sus responsabilidades, de sus competencias y de sus posibilidades".*[8]

En tercer lugar, la empresa gestora de un motor de búsqueda está sujeta a la normativa europea de protección de datos, a pesar de que su sede matriz radique fuera de la Unión Europea, siempre que mantenga un establecimiento en un Estado miembro a través del cual desarrolle una actividad económica vinculada con el motor de búsqueda.

Y, finalmente los motores de búsqueda deben respetar, en particular, los derechos de rectificación, supresión y bloqueo (Directiva 95/46/CE) y de modo que, en relación con búsquedas realizadas a partir del nombre de una persona, deben eliminar de la página de resultados los vínculos a páginas web que contengan información relativa a esa persona, con independencia de que la publicación de esa información haya sido lícita o siga siendo accesible en la página web, siempre que los datos personales contenidos en esa información resulten inadecuados, no pertinentes o excesivos en relación con los fines que justificaron su tratamiento.

La argumentación de la sentencia para fundamentar estas cuatro afirmaciones de principio se sostiene sobre tres grandes argumentos:

- la necesidad de una "protección eficaz y completa" de los derechos de los interesados.

- la singularidad de los motores de búsqueda y su impacto sobre los derechos de los interesados.

- la prevalencia, en principio, de los derechos de los interesados frente a los intereses económicos de los gestores de los motores de búsqueda y el interés del público en encontrar información personal mediante la búsqueda a partir del nombre de una persona.

[8] 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.

Uno de los puntos especialmente subrayados por el Tribunal es el carácter singular de los buscadores y como afecta su actividad sobre los derechos de las personas. En la sentencia (Directiva 95/46/CE) se enfatiza el impacto que tiene la difusión de datos personales a través de la página de resultados de un buscador porque se trata de una "difusión global" de esos datos y que ofrece "una visión estructurada" de la información relativa a una persona que permite establecer "un perfil más o menos detallado" de ésta.

Estos factores hacen que el tratamiento realizado por el buscador de datos personales previamente divulgados en páginas web tenga un impacto adicional al de esa publicación original y afecte significativamente a los derechos fundamentales de respeto de la vida privada y de protección de datos personales (arts. 7 y 8 Carta Europea de Derechos Fundamentales). A partir de estas consideraciones, el Tribunal concluye la especial necesidad de protección de los derechos de los interesados frente a la "gravedad potencial" de la información personal potencialmente pública con sólo teclear el nombre de una persona.

Como excepción, el artículo 17 de la Ley 34/2002, reguladora de los servicios de la sociedad de la información, prevé una regla de exención de responsabilidad por los enlaces a la información de terceros que ofrece este tipo de prestadores de servicios si se cumplen las siguientes circunstancias:

- que no tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o que lesiona bienes o derechos de un tercero susceptibles de indemnización;

- o si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

La ley, en principio, delimita los medios a través de los cuales el prestador del servicio puede ser sabedor del carácter ilícito de la información y, por tanto, tener "conocimiento efectivo":

"Cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse".

La Sentencia del Tribunal de Justicia de la Unión Europea (TJUE) de Mayo de 2014

Disponible en:
http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES

Se trata de una sentencia de enormes consecuencias en el ámbito del derecho al olvido. El pronunciamiento del Tribunal definitivamente regula el régimen de responsabilidades de los buscadores de internet en relación con la protección de los datos personales.

En la sentencia del TJUE se establece que:

- La actividad de los motores de búsqueda como Google constituye un tratamiento de datos de carácter personal, del que es responsable el propio motor, dado que éste determina los fines y los medios de esta actividad.

- Ese tratamiento está sometido a las normas de protección de datos de la Unión Europea, dado que Google ha creado en un Estado miembro un establecimiento para la promoción y venta de espacios publicitarios y cuya actividad se dirige a los habitantes de ese Estado.

- Las personas tienen derecho a solicitar del motor de búsqueda, con las condiciones establecidas en la Directiva de protección de datos, la eliminación de referencias que les afectan, aunque esta información no haya sido eliminada por el editor ni dicho editor haya solicitado su desindexación. En caso de no atenderse su solicitud, las personas tienen derecho a recabar la tutela de la AEPD y de los Tribunales.

- El derecho a la protección de datos de las personas prevalece, con carácter general, sobre el mero interés económico del gestor del motor de búsqueda salvo que el interesado tenga relevancia pública y el acceso a la información esté justificado por el interés público.

Entre otras, la Agencia Española de Protección de Datos (AEPD) destaca las siguientes cuestiones:

- **Responsabilidad de los motores de búsqueda.** La sentencia establece que los motores de búsqueda realizan un tratamiento de datos personales y sus gestores están obligados a asumir las responsabilidades en los términos previstos en la normativa europea y, en particular, a respetar los derechos de cancelación y de oposición reconocidos a todos los individuos.
- **No se elimina información.** La sentencia declara expresamente que el ejercicio de los derechos de cancelación y oposición sólo afecta a los resultados obtenidos en las búsquedas hechas mediante el nombre de la persona y no implica que la página deba ser suprimida de los índices del buscador ni de la fuente original. En

consecuencia, la información continua intacta en la web original y seguirá siendo accesible a través del buscador por cualquier otra palabra o término que no sea el nombre del afectado.

- **Análisis caso por caso.** El Tribunal destaca el impacto que la actividad de los buscadores tiene en los derechos a la privacidad y a la protección de los datos personales por cuanto permiten acceder desde cualquier lugar a múltiples informaciones personales que posibilitan la elaboración de perfiles. Dada la importancia de este impacto, considera que los derechos de los afectados prevalecen sobre el interés económico de los buscadores y sobre el interés de los internautas en acceder a información personal. Sin embargo, señala que es necesario realizar un estudio caso por caso para alcanzar un «un justo equilibrio» entre los derechos e intereses. Por lo tanto, el resultado dependerá, en cada supuesto, de la naturaleza y sensibilidad de los datos y del interés del público en acceder a una determinada información.
- **Libertades de expresión e información.** El impacto de estos derechos sobre las libertades de expresión y de información, tanto de los editores como de los usuarios de internet, es muy limitado. Puesto que en la valoración de las circunstancias de cada solicitud se debe tener en cuenta el interés de los usuarios en acceder a una información, aquellas que resulten de interés público no serán bloqueadas. La libertad de información no se verá afectada cuando se trate de información con interés general, ya que en esos casos no procede reconocer el derecho al olvido.
- **Buscadores internos.** Los buscadores propios incluidos en las webs de diferentes páginas o medios de comunicación no están afectados por la sentencia. Estos buscadores internos sólo recuperan la información contenida en páginas web específicas además que no permiten establecer un perfil completo de la persona afectada, algo que sí permiten los motores de búsqueda.
- **Ejercicio de derechos.** Los ciudadanos se pueden dirigir directamente al motor de búsqueda sin necesidad de acudir previamente al sitio original. Los motores de búsqueda y los editores originales realizan dos procesamientos de datos diferenciados. Por eso puede suceder, que el contenido que publica el editor siga siendo legal con el paso del tiempo mientras que la difusión universal que realiza el buscador, sumado a la información adicional que facilita sobre el mismo individuo cuando se busca por su nombre, tenga un impacto desproporcionado sobre su privacidad.
- **Ámbito de aplicación**. Un adecuado cumplimiento de la sentencia requiere que los datos de las personas estén protegidos de forma eficaz y completa, y que la legislación de la Unión Europea no pueda eludirse fácilmente. En la práctica, ello implica que la exclusión debe también ser eficaz en todos los dominios

relevantes, incluidos los «.com», es decir, aquellos que sean accesibles desde el territorio europeo.

- **Política de avisos.** La práctica de algunos buscadores de informar a los usuarios de que la lista de resultados puede no estar completa como consecuencia de la aplicación del derecho europeo no encuentra fundamento en ninguna normativa. Por lo tanto, esta práctica sólo puede ser aceptable si la información se ofrece de tal manera que los usuarios no puedan deducir que una persona concreta ha solicitado la retirada de ciertos resultados asociados a su nombre.
- **Comunicación a terceros.** En relación con la práctica desarrollada por algunos buscadores de comunicar a los responsables de las webs que ciertas páginas dejarán de ser accesibles en determinadas búsquedas realizadas por nombres de personas se manifiesta que no existe base legal que ampare dicha comunicación.
- **Transparencia.** Teniendo en cuenta la relevancia del acceso a páginas web a través de buscadores y las expectativas de indexación de editores y propietarios de esas páginas, se considera necesaria una mayor transparencia a la hora de llevar a cabo las valoraciones. La Autoridades europeas instan a los buscadores a que hagan públicos los criterios de exclusión que están aplicando y que faciliten estadísticas detalladas y anonimizadas sobre los tipos de casos en los que han aceptado o rechazado las correspondientes solicitudes.

La sentencia del TJUE supone por lo tanto un paso adelante en el derecho al olvido de los ciudadanos

4.2 Redes sociales

Las redes sociales han multiplicado exponencialmente las posibilidades de comunicación entre personas, de acceso a información, y de establecer nuevos instrumentos de colaboración y asociación. Han creado un nuevo entorno social en el que el elemento básico de la interacción es compartir información personal. Facebook, Tuenti, Twitter o LinkedIn permiten a sus millones de usuarios publicar y difundir datos personales y fortalecer lazos con personas ya conocidas o darse a conocer a otras, en el caso de Google + permite difundir la información con el mundo entero.

Por la propia naturaleza y esencia de los servicios de las redes sociales, no hay que olvidar que nos hallamos ante plataformas de contactos y de intercambio de información, y precisamente por ello, estas comunidades representan en sí mismas una amenaza y un riesgo para sus usuarios.

La información que publicamos en Internet puede ser vista en el presente desde cualquier parte del mundo y perdurará siendo accesible en el futuro. Podríamos decir

que las virtudes y defectos del mundo real se encuentran reflejados también en internet, si bien los principios que se aplican en ambos espacios no se corresponden exactamente.

Al contrario del pensamiento generalizado de seguridad, lo que sucede en Internet no desaparece cuando cerramos la aplicación y apagamos el ordenador, y los efectos y las consecuencias permanecen, y afectan no sólo a nuestros intereses en internet, sino también a nuestra realidad física.

