Privacidad y Facebook: estudio sobre los datos personales en las redes sociales online

Trabajo Fin de Máster

VNiVERSiDAD D SALAMANCA

Universidad de Salamanca

Facultad de Traducción y Documentación

MÁSTER EN SISTEMAS DE INFORMACIÓN DIGITAL

Presentado por:

Carlos Fernández Moran

Dirigido por:

Luis Hernández Olivera

Universidad de Salamanca
Facultad de Traducción y Documentación
MÁSTER EN SISTEMAS DE INFORMACIÓN DIGITAL
Trabajo Fin de Máster

Privacidad y Facebook:
estudio sobre los datos personales en las redes sociales online

REALIZADO POR:
CARLOS FERNÁNDEZ MORÁN

VISTO BUENO:
LUIS HERNÁNDEZ OLIVERA

SALAMANCA, 2011

Asiento catalográfico

Autor	Fernández Morán, Carlos
Título	Privacidad y Facebook: estudio sobre los datos personales en las redes sociales online
Director	Hernández Olivera, Luis
Departamento	Universidad de Salamanca (España). Departamento de Biblioteconomía y Documentación
Fecha	2011-07-29
Descripción Física	158 p.
Palabras clave	Español: Facebook, privacidad, redes sociales, Ley de protección de datos, datos de carácter personal
	Inglés: Facebook, privacy, social networks, data protection law, personal data.
Descripción	Trabajo de Fin de Máster del Máster en Sistemas de Información Digital, curso 2010-2011
	.

Resumen

[ES] En el año 2004 nació una nueva forma de comunicación por Internet creada en un principio como punto de encuentro entre antiguos compañeros de clase, un lugar donde relacionarse con amigos u otras personas con gustos comunes: Facebook. A lo largo de estos años la red social ha conseguido un número de usuarios tan importante que ni sus propios creadores contaban con ello. El siguiente trabajo nos llevará a estudiar Facebook desde el punto de vista de la privacidad con el objetivo de comprender el nivel de protección de la privacidad y de los datos de carácter personal que en esta red social se recogen. La privacidad es un tema que está en auge en los últimos años debido a una incipiente preocupación de los usuarios de las redes sociales por conocer qué ocurre con sus datos. Para ello veremos cómo ha ido evolucionando la privacidad con el paso de los años, analizando la actual política de Facebook y realizando un análisis de las leyes por las que se rige tanto a nivel español como europeo, conociendo los posibles riesgos que se producen en las redes sociales.

[EN] A new form of communication was born in 2004. At the beginning, it was created only as a meeting space for old classmates, a place where one could encounter friends and people with common interests: This place is Facebook. Throughout all of these years, the social network has increased its number of users to such an extent, that even its own creators would never have expected. The following research paper will lead us to study Facebook from the perspective of its privacy issues; with the main goal of understanding the privacy protection level, and the personal data that is gathered in this social network. Privacy has been a crucial topic during the last years because of the user's growing concern to know how their personal data is treated. To study this, we will examine how has the privacy evolved throughout the years, we will analyze the current Facebook's privacy policy, and we will also analyze the privacy laws - both in the Spanish and European contexts - in order to understand and recognize possible risks that the users of the social networks are exposed to.

Mark Zuckerberg

"The age of privacy is over"

Índice general

Índice general……VI-VII
Índice de figuras y tablas……VIII
Abreviaturas y acrónimos……..IX

Parte preliminar

Presentación……..XI-XII
Introducción……XIII-XX

Parte 1

Un mundo de relaciones virtuales: las redes sociales

1. El concepto de redes sociales……..22-23
2. Redes Sociales: características……24-25
3. Análisis de las tipologías de redes sociales……26-27
4. Aproximación a la historia de las redes sociales……28-32

Parte 2

La revolución de las redes sociales: Facebook

5. Orígenes y evolución de Facebook……34-44
6. Principios de Facebook……45-47

Parte 3

El derecho a la privacidad en Facebook

7. Intimidad y privacidad……49-61
7.1 La regulación europea de la privacidad
7.2 El ordenamiento jurídico español
7.3 El dato de carácter personal

8. El largo camino para la protección de la privacidad en Facebook.....62-72
9. La política de privacidad de Facebook……73-90
10. Las opciones para configurar la privacidad en Facebook……91-97
11. Los riesgos y peligros de la privacidad en Facebook……..98-101
12. Conductas lesivas……102-104
13. Derecho al olvido……105-108

Parte final

Conclusiones……110-114
Bibliografía……115-121
Anexos……122-158

Índice de figuras

Fig. 1 Evolución de las redes sociales

Fig. 2 Página inicial Facebook 2004

Fig. 3 Perfil Facebook año 2005

Fig. 4 Página inicial Facebook año 2006

Fig. 5 Perfil Facebook año 2007

Fig. 6 Página de inicio Facebook año 2008

Fig. 7 Página de inicio Facebook año 2009

Fig. 8 Página de inicio Facebook año 2010

Fig. 9 Página de perfil Facebook año 2011

Fig.10 Países con más usuarios en Facebook

Fig. 11 Expansión de la política de privacidad

Fig. 12 Privacidad en Facebook año 2005

Fig. 13 Privacidad en Facebook año 2010

Fig. 14 Información que se recoge en Facebook

Fig. 15 Pantalla configuración de la privacidad

Fig. 16 Pantalla “Cosas que comparto”

Fig. 17 Pantalla “Cosas que otros comparten”

Fig. 18 Pantalla “Información de contacto”

Abreviaturas y acrónimos

AEPD: Agencia Española de Protección de Datos

CE: Constitución española

CoE: Comisión Europea

CEDH: Convenio Europeo de Derechos Humanos

CIPPIC: Canadian Internet Policy and Public Interest Clinic de la Universidad de Ottawa

DRAE: Diccionario de la Real Academia Española

EFF: Electronic Frontier Foundation

FTC: Comisión Federal de Comercio de los Estados Unidos

G29: Grupo de Trabajo del Artículo 29

INTECO: Instituto Nacional de Tecnologías de Comunicación

LOPD: Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

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

PIPEDA: Ley de Protección de la Información Personal y los Documentos Electrónicos de Canadá

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

STC: Sentencias del Tribunal Constitucional

UE: Unión Europea

PARTE PRELIMINAR

Presentación

En los últimos años, hemos sido testigos del tremendo auge de las redes sociales en Internet. Hasta hace relativamente poco era un fenómeno apenas conocido, pero ha pasado a convertirse en un elemento importante en la vida de muchas personas.

Desde el punto de vista del profesional de la Documentación, las redes sociales han abierto un abanico importante de posibilidades que debemos aprovechar. Estas oportunidades van desde ofrecer una visión más social del servicio de información en el que trabajemos pudiendo mostrar de una forma más directa nuestros “productos” hasta tener una comunicación más cercana con los usuarios. Aunque muchos profesionales piensan que las redes sociales son una moda y que no tienen futuro, en el contexto que nos encontramos debemos aprovechar de todos los medios posibles para ofrecer un mejor servicio a los usuarios.

El presente trabajo se ha centrado en analizar la red social online que cuenta con más usuarios hasta el momento, Facebook. Esta red ha supuesto un cambio en la forma tradicional de las comunicaciones, y ha llegado a alcanzar una importancia que ni su propio creador llegó a imaginar.

Pero el análisis no va a ser específicamente sobre cómo podemos comunicarnos con los demás usuarios de la red, ni va a enumerar las distintas aplicaciones que en ella encontramos. Nos vamos a centrar en analizar un tema que todos los usuarios de las redes sociales deberíamos prestar más atención, la privacidad. Es imprescindible que todos estemos concienciados sobre los riesgos a los que nuestra privacidad está sometida.

La privacidad es un tema que está en auge en los últimos años debido a una incipiente preocupación de los usuarios de las redes sociales por conocer qué ocurre con sus

datos, pero a la hora de ponerlo en práctica son muy pocos los que trasladan esa preocupación a la gestión de Facebook.

Aprovechando estas líneas quería agradecer a una serie de personas que han hecho que la realización de este trabajo no fuera una labor tan tediosa como me imaginaba, ayudándome y haciendo las horas de investigación y redacción más amenas. En primer lugar a mi familia, por el apoyo recibido; a mis compañeros tanto de clase como de piso, que además de hacer que este año haya sido maravilloso siempre he podido contar con ellos en los momentos de dudas. Por último, agradecer a mi tutor y director de este trabajo, Luis Hernández Olivera la gran profesionalidad que me ha mostrado, guiándome siempre por el camino correcto y ofreciéndome continuamente su ayuda.