En efecto, si consideramos que el fin y la esencia de las redes sociales se haya en compartir información, amigos, contactos, experiencias, no resulta difícil comprender los recelos y las reservas que las redes sociales despiertan en instituciones, empresas y juristas. Obviamente, vienen a nuestra mente actividades humanas que conllevan riesgo, incluso peligro para la propia vida y la de los demás, y no por ello dejamos de realizarlas, ni desde las instituciones se recomienda abstenerse en su realización. Así el usuario debe identificar y conocer la existencia de los riesgos inherentes a las redes sociales como instrumentos de comunicación, sin que por ello deba denostarse el uso de esta herramienta, al tiempo que se ensalzan sus innegables ventajas y bondades, deben señalarse sus peligros. Además debe informarse y educarse para una actuación prudente, ordenada y actualizada, que ayude al usuario a actuar con el sentido común y la prudencia deseables en todas las situaciones de la vida cotidiana.

En términos generales, la 30ª Conferencia Internacional de Autoridades de Protección de Datos[9], expone alguno de los riesgos más destacados para la protección de los datos personales de los usuarios de estas plataformas, distinguiendo, entre otros:

- La dificultad para eliminar el perfil y cancelar los datos personales.

- La indexación de la información personal por motores de búsqueda.

- El rastreo por terceros de los datos personales que quedan expuestos públicamente en la red social.

- La obtención de información personal por terceros para obtener perfiles diferentes al deseado y creado por la propia persona.

- La facilidad con la que terceros se pueden apropiar ilícitamente de la identidad de la persona, lo que escapa al control de cada uno si no es usuario de la red social y no le avisan de ello. La suplantación de la identidad tendrá intención bien

[9] 30. ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad, Resolución sobre la protección de la privacidad en los servicios sociales, Estrasburgo, 15-17 de octubre de 2008.

de dañar a la propia persona o a un tercero. Para cuando la denuncia se presenta el abuso está ya cometido.

- La utilización comercial de nuestros datos personales, para enviar publicidad no deseada de manera personalizada al usuario.

- La descontextualización de la información personal del usuario, que amenaza la privacidad del individuo y su derecho a la protección de datos personales.

Aunque pudiera parecer que los protagonistas de las redes sociales son los usuarios, lo cierto es que lo son los prestadores de servicios. Si nos centramos en su funcionamiento, vemos como al darse de alta el usuario proporciona una gran cantidad de datos personales, muchos de los cuales pueden calificarse de sensibles, no proporcionándolos el usuario voluntariamente, aunque puede dar esta impresión, sino compelido por el sistema, con el fin de poder acceder a determinados servicios o aplicaciones.

Esta captación de datos tiene transcendencia respecto de la privacidad, ya que las plataformas disponen de potentes herramientas de procesamiento y análisis de los datos facilitados por los usuarios.

Además, a ello se añade la circunstancia de que en múltiples redes, los perfiles de los usuarios aparecen indexados en determinados buscadores de Internet, así como que se detecta, en términos generales, una ausencia de mecanismos que permitan controlar la edad de las personas que se conecta a las redes y evitar que accedan los menores de 14 años, sin el preceptivo consentimiento o autorización de los padres o tutores, tal como determina el Art. 13.1 y 13.4 del RLOPD. [10]

Como cierre, lo cierto es que la política de privacidad de las redes sociales es poco clara, y no se detalla con suficiente especificidad el uso que se puede hacer de datos personales, ni por supuesto de las imágenes o videos, con las consecuencias de

[10] 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. Por el cual se establece en los Artículos 13.1 y 13.4 del RLOPD lo siguiente:
13.1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores.
13.4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales.

conductas lesivas a la privacidad que se pueden producir, una vez introducidos esos datos en la red "sin control".

El control sobre esa información resulta vital, especialmente cuando se trata de datos que podemos arrepentirnos de haber publicado o no queremos que continúen siendo accesibles. El mecanismo para hacer valer el derecho al olvido es el derecho a consentir el tratamiento de datos personales y el derecho a revocar en cualquier momento ese consentimiento. A la hora de evaluar los contextos de ejercicio de este derecho, debe distinguirse entre la información publicada por uno mismo en la red social y aquella publicada por terceros y que contiene datos personales nuestros (por ejemplo, una fotografía de alguien colgada en la página de otra persona). Cuando dicha información afecta a datos personales existe un riesgo claro de que esa información descontextualizada provoque un peligro para la percepción social del sujeto al que esos datos se refieren. En el primer caso, el titular de los datos mantiene en todo caso el control sobre ellos, y el responsable del tratamiento debe acceder a eliminar todos aquellos respecto de los cuales se produce una revocación del consentimiento.

El artículo 6.3 LOPD establece que el consentimiento al tratamiento de datos puede ser revocado "cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos", y que el artículo 17.1 del Reglamento de desarrollo de la LOPD dice que esa revocación podrá efectuarse a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del tratamiento.

En un segundo caso, cuando los datos personales son publicados por un tercero en una red social, se plantea el problema de si ese tratamiento de datos está sujeto a la normativa en esta materia o si, por el contrario, está excluido del régimen de protección de datos personales, al ser considerados "ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas" [art. 2.2.a) LOPD y art. 3.2 Directiva 95/46/CE].

Esta exclusión de aplicación de la legislación de protección de datos, conocida como excepción doméstica, implica que cuando los datos de otro son objeto de tratamiento en el seno de las relaciones mantenidas dentro del círculo familiar o de amistad, no es necesario, por ejemplo, recabar el consentimiento: álbumes de fotos, recopilación de cartas o mensajes, etc., son los casos típicos en los que resulta aplicable esta excepción.

Publicar datos personales de otro en el perfil propio de una red social no cae, en principio, en el ámbito de la excepción doméstica. El Tribunal de Justicia, en el asunto Lindqvist (sentencia de 6 de noviembre de 2003, C-101/01, par. 47)[11], sostuvo que "esta excepción debe interpretarse en el sentido de que contempla únicamente las actividades que se inscriben en el marco de la vida privada o familiar de los particulares".

[11] Sentencia del Tribunal de Justicia de 6 de noviembre de 2003. Procedimiento Penal entablado contra Bodil Lindqvist. Disponible en: http://goo.gl/YMKstx

Evidentemente, no es este el caso de un tratamiento de datos personales consistente en la difusión de dichos datos por Internet de modo que resulten accesibles a un grupo indeterminado de personas.

De este modo la difusión de datos personales a través de las redes sociales está sujeta a la normativa de protección de datos, porque, por regla general, son accesibles a una pluralidad indeterminada de personas. Por ello, la publicación de fotografías u otros datos de una tercera persona precisa el consentimiento inequívoco de esta. Así lo ha expresado la AEPD en relación con las fotografías en su informe núm. 615/2008.

En cambio si el espacio de la red social se configura como cerrado, privado y solo accesible a un número determinado de personas, puede sostenerse que el tratamiento de datos que se puede efectuar en este ámbito se inscribe dentro de la esfera personal del individuo y, por tanto, no está sujeto a la legislación de protección de datos.

En este "ámbito de relación cerrado", normalmente limitado a personas que comparten lazos de amistad, el riesgo de que determinada información personal sea descontextualizada es mucho menor, porque el interesado siempre tiene el recurso de elegir sus relaciones de amistad. Sin embargo, aunque la legislación de protección de datos no sea aplicable cuando la excepción doméstica permita cubrir un determinado ámbito de interacción dentro de una red social, ello no significa que el afectado por una información compartida en ese círculo no pueda acudir a otros instrumentos para que cese la intromisión, como por ejemplo, los mecanismos de tutela del derecho a la intimidad o el honor.

4.3 Private Shield: Marco regulativo actual

Estados Unidos y la Comisión Europea llegan a un acuerdo sobre la transferencia de datos personales

El Tribunal de Justicia de la UE invalidaba el pasado 6 de octubre de 2015 una decisión de la Comisión Europea (CE) que declaraba que EEUU garantiza una protección adecuada de los datos personales y avalaba la transferencia de esa información, en una sentencia histórica que obliga a Bruselas a negociar un nuevo marco más fuerte y seguro. Tras la decisión de la UE el pasado octubre, eran miles las empresas del continente que se encontraban en un limbo legal y con su situación problemática al depender de servicios que estaban en EEUU.

Sin embargo Estados Unidos y la Comisión Europea han llegado a un "acuerdo político" en Febrero de 2016 sobre el establecimiento de un nuevo marco legal para las transferencias transatlánticas de datos personales. Este acuerdo plantea garantías de "seguridad" y "obligaciones de transparencia" por parte de las autoridades estadounidenses sobre el acceso a los datos personales de los ciudadanos europeos

cuando sean trasladados a territorio americano. Así, en el caso de que los europeos consideren que sus datos personales han sido violados en EEUU, el acuerdo les permitirá, como "último recurso", acceder a un "mecanismo de arbitraje.

El acuerdo conocido como “Private Shield” se puede desglosar en los siguientes puntos relevantes:

- **Obligaciones rigurosas para las empresas que trabajan con los datos personales de los europeos y estricta aplicación:** Las empresas estadounidenses que deseen importar datos personales desde Europa deberán comprometerse a cumplir obligaciones rigurosas en cuanto al tratamiento de datos personales y a la garantía de los derechos individuales. El Departamento de Comercio velará por que las empresas publiquen sus compromisos con arreglo a la legislación de los EE.UU. Además, toda empresa que gestione datos de recursos humanos de Europa deberá comprometerse a cumplir las decisiones adoptadas por las autoridades europeas de protección de datos.
- **Obligaciones en materia de transparencia claras para el acceso de la administración estadounidense:** Por primera vez, los Estados Unidos han concedido a la UE sólidas garantías de que el acceso de las autoridades públicas encargadas de los servicios coercitivos y de la seguridad nacional estará sujeto a limitaciones y mecanismos de supervisión claros. Estas excepciones deben utilizarse únicamente en la medida de lo necesario y de forma proporcionada. Los EE.UU. han descartado la vigilancia masiva indiscriminada de los datos personales transferidos a los EE.UU. en el marco del nuevo mecanismo. Con el objetivo de supervisar regularmente el funcionamiento del mecanismo habrá una revisión conjunta anual, que también incluirá la cuestión del acceso de la seguridad nacional. La Comisión Europea y el Departamento de Comercio de los EE.UU. llevarán a cabo la revisión e invitarán a la misma a expertos de los servicios de inteligencia de los EE.UU. y de las autoridades europeas de protección de datos.
- **Protección eficaz de los derechos de los ciudadanos de la UE con varias posibilidades de recurso:** Todos los ciudadanos que consideren que sus datos se han utilizado de forma indebida en el nuevo mecanismo disponen de varias posibilidades de recurso. Se fijan plazos para que las empresas respondan a las reclamaciones. Las autoridades europeas de protección de datos pueden remitir reclamaciones al Departamento de Comercio y a la Comisión Federal del Comercio. Se creará un nuevo Defensor del Pueblo para tratar las reclamaciones relativas al acceso por parte de las autoridades de inteligencia nacionales.