Introducción

Las redes sociales son parte de nuestra propia naturaleza, tanto desde un punto de vista biológico como cultural. Los seres humanos somos sociales por naturaleza y desde que nacemos pertenecemos a una red. Siempre hemos sentido la necesidad natural de relacionarnos y de comunicarnos y así compartir experiencias y sentimientos y gozar de la compañía de otros. Por eso se dice que somos “seres sociales” y tendemos a formar comunidades y organizaciones sociales.

Desde que surgieron las primeras redes sociales online, allá por el año 1995 hasta su explosión en la segunda mitad de la primera década del siglo XXI han generado una considerable expectación entre los internautas, muchos de ellos deseosos de que la red ofreciera una mayor interacción y visualización de las relaciones sociales.

Entre todas las redes sociales que existen actualmente, hay una de ellas que destaca por encima de todas. Se trata de Facebook, creada en el año 2004 por Mark Zuckerberg como un servicio exclusivo para los estudiantes de Harvard.

La gran evolución que ha sufrido Facebook durante estos años ha hecho que cuente ya con 650 millones de usuarios, y el ritmo no cesa, ya que en sus previsiones se encuentra alcanzar la cifra de los 700 millones de usuarios a finales del año 2011.

A lo largo de su corta historia, Facebook ha tenido serios problemas en relación a la privacidad. Estos han sido provocados, en medida, por los distintos cambios que han ido añadiendo haciendo de Facebook una red social cada vez más transparentes, o bien por los distintos servicios que pretendían añadir como Beacon o News Feed, o debido a terceros, por culpa de las aplicaciones.

Los usuarios de esta red social siempre hemos tenido dudas acerca de los verdaderos intereses de Facebook en relación al tratamiento de los datos de carácter personal. Desde el primer momento en el que pasamos a formar parte de una red social online, estamos suministrando información, datos personales que, sin ninguna actividad muy compleja, pueden ofrecer un perfil de nuestra persona, y que en algunos casos nos ayudará a desarrollarnos más libremente como personas, pero, en otros casos -y por desgracia, en la mayoría- suponen un grave riesgo para nuestra vida privada.

Cuando nos registramos en la red añadimos una serie de datos personales que son muy valiosos para cualquier marca comercial puesto que, muchos de nosotros indicamos los gustos que tenemos, nuestras preferencias, etc. Las redes sociales se basan en la publicación e intercambio de información personal por parte de los usuarios, siendo en muchos casos información perteneciente a la esfera más íntima y personal: ideología, orientación, sexual, creencias religiosas.

Si nos parasemos a leer detenidamente las condiciones que nos ofrece Facebook cuando nos registramos, más de uno daría un paso hacia atrás, ya que, entre otras cosas, una vez que subes una fotografía a Facebook, cedes parte de tus derechos a la red.

Debido a esta serie de dudas que se presentaban, decidimos realizar este trabajo enfocando el asunto desde el punto de vista de la privacidad. Antes de comenzar con la realización del estudio partíamos de una base con unos conocimientos previos sobre el tema a tratar limitados, sobre todo en el apartado jurídico, ya que mi formación en derecho es escasa.

La privacidad en las redes sociales es un tema que no se ha tratado mucho en España, principalmente porque se trata de un fenómeno relativamente nuevo, ya que en España, el boom de las redes sociales se produjo a partir del año 2008. De hecho, no es hasta este año cuando Facebook pone a disposición de sus usuarios hispanos su web en español.

Es tal el crecimiento de Facebook en España que los usuarios de esta red son los que más han aumentado en los últimos tres años. Actualmente el 78 por ciento de los internautas españoles tienen cuenta en la red creada por Mark Zuckerberg, mientras que en 2008 solamente el 13 por ciento tenía perfil.

Estos datos mencionados anteriormente nos demuestran que Facebook ha calado en la sociedad española convirtiéndose en la primera red social, muy por delante de sus dos principales competidoras, Tuenti y Twitter.

Cuando nos propusimos realizar este estudio, teníamos la firme intención de dar respuesta a una serie de dudas. Cuando nos registramos en una red social, desde un principio estamos añadiendo datos personales, lo mismo que cuando interactuamos con la red. Las dudas se centraban sobre todo en responder a la pregunta ¿qué harán las redes sociales con todos nuestros datos?, ¿cómo manejarán toda esa

información?. A medida que iba que iba investigando surgían más preguntas sobre todo en relación con la finalidad que tienen esos datos, si Facebook los utilizará con un objetivo comercial, beneficiándose de su uso.

El objetivo principal que nos ha llevado a realizar este trabajo es hacer un análisis de la política de privacidad de Facebook, averiguando cual es la situación en la actualidad, conociendo toda la información que debemos compartir con la red social, en definitiva, cómo controla, cómo gestiona Facebook los datos personales que añadimos a su red.

Junto a este objetivo principal también se ha pretendido dar respuesta a otros objetivos más específicos como serían:

- Conocer qué son las redes sociales
- Mostrar las distintas características de las redes sociales
- Conocer los tipos de redes sociales online
- Analizar el origen y evolución de Facebook
- Detallar los principios sobre los que se asienta Facebook.
- Conocer la diferencia entre intimidad y privacidad
- Conocer las distintas leyes que han regulado la privacidad tanto en el ámbito europeo como en el español
- Conocer la evolución de las distintas políticas de privacidad que ha tenido Facebook a lo largo de su historia, desde el año 2004 hasta el año 2011.
- Detectar los principales cambios sufridos en las políticas privacidad
- Revelar cuál de todas las distintas políticas era la que más protección daba a los datos de los usuarios.
- Mostrar los posibles riesgos que conlleva el uso de las redes sociales y conocer algunos casos que ya han sido juzgados.
- Conocer qué es el derecho al olvido, en qué consiste y cuáles son sus consecuencias en Facebook.

Al tratarse de un tema relativamente reciente, la cantidad de información que encontramos no era suficiente. La mayor parte de las monografías y artículos analizados se centraban en un punto de vista más general sobre la evolución de las redes sociales, explicando en qué consiste cada una de ellas, pero pocos artículos hacían hincapié en el tema de la privacidad. A medida que íbamos buceando en bases

de datos e involucrándonos cada vez más en el tema, conseguimos averiguar que el asunto que tratamos de investigar ha sido tratado, aunque quizás no con toda la importancia que se merece, ya que, a día de hoy, Facebook es la mayor red social online que existe y maneja unos volúmenes de información muy importantes.

Entre las obras consultadas destacaríamos en relación a la historia de las redes sociales el estudio realizado por Boyd y Ellison "Social network sites: definition, history, and scholarship" puesto que todos los demás artículos que hemos consultado se basan en él. Entre los artículos que se centran en la privacidad no hay ninguno que destaque por encima del resto, ya que algunos tratan la privacidad desde otro punto de vista. Pero si cabe destacar el "Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online" llevado a cabo por la Agencia Española de Protección de Datos (en adelante, AEPD) y el Instituto Nacional de Tecnologías de Comunicación (en adelante, INTECO), así como el artículo de Christian Fuchs "An alternative view of privacy on Facebook", éste último por ser más reciente y tratar temas que otros artículos no profundizaban, centrándose sobre todo en analizar la política de privacidad que sigue Facebook.

La primera fase del trabajo consistió en la recopilación de la información. Para obtener las distintas referencias bibliográficas utilizadas se realizaron búsquedas en las principales bases de datos especializadas en Humanidades y Ciencias Sociales, consultando con más insistencia las bases de datos jurídicas. Entre las bases de datos consultadas están SpringerLink, ScienceDirect o Mendeley.

En las específicas sobre derecho las bases que más se consultaron fueron Aranzadi y el portal jurídico Iustel. De estas bases de datos fue donde se consultaron las leyes que luego hemos analizado en este estudio, así como una serie de noticias que hacían referencia a los casos juzgados en relación a los problemas. Pero sobre este último tema, además de los periódicos también se ha extraído mucha información de los informes que realiza la AEPD.

A la hora de realizar las búsquedas en las bases de datos empleamos términos como privacidad, Facebook, protección de datos, datos de carácter personal, redes sociales, Ley de Protección de Datos, etc., unas veces se utilizaban de forma individual y otros en combinación con los operadores booleanos, todos ellos tanto en español como en inglés. El resultado que nos mostraban era limitado, ya que en algunas bases de datos el número de resultados era más amplio pero la mayor parte de los documentos eran irrelevantes.

Como hemos mencionado en los párrafos anteriores, no había tanta información como imaginábamos, por lo que se tuvo que recurrir a otras bases de datos menos especializadas pero igual de eficaces, como es el caso de Google Académico.