Además se incluyen reglas nuevas como:

- El derecho al “olvido”, mediante la rectificación o supresión de datos personales.

- La necesidad de “consentimiento claro y afirmativo” de la persona concernida al tratamiento de sus datos personales.
- La “portabilidad”, o el derecho a trasladar los datos a otro proveedor de servicios,
- El derecho a ser informado si los datos personales han sido pirateados.
- Lenguaje claro y comprensible sobre las cláusulas de privacidad.
- Multas de hasta el 4% de la facturación global de las empresas en caso de infracción.

El 8 de Julio de 2016 los representantes de los estados miembros de la UE votaron a favor del acuerdo UE-EEUU denominado Privacy Shield, que servirá de base para el comercio transatlántico en servicios digitales por 250.000 millones de dólares al facilitar las transferencias de datos transfronterizas que son cruciales para los negocios internacionales.

Su introducción debería poner fin a meses de incertidumbre legal para empresas como Google, Facebook y MasterCard después de que la Unión Europea invalidara el marco previo de transferencia de datos, Safe Harbour, por preocupaciones sobre espionaje por parte de Estados Unidos.

5. Protección del menor en las redes sociales

En la actualidad hay una generación de jóvenes que han nacido con un universo digital a su disposición, son conocidos como “nativos digitales”. Se trata de jóvenes que tienen un ordenador personal en sus habitaciones y que en su mayoría han sido autodidactas en el uso de las nuevas tecnologías.

Los menores encuentran una gran cantidad de herramientas tecnológicas que, salvo excepciones, nadie les ha enseñado a utilizar de forma responsable y prudente. Además gran parte de estos jóvenes navegan por la red en solitario, sin la compañía de un adulto que le oriente sobre el uso de las mencionadas herramientas. Esto es debido a factores cada vez más comunes como la falta de tiempo, la desidia parental y la cada vez mayor, brecha digital entre ambas generaciones. En este sentido, la Agencia Española de Protección de Datos ha manifestado en repetidas ocasiones que los menores de 14 años necesitan el permiso de los padres para registrarse en redes sociales y que no lo pueden hacer por sí solos.

La Decisión 1351/2008/CE del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, establece un programa comunitario plurianual sobre la protección de los niños en el uso de internet y de otras tecnologías.

"La evolución de la tecnología, la transformación de la manera en que niños y adultos utilizan internet y las demás tecnologías de la comunicación y la modificación de los comportamientos crean nuevos riesgos para los niños. Resulta necesario combinar medidas y acción de forma polifacética y complementaria, por ejemplo, mediante la adopción de medidas que fomenten el uso seguro y responsable de internet, la prosecución del desarrollo de tecnologías de apoyo, el fomento de las mejores prácticas para elaborar códigos de conducta que incluyan unos cánones de comportamiento que cuenten con la aprobación general o de la cooperación con la industria sobre objetivos concertados"[12]

En los Estados Unidos, la Children's Online Privacy Protection Act (1998) establece una serie de salvaguardas para la privacidad de los menores en Internet. De las que destacamos que no se puede recabar por Internet ninguna información o dato de carácter personal de menores de 13 años sin el permiso verificable de sus padres o representantes legales. Los cuales tienen el derecho a conocer qué información sobre sus hijos se les ha solicitado y su finalidad, así como el derecho a decidir sobre su cesión a terceros o sobre su cancelación.

Los usuarios, con una gran mayoría de menores, de forma consciente o inconsciente publican su vida al completo en la Red, denotando así un problema de falta de consciencia de que sus datos personales serán accesibles a cualquier persona y el valor que éstos pueden alcanzar en el mercado de la Red.

Éstos hacen completamente públicos datos, imágenes, videos, etc., que, en muchas ocasiones, no estarían dispuestos a exponer en su vida diaria, como pueden ser todo tipo de fotografías con posturas, gestos del rostro, signos identificativos en el cuerpo, así como otros, que pueden ser utilizados por terceros de forma ilícita con multitud de propósitos.

Lo más relevante es que, en las nunca leídas condiciones de registro aceptadas por la gran mayoría de los usuarios menores de las redes sociales, éstos están cediendo derechos plenos e ilimitados sobre todos aquellos contenidos propios que se alojen en la plataforma, de manera que pueden ser explotados económicamente por parte de la red social.

Conviene señalar, que una vez que un perfil se constituye en una red social, éste queda para el futuro, siendo realmente muy dificultosa la posibilidad de persecución legal, aunque exista la opción de denunciar.

[12] DECISIÓN No 1351/2008/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 16 de diciembre de 2008, por la que se establece un programa comunitario plurianual sobre la protección de los niños en el uso de Internet y de otras tecnologías de la comunicación.

Nos sirve de ejemplo la política de privacidad de una de las redes sociales más utilizadas a nivel global, Facebook. Sobre esta red en particular, sólo mencionar que como todo sitio en Internet, esta red social hace uso de las llamadas cookies[13]. Estos son fragmentos de información que se almacenan en el disco duro del usuario cuando accede a una página web a través de un navegador, es decir supone el almacenamiento de información relativa al usuario para poder ser utilizada en posteriores visitas al mismo sitio web y, así conocer ciertas características y preferencias del mismo.

En la política de privacidad se informa a los menores que las cookies, que la plataforma almacena, son destruidas tras la desconexión, sin embargo las almacenadas por terceros, no se encuentran bajo ningún control porque sí están autorizados para llevar a cabo esta recopilación oculta de información del propio usuario. En la práctica esto se muestra al usuario como ciertos anuncios publicitarios diseñados especialmente basados en sus gustos y en su actividad en la web.

Si nos centramos en los datos de tipo personal introducidos en el perfil que, cada usuario introduce al darse de alta en la red social se avisa, en teoría, de que éstos están disponibles para cualquier socio de la red o de redes asociadas, no sabiendo en ningún momento a qué tipo de red o de redes asociadas estamos haciendo visibles tanto datos de carácter personal como imágenes. Además se advierte que dichos datos podrán ser utilizados con fines promocionales y como material publicitario de la red.

En cuanto a la seguridad de los datos que se almacenan, no se informa al usuario de si se tiene en cuenta algún tipo de estándar en seguridad de redes o si se atiene a algún tipo de legislación, como la Ley de Protección de datos de Carácter Personal, que pueda dar unas mínimas garantías de seguridad sobre los datos personales introducidos por los usuarios de las mismas.

Lo cierto es que cuando, los usuarios vuelcan información sobre terceros, ya sean menores o no, con fotografías etiquetadas con comentarios sobre su apariencia o sobre su comportamiento, se exige el consentimiento de la persona antes de la publicación de una información personal o, con carácter previo a proceder a colgar una fotografía o video. Y es la Legislación sobre Protección de Datos la que habrá de ser respetada, sin perjuicio de la necesidad de que las redes sociales se involucren en el establecimiento de sistemas de control más potentes y efectivos, poniendo mayor énfasis en los supuestos de menores de edad.

Uno de los aspectos más relevantes que habrán de ser tenidos en cuenta para evitar conductas lesivas para el usuario, será la necesaria información y comprensión sobre las condiciones de privacidad que se establecen en las distintas redes sociales, más si cabe para los menores. Según la encuesta del CIS sobre protección de datos personales, un

[13] "Cookies". Véase el anexo I, sobre las Políticas de Privacidad en algunas de las redes sociales. Página 41.

35% de los encuestados manifestaba que nunca leía dicha política, un 27% reconocía que raramente lo hacía y un 5% confesaba que no sabía cómo hacerlo.[14]

Cuando los clientes se dan de alta es necesario que los menores comprendan que han de ser conscientes de los problemas que generan el uso indiscriminado de los datos personales en las redes, y la forma de utilización más segura.

De igual forma conviene recordar la importancia que tiene el que los proveedores de servicios de las distintas redes sociales estén atentos y sean diligentes en el cumplimiento de las Leyes sobre Protección de Datos Personales, no solamente respecto de los usuarios en general, pero de forma más estricta relación con los menores.

En definitiva, es una pérdida de control de los propios datos personales, entre otros las imágenes o vídeos, lo que no genera más que una pequeña parte para el surgimiento de terceros malintencionados en la utilización de los mismos, que pueden derivar en conductas no sólo inconsentidas, sino ilícitas.

Mención aparte merece el uso de fotografías, por un lado las imágenes son datos personales y para su utilización, lo mismo que el resto de datos, es necesario el consentimiento del titular, que en el caso de los menores de 14 años deberá estar autorizado por sus padre o tutores, lo que en caso contrario, podría constituir revelación de secretos o violaciones de la privacidad e intimidad.

Por otro lado, si son imágenes de contenido sexual pueden tener transcendencia delictiva si se trata de menores de edad con conductas que puedan estar relacionadas con la pornografía infantil; acoso sexual (Art. 184 CP); exhibicionismo obsceno y provocación sexual (Art. 185 y 186 CP); corrupción de menores (Art. 187 CP); o pueden tipificar el “sexting” o intercambio de imágenes sugerentes, con imágenes robadas o entregadas de forma privada que pueden ser sumamente nocivas cuando pasan al dominio público, vulnerando la intimidad y privacidad de la víctima que queda desprotegida a merced de cualquier agresión o acoso, como el ciberbullying, que constituye uno de los principales peligros para los menores en Internet con resultados emocionalmente devastadores, cuyo aumento de potencialidad lesiva en las redes sociales podría constituir un delito contra la integridad moral.

El uso de las tecnologías de la comunicación y de la información en el ciberacoso ofrece cuatro nuevas dimensiones que deben ser analizadas para comprender los posibles daños e identificar medidas que los eviten o los contrarresten:

Los sistemas de utilización de Internet y las redes sociales permiten que las personas que llevan a cabo los acosos se beneficien de un anonimato prácticamente absoluto

[14] Centro de Investigación Sociológica (CIS). Encuesta sobre protección de datos, 2009

proporcionado por los servicios online, puesto que no requieren una identificación sólida, ni tan siquiera un simple registro, ofreciendo a estos individuos una posición de "inmunidad"

Se deberían garantizar que las plataformas de las distintas redes sociales, deban dar cumplimiento estricto a la Legislación de protección de datos. Para ello se debe mantener un equilibrio entre el uso lesivo de los datos personales y los que permiten la utilización efectiva de la publicidad, con los ingresos que de ello se genera.

Los proveedores de las plataformas tienen la posibilidad de limitar técnicamente determinadas capacidades que las mismas ofrecen en la actualidad, como la difusión de fotografías de personas que al ser colgadas y compartidas por los usuarios menores en Red, son puestas de forma instantánea en conocimiento del público en general.