Además de lo anterior, también hemos encontrado mucha información dentro de la propia página de Facebook, así como en el blog que ellos mismos desarrollan. Mencionar que de la propia página web de Facebook hemos extraído información como la política de privacidad, además de la información necesaria para conocer cómo

debemos configurar nuestra cuenta de un modo seguro. Los blogs nos han servido de ayuda para conocer más datos estadísticos y cuestiones relativas a las políticas de privacidad que Facebook ha ido teniendo, como serían las quejas mostradas por los usuarios o los cambios sufridos.

Añadir también que se han consultado fuentes documentales de prensa online, en especial periódicos, como son El País, El Mundo o La Vanguardia, y agencias de noticias como Europa Press para mantenernos informados sobre los conflictos surgidos y para documentar los casos que ya han sido juzgados.

Una vez recogida toda la información necesaria para comenzar el trabajo, procedimos a lectura y al análisis de la bibliografía recopilada. A continuación revisamos los textos normativos reguladores de la protección de datos, completando lo anterior con el análisis de la política de protección de datos y con la comprobación de la adecuación a la normativa española.

Además, con respecto a los estudios bibliográficos empleados, como se puede comprobar, en temas más generales sobre las redes sociales destaca la literatura en castellano, mientras que los trabajos más especializados están escritos en lengua inglesa.

Para la elaboración de la bibliografía se ha seguido la norma internacional ISO 690 y la ISO 690-2, para el caso de los documentos electrónicos y sus partes. El sistema de citación empleado se ajusta al estándar de la APA (American Psychological Association) según el principio autor, fecha y página específica de la cita en el texto. Aclarar que todas las citas en el texto tienen su correspondiente entrada en la bibliografía.

Por lo que se refiere a la estructura del trabajo, después de los apartados preliminares necesarios en todo estudio de carácter académico (resumen, sumario, índices e introducción), se puede dividir el trabajo en tres bloques diferenciados entre sí.

La primera parte está dedicada a las redes sociales desde un punto de vista general. El desarrollo que han sufrido en los últimos años ha sido tan importante que las ha convertido en un fenómeno social, abriendo a los seres humanos una nueva vía de comunicación.

En el primer capítulo nos vamos a centrar en conocer el concepto red social, conociendo distintas definiciones para terminar ofreciendo una definición que reúna todas las características principales de las otras.

El segundo capítulo nos centramos en conocer cuáles son las características comunes de las redes sociales. Cada red tiene una misión, un público distinto y un objetivo que le hace diferente a las otras, pero, a pesar de esto todas tienen algo en común que las hace no ser muy diferentes entre sí.

El tercer apartado nos muestra cuales son los distintos tipos de redes que existen. Entre estos tipos podemos hacer una clasificación agrupando las redes sociales en tres grandes grupos, cada uno con características comunes y elementos particulares que las diferencian de los otros grupos. Por un lado estarían las redes sociales de ocio o generales, por otra parte las redes especializadas y el tercer grupo, las redes sociales profesionales.

Esta primera parte termina con un capítulo dedicado a explicar la historia y evolución de las redes sociales. Cuáles han sido las primeras en aparecer, por qué no tuvieron éxito hasta llegar a las redes sociales más actuales.

La segunda parte (La revolución de las redes sociales: Facebook) está centrada en analizar la red social objeto de este estudio.

Dividida en dos capítulos, en el primero de ellos vamos a ver cuál es el origen y la evolución que ha tenido Facebook durante estos años. Desde su creación en el año 2004 como un servicio dedicado exclusivamente para los alumnos de Harvard a cómo ha ido ganado adeptos con el paso de los años hasta convertirse en la red social con más usuarios en todo el mundo. Prestaremos especial atención a los cambios que se han ido produciendo año a año, los nuevos servicios que se han incorporado, la apertura de la red a todo el mundo en el año 2006, y lo que supuso la creación de la web en español allá por el año 2008.

En el sexto capítulo vamos a analizar los principios sobre los que se ha creado Facebook, donde se definen los valores por los que fue creada, comprobando si esos principios realmente se cumplen el objetivo con el que fueron diseñados por Mark Zuckerberg.

El tercer bloque, el más extenso, es el que se centra en analizar la privacidad tanto en los aspectos jurídicos como en su concreción práctica en Facebook. Esta tercera parte se divide a su vez en siete apartados.

En el séptimo capítulo vamos a ver cómo surge el concepto de privacidad, diferenciándolo del término intimidad. Además se analizarán las distintas normativas que regulan o han regulado la privacidad a nivel europeo y centrándonos sobre todo en España a través de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en adelante, LOPD) y su posterior desarrollo en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos (en adelante, RDLOPD). En este primer capítulo mostraremos también qué es el concepto jurídico de dato personal.

El octavo capítulo analiza cuales han sido las distintas políticas de privacidad que ha seguido Facebook, la red sobre la que se basa el estudio, desde su origen hasta la última modificación llevada a cabo a finales del año 2010. En estos años ha tenido seis políticas de privacidad que, en los cambios sucesivos que se han ido produciendo,

muestran un camino que han emprendido con un objetivo final, hacer que Facebook sea cada vez más transparente.

El noveno apartado desgrana cuál es la política actual de privacidad que sigue Facebook, analizando sus puntos y comprobando si esos principios se corresponden con lo que marca la ley española.

El cuarto apartado de este último bloque, nos va a mostrar la manera de realizar una configuración correcta de la privacidad para evitar que se muestren más datos de los que realmente se deberían mostrar debido a la política de privacidad predeterminada de Facebook abierta a "todos".

En el undécimo capítulo se van a analizar los distintos riesgos que pueden provocar las redes sociales. Estos peligros pueden llegar desde el momento en que te registras, cuando forma parte de la red social o cuando quieres darte de baja de la red.

El penúltimo apartado nos muestra las conductas conflictivas que provocan el uso de las redes sociales. Entre éstas señalaremos la suplantación de la identidad como la más importante de ellas, siendo la causa que más delitos ha causado.

Para finalizar, el último capítulo se va a centrar en explicar la futura directiva que está elaborando la Comisión Europea en relación al Derecho al olvido, es decir, el derecho en virtud del cual los usuarios pueden exigir a los proveedores de servicios de Internet que borren sus datos completamente cuando dejen de ser necesarios para los fines para los que se recabaron o cuando el cliente se dé de baja.

La parte final del estudio está dedicada a explicar las conclusiones surgidas del análisis de los puntos anteriores, acompañado de la bibliografía consultada y completada con una serie de anexos.

Las conclusiones que se derivan del estudio realizado nos van a mostrar que es excesiva la cantidad de datos que debemos añadir cuando nos registramos en Facebook, así como la información que está disponible para cualquier usuario que no pertenezca a la propia red social. En relación a las distintas políticas de privacidad que Facebook ha seguido hasta la actualidad se va a mostrar que la que más adecuada para preservar la información de los usuarios era la primera, en el año 2005, y cómo a medida que la red ha ido creciendo se ha vuelto más transparente. Además se comprobará cómo las aplicaciones presentes en Facebook deben mejorar en el asunto de la privacidad, puesto que para poder unirte a una de ellas es necesario permitirlas el acceso a todos tus datos. Por último, analizaremos los problemas de Facebook con la red social, más acentuados últimamente con la Ley del Olvido y con el problema del reconocimiento facial.

Para terminar, el trabajo se completa con un anexo donde encontraremos una serie de imágenes que nos muestran cómo ha ido evolucionando la privacidad en Facebook,

junto a la política de privacidad vigente de Facebook y las dos leyes españolas que regulan la protección de datos, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) y su posterior desarrollo en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica de Protección de Datos.

PARTE 1

UN MUNDO DE RELACIONES VIRTUALES: LAS REDES SOCIALES

Capítulo 1
El concepto de redes sociales

El concepto red social se remonta a principios del siglo XX, donde fue empleado para describir conjuntos complejos de relaciones entre los distintos miembros de los sistemas sociales en las diferentes dimensiones del comportamiento humano, esto es, desde las relaciones interpersonales, las actividades relacionadas con la vida pública (profesional, de negocios etc.) hasta los ámbito internacional.

El primero en utilizar el término como tal fue el antropólogo de la Universidad de Manchester J. A Barnes en 1954.

La aparición de las nuevas tecnologías, y especialmente con la llegada de la Web 2.0 ha provocado un cambio en la forma de comunicación de los seres humanos. Necesitamos relacionarnos con nuestros semejantes y con las redes sociales hemos encontrado una nueva forma de conseguirlo, ya que el objetivo principal de estas redes es fomentar y fortalecer las relaciones sociales (Monsoriu Flor, 2008, p.22). Las redes sociales reflejan la dinámica de interacción entre individuos, grupos e instituciones en un intercambio dinámico, por lo tanto en construcción permanente que involucra conjuntos que se identifican en las mismas necesidades y problemáticas y que se organizan para potenciar sus recursos.