Otra nota que facilita la existencia de acosadores y la dificultad de la trazabilidad de sus actuaciones, es la memoria de datos que persiste en Internet en lo que se refiere a la información utilizada para el acoso. Actualmente, una vez que la información de un acosado consta en Internet, es muy difícil su borrado. Por tales motivos, igualmente será necesario un escrupuloso respeto de la Legislación sobre Protección de Datos Personales, y la articulación de las herramientas técnicas necesarias.

Corresponde a las redes sociales configurar un entorno seguro para aquellos usuarios que como los menores de edad resultan especialmente vulnerables. Por ello, además de evitar la indexación de la información personal de los menores debe determinar una publicidad restringida para el perfil personal de estos usuarios, establecer el acceso por invitación, o actuar frente a la denuncia de actuaciones ofensivas o perjudiciales.

Se deben reforzar las medias de seguridad, especialmente en lo que afecta al control de edad, con la implantación de protocolos de control de la edad de los usuarios, con ágiles botones de denuncia de actuaciones abusivas o irrespetuosas, o con el diseño y redacción de políticas de privacidad.

En este contexto, destaca la actuación de Tuenti, esta plataforma española implantó en abril de 2009 un proceso de depuración de los perfiles de menores de 14 años[15], por el cual en los casos de perfiles que aparentan ser menores de 14 años se les envía desde la red social una solicitud para que aporten fotocopia del DNI o pasaporte en plazo inferior a 92 horas, y en el caso de no recibir respuesta, se advierte al usuario que su perfil será borrado. De igual forma, Tuenti ha realizado un cambio de configuración de los perfiles de menores de 18 años, que por defecto tendrán el grado de privacidad máximo.

[15] Véase el Anexo II, sobre Políticas de privacidad en la red social Tuenti, punto 3 "Edad mínima y calidad de los datos". Página 46.

6. Casos prácticos

Google y el derecho al olvido

Gran parte de la sociedad no había oído hablar del derecho al olvido hasta el caso Google. Este sirvió como reivindicación del mismo y sentó precedentes para futuros casos.

Este derecho adquiere importancia desde el momento en que basta teclear el nombre de alguien para que aparezca información relativa a esa persona y que en algunos casos puede atentar contra el derecho al honor, a la intimidad y a la propia imagen del individuo, y en definitiva vulnerar el derecho a la protección de datos. La rapidez en la obtención de esa información ha provocado que salten las alarmas.

En el caso de los buscadores como Google, exploran Internet de manera automatizada, constante y sistemática en busca de la información que se publica en la Red. El gestor del motor de búsqueda recoge tales datos, los extrae, registra y organiza en sus programas de indexación y los conserva en sus servidores, facilitando el acceso a los usuarios de tales buscadores en forma de listas de resultado.

Surgen varias cuestiones problemáticas con la conservación y publicidad de estos datos.

"Cometí un delito en el pasado y quiero rehacer mi vida"

Este podría ser el caso de cualquiera, que por una u otra razón cometió un delito en el pasado, por el que cumplió la pena que un juez le impuso y que habiendo transcurrido el tiempo por el que prescriben los antecedentes penales desde el cumplimiento de la pena, sigue apareciendo su nombre vinculado a ese lamentable acontecimiento mediante un enlace a un artículo de prensa digital.

¿Cómo podría esa persona obtener un empleo, por ejemplo, si al teclear su nombre en Google aparece la noticia de la comisión de un delito? ¿Debería esa persona estar "marcada" para siempre?

"Colgué unas fotos de borrachera y aparezco en google"

¿A quién no le ha pasado que en alguna fiesta ha bebido algo más de la cuenta? Mientras que antes solo se enteraban los presentes, ahora sin embargo, siempre hay un móvil con cámara que capta imágenes vergonzosas o fuera de lugar que luego se publican.

¿Es necesario que Google esté obligado a dejar de indexar esas imágenes? ¿O tenemos que ver que una persona tuvo un desfase en una ocasión siempre que pongamos su nombre en el buscador?

La sentencia del tribunal de justicia de la unión europea (TJUE) contra Google

El 13 de mayo de 2014, el Tribunal de Justicia de la Unión Europea dictó la sentencia contra Google en materia de protección de datos personales, considerando que ese buscador (y por ende todos) realizan labores de tratamiento de datos.

El camino hasta obtener tal resolución fue largo, porque el procedimiento lo inició el 5 de marzo de 2010, D. Mario Costeja Fernández, que presentó ante la Agencia Española de Protección de Datos una reclamación contra La Vanguardia Ediciones, S.L., contra Google Spain y Google Inc., alegando que cuando introducía su nombre en el motor de búsqueda de Google, obtenía como resultado vínculos del periódico La Vanguardia, del 19 de enero y del 9 de marzo de 1998, en las que aparecía un anuncio de una subasta de inmuebles a causa de un embargo por deudas a la Seguridad Social. Dicho embargo, en el momento de la reclamación, al parecer, estaba totalmente solventado, careciendo por tanto de relevancia dicha información.

Mediante esta reclamación, el Sr. Costeja González solicitaba, que se exigiese a La Vanguardia eliminar o modificar la publicación para que no apareciesen sus datos personales. Solicitaba también que se exigiese a Google España o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia.

La Agencia Española de Protección de Datos (AEPD) desestimó la reclamación contra la Vanguardia, pues la publicación había tenido lugar de forma legal por orden del Ministerio de Trabajo y Asuntos Sociales. En cambio, se estimó la reclamación dirigida contra Google España y Google Inc., interponiendo estas compañías sendos recursos contra dicha resolución ante la Audiencia Nacional, que decidió acumularlos, suspender el procedimiento y plantear al Tribunal de Justicia una serie de cuestiones prejudiciales que resuelven en la Sentencia sobre la indexación de datos en Internet relativos a una persona.

La sentencia

En dicha sentencia se declara por el Tribunal de Justicia de la Unión Europea lo siguiente:

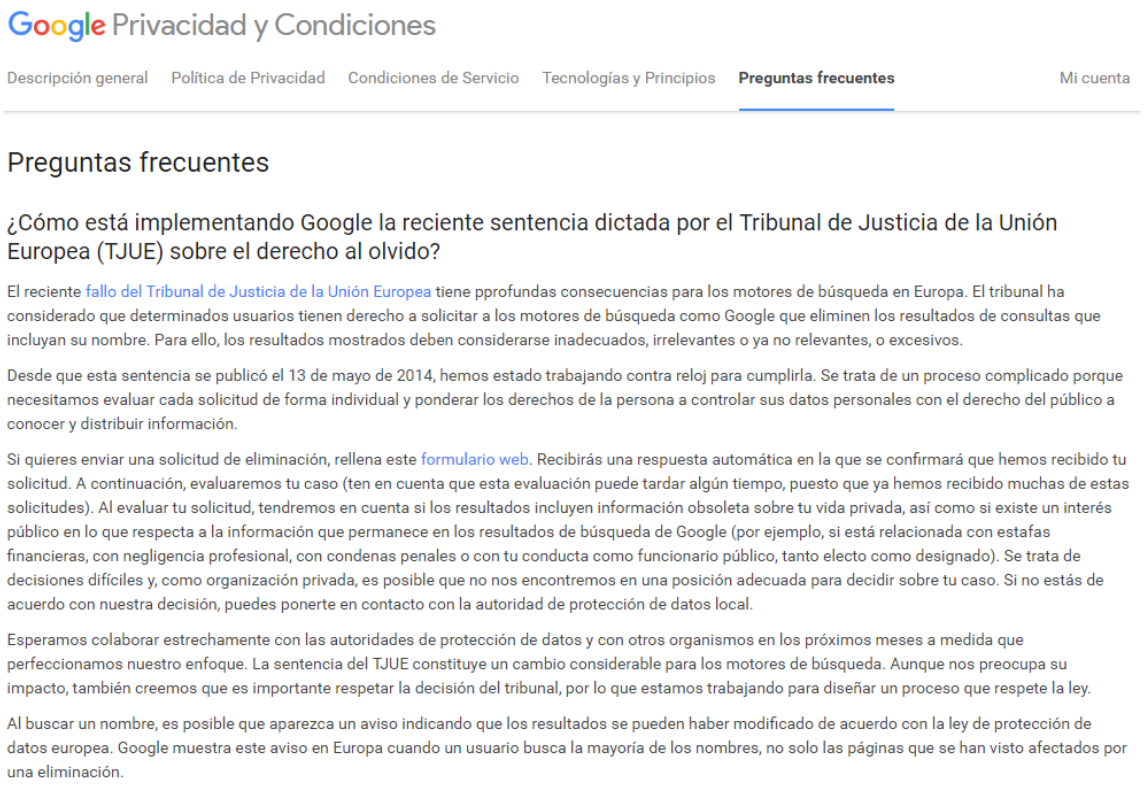
Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, interpreta que la actividad de un motor de búsqueda de recoger información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y ponerla a disposición de los internautas según un orden de preferencia determinado, debe calificarse de “tratamiento de datos personales”, siempre que la información contenga datos personales y por lo tanto es el responsable de dicho tratamiento.

El gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona, vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona.

Además se establece que se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre.

Reacción de Google

Este conocido motor de búsqueda publicó una página en sus FAQ's (preguntas frecuentes) en la que se responde a la pregunta ¿Cómo está implementando Google la reciente sentencia dictada por el Tribunal de Justicia de la Unión Europea (TJUE) sobre el derecho al olvido?, afirmando que se encuentran trabajando a contrarreloj para cumplirla, y que se trata de un proceso complicado, pues necesitan evaluar cada solicitud de forma individual.



Google Privacidad y Condiciones

Descripción general | Política de Privacidad | Condiciones de Servicio | Tecnologías y Principios | **Preguntas frecuentes** | Mi cuenta

Preguntas frecuentes

¿Cómo está implementando Google la reciente sentencia dictada por el Tribunal de Justicia de la Unión Europea (TJUE) sobre el derecho al olvido?

El reciente fallo del Tribunal de Justicia de la Unión Europea tiene pprofundas consecuencias para los motores de búsqueda en Europa. El tribunal ha considerado que determinados usuarios tienen derecho a solicitar a los motores de búsqueda como Google que eliminen los resultados de consultas que incluyan su nombre. Para ello, los resultados mostrados deben considerarse inadecuados, irrelevantes o ya no relevantes, o excesivos.

Desde que esta sentencia se publicó el 13 de mayo de 2014, hemos estado trabajando contra reloj para cumplirla. Se trata de un proceso complicado porque necesitamos evaluar cada solicitud de forma individual y ponderar los derechos de la persona a controlar sus datos personales con el derecho del público a conocer y distribuir información.

Si quieres enviar una solicitud de eliminación, rellena este formulario web. Recibirás una respuesta automática en la que se confirmará que hemos recibido tu solicitud. A continuación, evaluaremos tu caso (ten en cuenta que esta evaluación puede tardar algún tiempo, puesto que ya hemos recibido muchas de estas solicitudes). Al evaluar tu solicitud, tendremos en cuenta si los resultados incluyen información obsoleta sobre tu vida privada, así como si existe un interés público en lo que respecta a la información que permanece en los resultados de búsqueda de Google (por ejemplo, si está relacionada con estafas financieras, con negligencia profesional, con condenas penales o con tu conducta como funcionario público, tanto electo como designado). Se trata de decisiones difíciles y, como organización privada, es posible que no nos encontremos en una posición adecuada para decidir sobre tu caso. Si no estás de acuerdo con nuestra decisión, puedes ponerte en contacto con la autoridad de protección de datos local.

Esperamos colaborar estrechamente con las autoridades de protección de datos y con otros organismos en los próximos meses a medida que perfeccionamos nuestro enfoque. La sentencia del TJUE constituye un cambio considerable para los motores de búsqueda. Aunque nos preocupa su impacto, también creemos que es importante respetar la decisión del tribunal, por lo que estamos trabajando para diseñar un proceso que respete la ley.

Al buscar un nombre, es posible que aparezca un aviso indicando que los resultados se pueden haber modificado de acuerdo con la ley de protección de datos europea. Google muestra este aviso en Europa cuando un usuario busca la mayoría de los nombres, no solo las páginas que se han visto afectados por una eliminación.

Nos indican que para realizar la solicitud de eliminación hay que rellenar un formulario web, advirtiéndonos que puede que el trámite tarde un tiempo, pues ya han recibido muchas solicitudes.

En resumen, una vez recibida la solicitud Google evaluará si efectivamente se trata de información obsoleta de la persona del solicitante y si es lesiva a sus intereses, ponderando si existe un interés público en lo que respecta a la información que permanece en los resultados de búsqueda, decidiendo de forma unilateral si deja de indexar esa información.

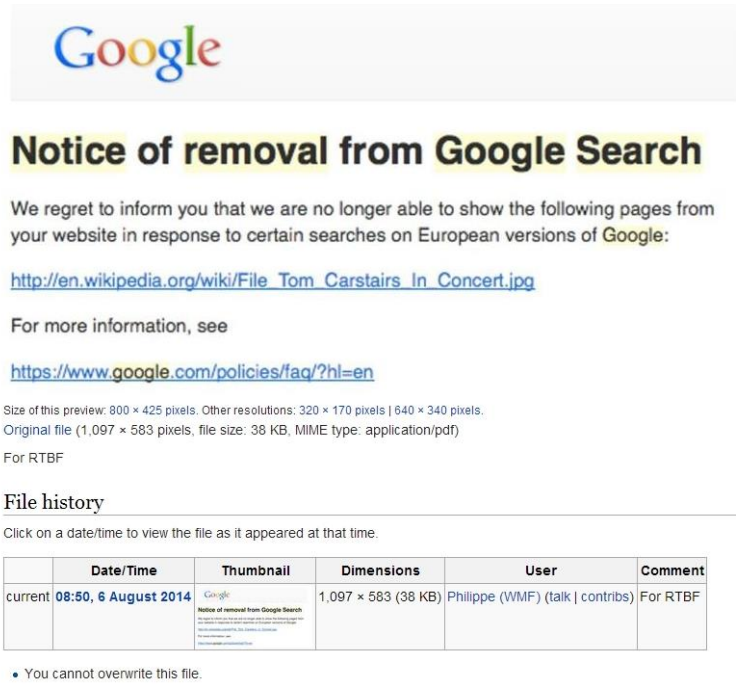
Por lo tanto, es Google el que decide. No existe otro mecanismo que no sea acudir a las autoridades de cada país en materia de protección de datos o a los tribunales.

Reacciones externas al caso Google por el derecho al olvido

La sentencia de la Justicia europea del caso que se enfrentaba a Google España por el derecho al olvido está afectando también a la Wikipedia. La enciclopedia ha visto cómo el buscador ha eliminado de sus resultados más de 50 enlaces a sus artículos. Durante la presentación de su Informe de Transparencia, los responsables de la Fundación Wikipedia denunciaron que la decisión judicial es un golpe a la libertad de conocimiento y rechazan borrar los artículos desaparecidos de Google.

Desde entonces y hasta mediados de julio del 2014, Google ha recibido más de 91.000 peticiones de retirada de referencias que afectaban a 328.000 direcciones únicas de páginas web (URL). El buscador ha accedido a retirar el 53% de ellas. Algunas hacían referencia a informaciones aparecidas en periódicos españoles como El Mundo o La Vanguardia. Ahora se ha sabido que la Wikipedia también se ha visto afectada.

Durante la presentación en Londres de su primer Informe de Transparencia, la Fundación Wikimedia, responsable de la Wikipedia, desveló que más de 50 enlaces a artículos de la enciclopedia habían sido retirados por Google de sus resultados de búsqueda. Aunque 50 enlaces no parecen muchos entre tantos miles, para la directora ejecutiva de la Fundación Wikimedia, Lila Tretikov, la aplicación de la sentencia "está minando la capacidad de la gente de acceder libremente a registros precisos y verificables sobre personas y acontecimientos". Para ella, "el impacto en la Wikipedia es directo y crítico".



Google

Notice of removal from Google Search

We regret to inform you that we are no longer able to show the following pages from your website in response to certain searches on European versions of Google:

http://en.wikipedia.org/wiki/File_Tom_Carstairs_In_Concert.jpg

For more information, see

https://www.google.com/policies/faq/?hl=en

Size of this preview: 800 × 425 pixels. Other resolutions: 320 × 170 pixels | 640 × 340 pixels.
Original file (1,097 × 583 pixels, file size: 38 KB, MIME type: application/pdf)

For RTBF

File history

Click on a date/time to view the file as it appeared at that time.

	Date/Time	Thumbnail	Dimensions	User	Comment
current	08:50, 6 August 2014		1,097 × 583 (38 KB)	Philippe (WMF) (talk | contribs)	For RTBF

• You cannot overwrite this file.

Aviso de Google a Wikipedia de la retirada de su buscador de uno de sus artículos de su edición inglesa / Wikipedia

Tras la sentencia, Google habilitó una página web en la que los interesados pueden solicitar la retirada de contenido que pudiera afectar a su derecho a la privacidad. El buscador revisa manualmente cada petición y, como indicaba la resolución judicial, caso por caso. A la hora de retirar un resultado de su buscador, Google tiene en cuenta cómo puede afectar al derecho a la información. Otros criterios a tener en cuenta son el carácter público o no del interesado, si la información denunciada es antigua o ha dejado de ser pertinente. El ejemplo típico es el tratado anteriormente de Mario Costeja, el español que consiguió que se le reconociera su derecho al olvido por un asunto de la subasta de un inmueble por impago de 1998 en el que la deuda ya estaba saldada.

Sin embargo, la Wikipedia no admite excepciones a su defensa del libre conocimiento.

“Al hacer esto, el tribunal europeo ha abandonado su responsabilidad en la protección de uno de los derechos más importantes e universales: el derecho a saber, recibir y difundir la información”, escribe Tretikov en el blog de la Fundación Wikimedia.

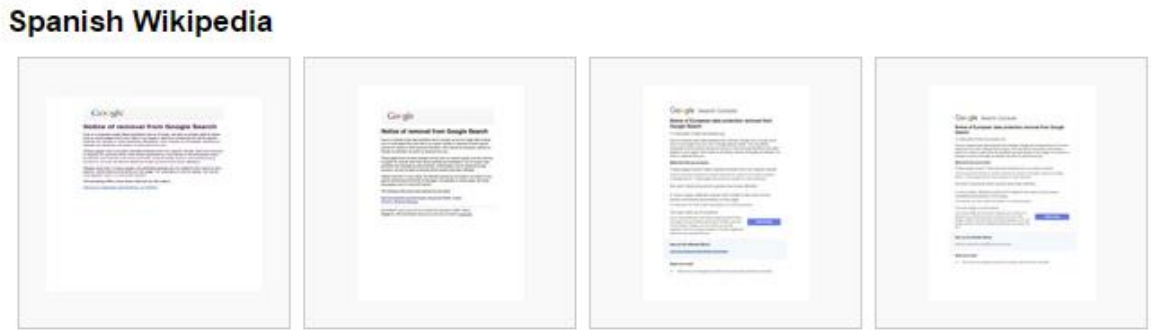
“En consecuencia, resultados de búsqueda rigurosos están desapareciendo en Europa sin ninguna explicación pública, ninguna prueba real, sin revisión judicial y ningún proceso de apelación. El resultado es una internet plagada de agujeros de memoria, lugares donde la información inconveniente simplemente desaparece”.

En realidad, la información no desaparece de internet, sólo lo hace de Google. De hecho, los artículos borrados del buscador siguen estando en Wikipedia y sus responsables ya

han dicho que no piensan borrarlos. Si alguien tiene que borrar cualquier información deberían ser los editores del contenido.

Ejemplos de derecho al olvido en la Wikipedia

La Fundación Wikimedia ha creado una página donde recopila los avisos que ha recibido y los clasifica por el país donde han sido publicados. Por ejemplo, en el caso de España observamos 4 avisos.



Cuatro publicaciones, en el caso de España, que Google ha borrado de la Wikimedia

Analizando dos casos (uno italiano y uno que no se llegó a producir) muestra lo complejo que puede ser la aplicación en la práctica del derecho al olvido.

Google ha avisado a Wikipedia que dos de sus artículos de su versión italiana sobre una banda de delincuentes comunes ya no van a aparecer en los resultados del buscador. Se trata de las entradas sobre la banda della Comasina y su jefe, Renato Vallanzasca. Durante los años 70 del siglo pasado asaltaron bancos y joyerías. Ya en prisión, Vallanzasca protagonizó varias fugas y motines donde murieron varias personas. El jefe de la banda della Comasina, con varias condenas a cadena perpetua, sigue en prisión.

Por el contrario, el caso de Gerry Hutch es totalmente diferente. Acusado, aunque nunca condenado, de dos de los mayores robos del siglo XX en Irlanda, Hutch pasó varios años en la cárcel por otros delitos. En prisión descubrió la espiritualidad y al salir de ella consiguió enderezar su vida como taxista. Incluso los editores de la Wikipedia discutieron la posibilidad de borrar la entrada sobre Hutch debido a su reinserción. Pero dicho borrado nunca se produjo. La comparativa de ambos casos refleja perfectamente la complejidad sobre la elección de los casos idóneos para aplicar el derecho al olvido.