Pero lo que se pretende definir no es lo que consideramos como una red social "tradicional" sino una red social "online". El concepto de red social online ha sido estudiado por tantos profesionales de diferentes sectores que ha provocado que no exista una definición concreta que sea aceptada por todos para referirse a este concepto.

Entre las distintas definiciones, una de las más importantes es la que realizaron en 2007 Danah M. Boyd y Nicole Ellison (2007, p. 2) quienes, en un artículo de la sección

especial del Journal of Computer-Mediated Comunication, definen como “sitios de redes sociales a los servicios basados en la web que permiten a los individuos (1) construir un perfil público o semi-público dentro de un sistema delimitado, (2) articular una lista de otros usuarios con lo que comparten una conexión, y (3) ver y recorrer su lista de conexiones y aquellas hechas por oros dentro del sistema”.

A nivel nacional, una de las autoras que más ha tratado el tema de las redes sociales online es Natalia Arroyo (2008, p.3). Define a las redes sociales online “como aquellos sitios web que permiten a los individuos construir un perfil público o semi-público dentro de una plataforma en línea y articular sus relaciones con otros usuarios de la misma, de forma que cualquiera que lo desee, pueda acceder a su perfil y contactar con él”.

Por último, la definición del Instituto Nacional de Tecnologías de la Comunicación (INTECO) (2009, p.6) quien define a las redes sociales online como “servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado”.

En resumen, analizando todas las definiciones anteriores, podríamos establecer una definición estándar donde los dos aspectos más importantes serían 1: construir un perfil público, para que, a partir de ese perfil, una vez añadidos tus datos personales puedas comunicarte con las otras personas de la red; y 2: crear una red en base a unos criterios comunes que permitan el contacto con las otros usuarios y la posibilidad de interactuar con ellos.

Capítulo 2
Redes Sociales: características

A pesar de que cada red social ha sido creada con un objetivo concreto, todas ellas tienen unas características comunes. Si tomamos en consideración todas estas características en su conjunto, pueden observarse cambios importantes en cómo las personas se interrelacionan en red y manejan sus contactos sociales en entornos sociales distintos. Según Romina Cachia (2008) estas características serían:

- La presentación del usuario a través de un perfil: es la plataforma básica de entrada a cualquier red social. Cada usuario se presenta a sí mismo a través de una serie de datos personales o profesionales, o añadiendo fotografías, música o videos. Este contenido creado por los usuarios está vinculado a sus propios intereses y a su vida personal.

- Organización de los datos a través de redes o grupos. La organización de los datos del perfil está habitualmente determinada por la infraestructura de las redes sociales. Aunque algunos sitios de redes sociales permiten un diseño abierto, otros limitan la presentación a categorías específicas para la visualización de la información de los usuarios.

- Control de acceso del usuario a crear contenidos. A menos que el usuario especifique otra cosa, la mayoría de los sitios de creación de redes sociales permiten ver los contactos de tus 'amigos' y de manera transversal en estas redes (Boyd, 2006). Algunos sitios de creación de redes sociales ofrecen también una plataforma para describir la relación entre amigos, que cualquier miembro de tu red o de la red de tus amistades podrá ver.

- Conexiones dinámicas: La gente se conecta no sólo a través de los contactos que conocen, sino también a través de objetos digitales, tales como etiquetas,

fotos o incluso aplicaciones incorporadas dentro de la red social, como por ejemplo la aplicación «estantería visual» (*visual shelf*) en Facebook. Esto permite la creación de comunidades virtuales sobre la base de intereses similares.

- Intereses comunes: la red ofrece la posibilidad de localizar a personas que tengan tus mismos intereses, con los que poder reunirse, colaborar u organizar actividades con eficacia a bajo coste y desde lugares diferentes.

- Facilidad de uso: una característica importante de la popularidad de las redes sociales es su sencillez. En comparación con las páginas web personales, cualquiera con conocimientos básicos de Internet puede crear y gestionar una presencia en línea. Las redes sociales son gratuitas y están abiertas a la incorporación de cualquiera. La mayor parte requiere alguna forma de inscripción, mediante la cual se pide a los usuarios que faciliten datos personales. Algunos sitios de creación de redes sociales limitan su afiliación según diversas especificaciones, por ejemplo la edad o la recomendación de un amigo.