Google Maps

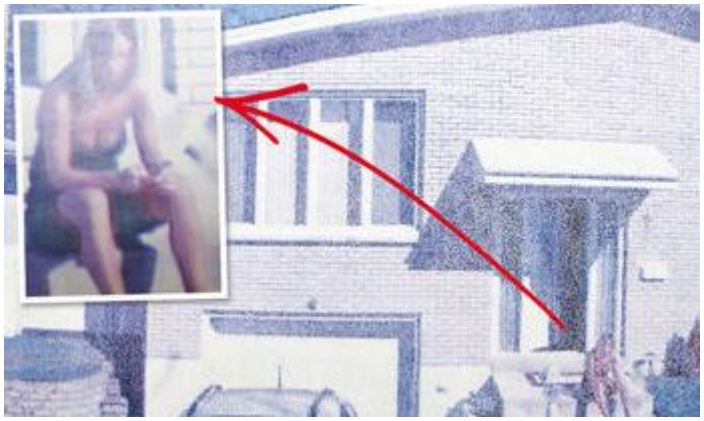
Son muchas las personas que han visto pasar los famosos coches de Google con la cámara arriba que toma fotografías de las diferentes calles de todas las ciudades para integrarlas a Google Street Maps. En algunas de estas fotos que aparecen en estos mapas de internet, aparecen personas que están en ese lugar en ese preciso momento. Es por ello que, aún y cuando se borra su rostro, estas personas han solicitado que la empresa los retire por distintas razones.

Esto se considera un claro ejemplo del derecho al olvido que hemos visto anteriormente.

El caso

En Montreal, una mujer estaba sentada afuera de su casa usando su smartphone cuando se tomó la foto para el mapa. Cuando se buscó en Google Maps se dio cuenta de que por la posición salía mostrando su escote, algo que consideró un abuso.

Esta es la foto en cuestión:



Esta mujer entabló una demanda contra Google y exigió el pago de cierta cantidad en modo de compensación puesto que se consideró un abuso a su privacidad y dignidad, de igual modo, también se estableció que borrar la cara de alguien no lo hace irreconocible.

7. Conclusiones

I. El usuario debe ser el primer interesado en la defensa de su privacidad, para ello debe tener una actividad online responsable y actuar con cautela con la información que no quiere hacer pública. Es importante trabajar en este asunto, puesto que, gran cantidad de estudios demuestran que es el propio usuario el que facilita el acceso y comercio de sus datos personales debido a un exceso de confianza en las redes sociales.

II. Aunque no se pueden desdeñar los problemas derivados del uso de las redes sociales en cuanto a la privacidad del usuario, es conveniente valorar el gran avance que suponen estas tecnologías en la comunicación entre las personas y no por los problemas comentados se debe limitar su uso.

III. En los aspectos más técnicos estas tecnologías tan importantes como son los buscadores y editores de información online, deben regirse por la legislación de un modo riguroso para no perjudicar a los usuarios y por ende, no criminalizar su producto de mercado. En especial, aquellas empresas que tienen servicios por todo el mundo y, por tanto, se rigen por diferentes legislaciones en cuanto a la privacidad y el tratamiento de datos personales, puesto que esta no es homogénea en la mayoría de ocasiones.

IV. Más específicamente, los buscadores deben de dejar de indexar todos los datos susceptibles de dañar de forma injusta la imagen de una persona. Como hemos visto en este trabajo, no se encuentran en una posición de neutralidad porque usen algoritmos matemáticos, sino que, tienen un gran poder sobre la filtración de información que afecte a la reputación de una persona.

V. Los editores de información deben tener una actitud responsable y respetar la intimidad y vida personal de cualquier usuario en la red, respetando y cumpliendo el derecho al olvido y valorando el daño que puede ocasionar cierta información en la vida de una persona, al igual que tener en cuenta que la información en la web no “caduca” y normalmente se mantiene con el paso del tiempo.

VI. En el sentido legislativo, la protección de la privacidad en la web se debe mantener totalmente actualizada teniendo en cuenta que el contexto digital donde se engloba cambia a un velocidad de vértigo. En este sentido, se da por cumplido, puesto que apenas días antes de la finalización de este trabajo se ha llegado a un importante acuerdo sobre el trasvase de datos personales entre USA

y la UE, al igual que la aprobación del Reglamento General de Datos de la Unión Europea mejorando en gran medida los derechos de los usuarios en este ámbito.

VII. Es muy importante tener una regulación especial sobre los menores, sin duda el público más sensible, como ya hemos analizado anteriormente no tienen la formación adecuada ni mucho menos la cautela necesaria en este tipo de servicios. Por ello, se recomienda trabajar en una formación especializada y potenciar el interés de sus padres o tutores para hacer un uso responsable de los servicios online y concienciar de los peligros que entraña su uso.

VIII. Los proveedores de servicios tienen gran parte de responsabilidad en el tema de menores, puesto que es su obligación tener mecanismos eficaces que regulen su uso (política de Tuenti). Actualmente, estos proveedores son obligados a cuidarse con políticas de privacidad y de acceso pero aún, se considera que es extremadamente fácil para un menor tener un perfil en una red social y tener una actividad sin ninguna restricción.

8. Bibliografía

- Antón, Ana María Gil. 2012. «El fenómeno de las redes sociales y los cambios en la vigencia de los derechos fundamentales». *Revista de Derecho UNED*, n.º 10: 209.

- Barriuso Ruiz, Carlos. 2009. «Las redes sociales y la protección de datos hoy». Disponible en: http://dspace.uah.es/dspace/handle/10017/6447. [Consultado el 1 de Julio de 2016]

- Cádima, Francisco Rui. 2015. «El control de Internet y de las "voces liberadas" en la emergencia del paradigma digital». *Historia y comunicación social* 20 (2): 413-25.

- De Mata, Federico Bueno, Erica Yamel Munive Cortés, y Humberto Martín Ruani. 2014. «Estudio comparativo entre España, México y Argentina sobre la protección del menor en las redes sociales». *Revista de Estudos Constitucionais, Hermenêutica e Teoria do Direito* 6.

- Espinosa, María Paz Prendes, Isabel Gutiérrez Porlán, y Linda Johanna Castañeda Quintero. 2015. «Perfiles de uso de redes sociales: estudio descriptivo con alumnado de la Universidad de Murcia». *Revista complutense de educación* 26 (1): 175-95.

- European Commission - PRESS RELEASES - Press release - La Comisión Europea y los Estados Unidos acuerdan un nuevo marco para los flujos transatlánticos de datos: Escudo de la privacidad UE - EE.UU. 2016. Disponible en: http://europa.eu/rapid/press-release_IP-16-216_es.htm. [Consultado el 11 de julio de 2016]

- Fullana, Antonia Paniza. 2009. «Redes sociales, derechos de los usuarios y privacidad». *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, n.º 41: 3-.

- García, Lorena Rodríguez, y José Rafael Magdalena Benedito. 2016. «Perspectiva de los jóvenes sobre seguridad y privacidad en las redes sociales.» *Icono14* 14 (1): 24-49.

- Membrado, Cristina Gil. 2015. «El consentimiento en las redes sociales», 105-35.

- Mieres Mieres, Luis Javier. 2014. *El derecho al olvido digital*. Madrid: Fundación Alternativas.

- Mitjans Perelló, Esther. 2009. «Impacto de las redes sociales en el Derecho a la protección de datos personales». Disponible en: http://dspace.uah.es/dspace/handle/10017/6439. [Consultado el 15 de Junio de 2016].

- Ortiz, Ana Isabel Herrán. 2010. «Las redes sociales digitales: ¿hacia una nueva configuración de los derechos fundamentales en Internet?» *Revista Vasca de Administración Pública. Herri-Arduralaritzako Euskal Aldizkaria*, n.º 87: 521-66.

- Pablo, Aparicio Vaquero, Juan, y Batuecas Caletrío Alfredo, eds. 2015. *En torno a la privacidad y la protección de datos en la sociedad de la información*. Comares. Disponible en: https://dialnet.unirioja.es/servlet/libro?codigo=580466. [Consultado el 15 de Junio de 2016]

- Portas, Vicente Guasch. 2015. «El derecho al olvido en internet/the right to be forgotten in internet». *Revista de Derecho UNED*, n.º 16: 989.

- Ramiro, Mónica Arenas. 2010. «"Derecho y Redes sociales" de Artemi Rallo Lombarte, Ricard Martínez Martínez (Coords.)». Anuario de la Facultad de Derecho, n.º 3: 571-78.

- Reigada, Antonio Troncoso. 2012. «Las redes sociales a la luz de la propuesta de Reglamento general de protección de datos personales. Parte uno». *IDP. Revista de Internet, Derecho y Política*, n.º 15: 61–75.

- Roig, Antonio. 2009. «E-privacidad y redes sociales». *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política*, n.º 9: 8.

- Sentencia del Tribunal de Justicia de 6 de noviembre de 2003. Procedimiento Penal entablado contra Bodil Lindqvist. Disponible en: http://goo.gl/YMKstx [Consultado el 11 de julio de 2016]

9. Apéndices

9.1 Apéndice legislativo

Leyes y sentencias	Disponible en
La Ley de Protección de Datos R.D. 1720/2007 (LOPD)	https://www.boe.es/buscar/act.php?id=BOE-A-2008-979
Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.	https://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750
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.	https://www.boe.es/buscar/doc.php?id=BOE-A-2008-979
Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico	https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758
Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.	https://www.boe.es/buscar/act.php?id=BOE-A-2003-20253
Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.	https://www.boe.es/buscar/act.php?id=BOE-A-2007-18243
Ley 59/2003, de 19 de diciembre, de firma electrónica.	https://www.boe.es/buscar/act.php?id=BOE-A-2003-23399
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 respeta al tratamiento de datos personales y a la libre circulación de estos datos.	https://www.boe.es/buscar/doc.php?id=DOUE-L-1995-81678
REGLAMENTO (UE) 2016/631 DE LA COMISIÓN de 14 de abril de 2016	https://www.boe.es/doue/2016/112/L00001-00068.pdf
SENTENCIA DEL TRIBUNAL DE JUSTICIA (Gran Sala) de 13 de mayo de 2014	http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=ES
30.ª Conferencia Internacional de Autoridades de Protección de Datos y privacidad, Resolución sobre la protección	https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Cooperation/Conference_int/08-10-

de la privacidad en los servicios sociales, Estrasburgo, 15-17 de octubre de 2008.	17_Strasbourg_social_network_ES.pdf
Sentencia del Tribunal de Justicia de 6 de noviembre de 2003. Procedimento penal entablado contra Bodil Lindqvist.	http://curia.europa.eu/juris/liste.jsf?language=es&num=C-101/01

10. Anexos

I. Política de privacidad referente a las redes sociales

Facebook y su política de Cookies.

Cookies y otras tecnologías de almacenamiento

Las cookies son pequeños fragmentos de texto utilizados para almacenar información sobre navegadores web. Se utilizan para almacenar y recibir identificadores, así como otra información sobre ordenadores, teléfonos y otros dispositivos. Otras tecnologías, incluidos datos que almacenamos sobre tu navegador web o dispositivo, identificadores asociados a tu dispositivo y otro software, se utilizan con fines similares. A efectos de esta política, todas estas tecnologías reciben el nombre de "cookies".

Utilizamos cookies si tienes una cuenta de Facebook, usas los servicios de Facebook, incluidos nuestro sitio web y nuestras aplicaciones (independientemente de que te registres o no, o de que inicies o no sesión), o visitas otros sitios web y aplicaciones que utilizan los servicios de Facebook (incluidos el botón "Me gusta" o nuestras herramientas de publicidad). En esta política se explica el uso que hacemos de las cookies y las opciones de las que dispones.

¿Por qué utilizamos cookies?

Las cookies nos ayudan a prestar, proteger y mejorar los servicios de Facebook, por ejemplo, personalizando el contenido, adaptando anuncios y midiendo su rendimiento, así como brindando una mayor seguridad. Aunque las cookies que utilizamos pueden cambiar de vez en cuando al mejorar y actualizar los servicios de Facebook, suelen dividirse en las siguientes categorías de uso:

- Autenticación

Utilizamos cookies para verificar tu cuenta y determinar cuándo inicias sesión, con el fin de ayudarte a acceder a los servicios de Facebook y mostrarte la experiencia y las funciones correspondientes.

Por ejemplo: utilizamos cookies para mantener tu sesión abierta mientras navegas entre páginas de Facebook. Las cookies también nos ayudan a recordar tu navegador, de tal modo que no tengas que iniciar sesión en Facebook constantemente y puedas hacerlo fácilmente mediante aplicaciones y sitios web de terceros.

- Seguridad e integridad de los sitios y productos

Utilizamos cookies para proteger tu cuenta, tus datos y los servicios de Facebook.

Por ejemplo: las cookies pueden ayudarnos a identificar e imponer medidas extras de seguridad en caso de que alguien intente acceder a una cuenta de Facebook sin

autorización, por ejemplo, adivinando rápidamente diferentes contraseñas. También utilizamos cookies para almacenar información que nos permita recuperar tu cuenta en caso de que olvides tu contraseña o para exigir información adicional de autenticación si nos indicas que te han pirateado la cuenta.

También utilizamos cookies para luchar contra actividades que infrinjan nuestras políticas o minen de cualquier otro modo nuestra capacidad para prestar los servicios de Facebook.

Por ejemplo: las cookies nos ayudan a combatir el spam y los ataques de phishing al permitirnos identificar los ordenadores utilizados para crear un gran número de cuentas de Facebook falsas. También usamos cookies para detectar ordenadores infectados con malware y adoptar medidas que impidan que provoquen daños mayores. Las cookies también nos ayudan a impedir que menores de edad se registren en Facebook.

- Publicidad, estadísticas y medición

Utilizamos cookies para mostrar anuncios de empresas y otras organizaciones a personas que pueden estar interesadas en los productos, los servicios o las causas que promocionan.

Por ejemplo: las cookies nos permiten mostrar anuncios a personas que hayan visitado anteriormente el sitio web de una empresa, comprado sus productos o utilizado sus aplicaciones. Asimismo, nos permiten limitar el número de veces que se muestra un anuncio, de tal modo que no veas el mismo una y otra vez.

También utilizamos cookies para medir el rendimiento de las campañas publicitarias de empresas que utilizan los servicios de Facebook.

Por ejemplo: utilizamos cookies para contar el número de veces que se muestra un anuncio y calcular su coste. También utilizamos cookies para medir la frecuencia con la que se realizan determinadas acciones, como hacer clic en un anuncio o visualizarlo.

Las cookies nos ayudan a mostrar y medir anuncios en diferentes navegadores y dispositivos utilizados por la misma persona.

Por ejemplo: podemos utilizar cookies para impedir que veas el mismo anuncio una y otra vez en los diferentes dispositivos que utilices.

Las cookies también nos permiten proporcionar estadísticas sobre las personas que utilizan los servicios de Facebook, y sobre las personas que interactúan con los anuncios, los sitios web y las aplicaciones de nuestros anunciantes y de las empresas que utilizan los servicios de Facebook.

Por ejemplo: utilizamos cookies para ayudar a las empresas a conocer qué tipo de personas indican que les gusta su página de Facebook o utilizan sus aplicaciones, de tal

modo que puedan ofrecer contenido más relevante y desarrollar funciones con mayores probabilidades de interesar a sus clientes.

También utilizamos cookies para ayudarte a indicar que no quieres ver anuncios de Facebook en función de tu actividad en sitios web de terceros.

- Funciones y servicios para sitios

Utilizamos cookies para habilitar las funciones que nos ayudan a prestar los servicios de Facebook.

Por ejemplo: las cookies nos ayudan a almacenar preferencias, conocer cuándo has visto contenido de servicios de Facebook o interactuado con él, y ofrecerte contenido y experiencias personalizadas. Por ejemplo, nos permiten realizaros a ti y a otras personas sugerencias, y personalizar el contenido de sitios de terceros que integren nuestros plugins sociales. Si eres administrador de una página, las cookies te permiten publicar en nombre de tu cuenta personal de Facebook o de tu página.

También utilizamos cookies con el fin de ofrecerte contenido relevante para tu configuración regional.

Por ejemplo: almacenamos información en una cookie colocada en tu navegador o dispositivo para que veas el sitio en tu idioma preferido.

- Rendimiento

Utilizamos cookies para ofrecerte la mejor experiencia posible.

Por ejemplo: las cookies nos ayudan a dirigir el tráfico entre los servidores y a saber con cuánta rapidez se cargan los servicios de Facebook para cada persona. También nos ayudan a registrar la relación de aspecto y las dimensiones de tu pantalla y tus ventanas, y a saber si tienes habilitado el modo de contraste alto, para que podamos mostrar correctamente nuestros sitios y aplicaciones.

- Análisis y estudios

Utilizamos cookies para conocer mejor cómo se utilizan los servicios de Facebook, con el fin de mejorarlos.

Por ejemplo: las cookies nos ayudan a conocer cómo se utilizan los servicios de Facebook, analizar qué partes de los servicios resultan más útiles e interesantes, e identificar funciones susceptibles de mejora.

¿Cómo utilizamos las cookies?

Podemos colocar cookies en tu ordenador o dispositivo y recibir información almacenada en ellas cuando utilices o visites:

- Los servicios de Facebook.
- Servicios prestados por miembros del grupo de empresas de Facebook.
- Servicios prestados por otras empresas que utilicen los servicios de Facebook (por ejemplo, empresas que incorporen el botón "Me gusta" o servicios publicitarios de Facebook en sus sitios web o aplicaciones).

También podemos definir y recibir información almacenada en cookies de otros dominios utilizados por el grupo de empresas de Facebook, incluidos "adtmt.com", "liverail.com" e "Instagram.com".

¿Utilizan otras partes cookies con relación a servicios de Facebook?

Sí, otras partes pueden utilizar cookies en los servicios de Facebook para prestarnos servicios a nosotros y a las empresas que se anuncian en Facebook.

Por ejemplo, nuestros socios de medición utilizan cookies en los servicios de Facebook para ayudar a los anunciantes a conocer la eficacia de sus campañas publicitarias de Facebook y a comparar el rendimiento de dichas campañas con el de anuncios mostrados en otros sitios web y aplicaciones. Obtén más información sobre las empresas que utilizan cookies en los servicios de Facebook.

Terceros también utilizan cookies en sus propios sitios y aplicaciones con relación a los servicios de Facebook. Para conocer cómo utilizan otras partes las cookies, consulta nuestras políticas.

¿Cómo puedes controlar el uso que hace Facebook de las cookies para mostrarte anuncios?

Una de las finalidades de utilizar cookies es mostrarte anuncios útiles y relevantes dentro y fuera de Facebook. Puedes controlar cómo utilizamos los datos para mostrarte anuncios mediante las herramientas que se describen a continuación.

- Si tienes una cuenta de Facebook:

- Puedes utilizar tus preferencias de anuncios para saber por qué ves un anuncio en particular y controlar el uso que hacemos de la información que recopilamos para mostrarte anuncios.
- Algunos de los anuncios que ves se basan en tu actividad en sitios web y aplicaciones fuera del grupo de empresas de Facebook. Es lo que denominamos "publicidad en internet basada en intereses". Puedes controlar si quieres ver anuncios en internet basados en intereses de Facebook en la configuración del anuncio.

- La red de públicos de Facebook permite a los anunciantes mostrarte anuncios en aplicaciones y sitios web fuera del grupo de empresas de Facebook. Una de las formas en las que la red de públicos muestra anuncios relevantes es mediante tus preferencias de anuncios, con el fin de determinar cuáles puede interesarte ver. Puedes controlar esta opción en la configuración de anuncios.

  - Todos:

Puedes indicar que no quieres ver anuncios en internet basados en intereses de Facebook ni de otras empresas participantes a través de laDigital Advertising Alliance en EE. UU., de la Digital Advertising Alliance of Canada en Canadá, de la European Interactive Digital Advertising Allianceen Europa, o en la configuración de tu dispositivo móvil.

  - Más información sobre la publicidad en internet:

Las empresas de publicidad con las que trabajamos suelen utilizar cookies y tecnologías similares como parte de sus servicios. Para obtener más información sobre el uso que hacen los anunciantes de las cookies y las opciones que ofrecen, consulta las siguientes direcciones web:

- Digital Advertising Alliance
- Digital Advertising Alliance of Canada
- European Interactive Digital Advertising Alliance

  - Controles de cookies de navegadores:

Además, tu navegador o tu dispositivo pueden ofrecer ajustes que te permiten indicar si quieres que se utilicen cookies de navegadores y eliminarlas. Para obtener más información sobre estos controles, visita el material de ayuda de tu navegador o dispositivo. Es posible que determinadas partes de los servicios de Facebook no funcionen correctamente si deshabilitas el uso de cookies por parte del navegador.

II. Tuenti y su política de Privacidad y Cookies.

Antes de registrarte como usuario de Tuenti, contratar y/o utilizar nuestros servicios, debes leer y aceptar tanto nuestras Condiciones de uso como esta política de privacidad.

1. Nuestra filosofía

La garantía de la privacidad se encuentra en el ADN de Tuenti y es una de nuestras señas de identidad que aplicamos siempre en el diseño y desarrollo de todos nuestros productos y servicios.

Para nosotros, la información y datos personales son propiedad exclusiva de cada usuario de Tuenti. Esto significa, por un lado, que tú eres el único con derecho a controlar la recogida, uso y revelación de cualquier información sobre ti y, por otro, que nosotros la almacenaremos y gestionaremos de forma responsable y segura, basándonos en los principios de confidencialidad, privacidad e integridad, así como en el cumplimiento de la legislación vigente.

2. Información básica

Para poder comenzar a utilizar Tuenti, sólo será necesario que te registres facilitando una serie de datos identificativos y de contacto básico sobre ti para poder identificarte como usuario, así como que verifiques tu número de teléfono móvil que deseas asociar a tu cuenta. Ahora bien, podrás dar voluntariamente a TUENTI más información para completar tu cuenta en Tuenti como tu foto. Esta información estará disponible y podrás modificarla directamente a través de Tuenti.

Por otro lado, en el caso de que el usuario tenga además contratado el servicio de telefonía móvil tradicional con alguna de las Operadoras con las que colaboramos (Tuenti España, Tuenti Perú, Tuenti Argentina, Tuenti México y Tuenti Ecuador), éste consiente que dichas Operadoras puedan, en caso de ser necesario, comunicar a TUENTI los datos personales y/o informaciones mínimas e indispensables que, en su caso, pudieran ser necesarias para que dicho usuario acceda a través de Tuenti a las funcionalidades de gestión de su línea telefónica móvil.

A estos efectos, te informamos de que todos los datos e informaciones que facilites pasarán a formar parte de los ficheros responsabilidad de Tuenti Technologies, S.L.U. ("TUENTI"), compañía con C.I.F. B-84675529 y domicilio en calle Gran Vía, nº 28, 6ª planta, C.P. 28013 - Madrid (España), con la finalidad de poder permitirte el acceso y uso de los distintos servicios y funcionalidades que te ofrecemos.

3. Edad mínima y calidad de los datos

Para poder registrarte y utilizar Tuenti tienes que ser mayor de 14 años o contar con la autorización de tus padres y/o tutores legales. Por tanto, al darte de alta en Tuenti, nos garantizas que eres mayor de esa edad o, en caso contrario, que cuentas con la mencionada autorización. TUENTI podrá ponerse en contacto contigo en cualquier momento y pedirte la documentación que sea necesaria para verificar que cumples esta condición.

En línea con lo anterior, tus datos personales, número de teléfono móvil y demás información que nos facilites bien en el registro y/o uso de los servicios de Tuenti deberá ser siempre real, veraz y estar actualizada. Además, TUENTI pone a disposición de los usuarios las herramientas y opciones necesarias para el control y actualización de su información personal. Por ello, mediante la entrega de tus datos personales a TUENTI, garantizas y te responsabilizas tanto frente a TUENTI como frente a terceros que tus datos son ciertos y te pertenecen.

Desde TUENTI nos reservamos el derecho a verificar esta información en cualquier momento y, en su caso, a cancelar tu cuenta en Tuenti.

4. Fines comerciales

Dándote de alta como usuario de Tuenti otorgas tu consentimiento expreso para que TUENTI pueda tratar tus datos e información personal para enviarte comunicaciones e información de los productos, promociones, ofertas y/o servicios de TUENTI y/o de las Operadoras con las que colaboramos, todo ello a través de Tuenti, por correo electrónico y/o mensajes a tu número de teléfono móvil.

En particular, dicha información podrá tratar sobre productos, servicios, concursos, ofertas y/o promociones de TUENTI y/o de las mencionadas Operadoras, todos ellos correspondientes a los sectores de internet,, tecnologías de la información y las telecomunicaciones en general. Podrás oponerte en cualquier momento a la recepción de este tipo de comunicaciones comerciales por email, SMS o similar procedentes de TUENTI con tan sólo enviarnos un email a unsubscribe@tuenti.com.

5. Servicios de pago

Para la contratación de nuestros servicios de pago, TUENTI te podrá solicitar determinada información adicional cuando sea necesario. Dichos datos pasarán a formar parte de nuestros ficheros y serán tratados de forma confidencial con la finalidad de tramitar y/o gestionar dicha contratación, la prestación de los servicios contratados y su facturación, pudiendo ser cedidos a otras empresas pertenecientes al sector de las

telecomunicaciones cuando resulte necesario para el correcto desarrollo y/o prestación del servicio contratado por el usuario.

En aquellos servicios que impliquen una obligación de pago para el usuario, autorizas que TUENTI pueda enjuiciar tu solvencia económica mediante el tratamiento de los datos que hubieses aportado y el acceso a la información contenida en ficheros comunes sobre solvencia patrimonial y crédito, con el objetivo de garantizar su cumplimiento así como para confirmar y valorar tu solvencia financiera. Igualmente, el usuario queda informado que, en caso de impago de las cantidades debidas, en su caso, con motivo de la contratación y/o utilización de los servicios de pago de Tuenti conforme a estas condiciones, TUENTI podrá comunicar los datos del mencionado impago a ficheros de solvencia patrimonial y crédito.

6. Política de cookies

Una cookie es un fichero que se descarga en tu dispositivo al acceder a determinadas páginas Web y/o aplicaciones. Las cookies permiten, entre otras cosas, almacenar y recuperar información sobre tu número de visitas, hábitos de navegación o de tu dispositivo y, dependiendo de la información que contengan y de la forma en que utilice, pueden utilizarse para reconocerte como usuario.

Ten en cuenta que para poder utilizar Tuenti es necesario que tengas habilitadas las cookies, especialmente aquellas de carácter técnico que resultan necesarias para que TUENTI pueda identificarte como usuario registrado. TUENTI utiliza los siguientes tipos de cookies, las cuales son tratadas bien por nosotros directamente o por terceros colaboradores:

− Cookies técnicas: Son aquellas utilizadas por TUENTI que permiten al usuario la navegación y la utilización de las diferentes opciones o servicios que se ofrecen como, por ejemplo, controlar el tráfico y la comunicación de datos, identificar la sesión, acceder a partes de acceso restringido, recordar los elementos que integran un pedido, realizar el proceso de compra de un pedido, realizar la solicitud de inscripción, utilizar elementos de seguridad durante la navegación o almacenar, difundir y/o compartir contenidos.

− Cookies de personalización: Son aquellas utilizadas por TUENTI que permiten al usuario acceder a Tuenti con algunas características de carácter general predefinidas en función de una serie de criterios en su dispositivo como, por ejemplo, el idioma, el tipo de navegador, la configuración regional desde donde accede, etc.

− Cookies de análisis: Son aquellas utilizadas por TUENTI y por AKAMAI, COMSCORE, MANYTHINGS y GOOGLE ANALYTICSque permiten cuantificar el número de usuarios y así realizar la medición y análisis estadístico de la utilización y

actividad que hacen los usuarios, así como elaborar perfiles de navegación de éstos para poder introducir mejoras en Tuenti.

− Cookies publicitarias y de publicidad comportamental: Son aquellas utilizadas por TUENTI y por nuestros colaboradores que gestionan los espacios que sirven publicidad de TUENTI que permiten difundir publicidad adecuada y relevante, medir la efectividad de nuestras campañas online, así como adecuar el contenido de los anuncios al perfil de navegación de cada usuario en internet.
Recuerda que puedes permitir, bloquear o eliminar estas cookies cuando quieras a través de las opciones de configuración de tu dispositivo o terminal, así como de tu navegador de internet. Para ello, puedes consultar la información de soporte de dichos dispositivos o navegadores para conocer el modo en que puedes eliminar las cookies, dado que el modo puede diferir entre distintas versiones y sistemas operativos.

7. Comunicaciones de datos

Salvo la información y/o datos que se podrán mostrar al resto de usuarios de Tuenti que formen parte de tu red de contactos en cada momento, con carácter general los datos que facilites a TUENTI no se cederán a otras personas o empresas. En el caso de que decidamos lo contrario, siempre te informaremos y solicitaremos tu consentimiento previamente. No obstante, algunos proveedores subcontratados por TUENTI podrían tener ocasionalmente acceso a tus datos e información personal como encargadas del tratamiento pero en ese caso sería bajo nuestro exclusivo control, cumpliendo estrictas medidas de seguridad y con la única finalidad de prestarnos un servicio necesario para el funcionamiento de Tuenti.

8. Derechos ARCO

En cualquier momento podrás ejercer ante TUENTI tus derechos de acceso, rectificación, cancelación u oposición (ARCO), en los términos previstos en la ley vigente. Esto significa que podrás preguntarnos qué datos tenemos sobre ti, solicitarnos su actualización o decirnos que ya no quieres que los utilicemos para una finalidad concreta, o simplemente, pedirnos que los cancelemos de nuestros ficheros.

Para todo ello deberás contactar con TUENTI preferiblemente a través de privacidad@tuenti.com o, si lo prefieres, por correo postal a la dirección calle Gran Vía, nº 28, 6ª Planta, C.P. 28013 - Madrid (España), indicando en todo caso el concreto derecho ARCO que deseas ejercitar y aportando una copia de tu documento oficial de identidad.

9. Seguridad

TUENTI se preocupa por garantizar la seguridad, el secreto y la confidencialidad de tus datos, comunicaciones e información personal. Por eso, como parte de nuestro compromiso y en cumplimiento de la legislación vigente, hemos adoptado las más exigentes y robustas medidas de seguridad y medios técnicos para evitar su pérdida, mal uso o su acceso sin tu autorización.
Además, nos comprometemos a actuar con rapidez y responsabilidad en el caso de que la seguridad de tus datos pueda estar en peligro, y a informarte si fuese relevante.

10. Baja de Tuenti

Por último, informarte que, salvo que seas un usuario que tiene contratado el servicio de telefonía móvil tradicional de TUENTI o bien de alguna de las Operadoras con las que colaboramos, cualquier usuario podrá darse de baja su cuenta a través de Tuenti en cualquier momento. En caso de baja, perderás la información y datos que pudieses tener en Tuenti, así como el derecho a utilizar cualesquiera beneficios o servicios que pudieses tener activos a la fecha de la baja y/o haber contratado con anterioridad como usuario de Tuenti.
De igual forma, te recordamos que también podrás desinstalar cuando quieras la aplicación de Tuenti de tu dispositivo o terminal móvil, mediante las distintas opciones que te ofrezca el mismo. En caso de que solicites tu baja de Tuenti y sin perjuicio de las obligaciones de conservación de datos que pudiesen establecerse por la legislación vigente, TUENTI se compromete a cancelar toda tu información y datos personales.