- Las distancias no existen: a través de las redes sociales las distancias geográficas han dejado de existir. Puedes pertenecer perfectamente a un grupo cuya sede se encuentre a miles de kilómetros de ti y estar informado al instante de lo que allí ocurre.

Como podemos ver, aunque cada red persiga un objetivo distinto o esté dirigida a un grupo de personas diferentes, lo cierto es que todas comparten unas características que, al final, no las hace tan diferentes una de otras. Entre las características más importantes cabe señalar la necesidad de crear un perfil y que ese perfil se puede conectar con el perfil de los distintos usuarios de la red.

Capítulo 3
Análisis de las tipologías de redes sociales

Existen diferentes tipos de redes sociales. Depende de la finalidad que cumplan. Hay redes que se utilizan simplemente como forma de comunicación entre los usuarios, otras que tienen un papel más destinado a cumplir un servicio informativo como una herramienta de marketing, etc. Es decir, cada red tiene una misión, un público distinto y un objetivo que le hace diferente a las otras. A pesar de que se pueden establecer muchos tipos de clasificaciones, podemos hacer una clasificación agrupando las redes sociales en tres grandes grupos, cada uno con características comunes y elementos particulares que las diferencian de los otros grupos. Esta división es la más utilizada aunque existen otras que, a pesar de hacer las mismas divisiones, utilizan un nombre distinto para nombrar a los grupos.

- Redes sociales de ocio o generales: son las más utilizadas. Entre ellas encontramos redes como Facebook, Tuenti o MySpace. La finalidad que persiguen es facilitar y potenciar las relaciones entre los usuarios registrados, no van más allá de la simple comunicación entre los usuarios. Esta tipología de redes ha sustituido a los medios de comunicación que se utilizaban no hace mucho tiempo como puede ser Windows Messenger. Se caracterizan porque cada usuario puede darse de alta libremente o a través de invitación, y una vez creado su perfil comienza a agregar conocidos invitándoles a formar parte de su comunidad. Se llaman redes de ocio porque están destinadas más a pasar el tiempo libre que de una manera profesional. La información que se comparte es de temática variada, desde fotografías, videos, tus pensamientos hasta la religión que profesas o tu película favorita.

- Redes especializadas: giran en torno a un eje temático común. Orientadas a colectivos que comparten unos intereses comunes. Entre este tipo de redes encontramos Flickr que trata sobre fotografías, Tripku sobre viajes, esfutbol sobre fútbol o Meetic para encontrar pareja.

Además, dentro de éstas se incluyen las redes sociales de microblogging, que a día de hoy están en auge como puede ser la red Twitter. Las redes de microblogging se basan en una actualización constante de los perfiles a través de unos mensajes de texto que no pueden superar los 160 caracteres. Así se crea una comunicación más clara, concisa y sobre todo rápida. Existen discusiones por las que no se consideran redes sociales a esta tipología ya que no conlleva una interacción entre los usuarios de la misma, limitándose ésta, como máximo, al envío de mensajes de texto o como mucho, al envío de fotografías comentadas.

- Redes sociales profesionales: a través del perfil creado, el usuario recoge principalmente datos relativos a su formación académica y a su trayectoria profesional. Están dirigidas a un público más especializado. Encontramos redes como LinkedIn, Xing, etc. Este tipo de redes se utilizan para buscar ofertas de trabajo, candidatos a un puesto, nuevas oportunidades de negocios, etc. Sirve de ayuda para establecer contactos profesionales con otros usuarios. El beneficio que supone al ámbito profesional tanto desde el punto de vista del trabajador como del empresario son enorme. Al trabajador le permite mantener contacto con profesionales de su mismo sector y al empresario le puede servir como herramienta complementaria en un proceso de selección de personal, además de las distintas alternativas de negocio que se abren en ellas.

De los tres grupos de redes sociales que hemos establecido el más importante, por el número de seguidores, y con una amplia diferencia sobre el resto, son las redes sociales de ocio. Sin embargo, las redes sociales especializadas están teniendo en los últimos tiempos un auge importante, como es el caso de Twitter, que se está convirtiendo en una herramienta de comunicación muy importante.

Capítulo 4
Aproximación a la historia de las redes sociales

La creación de redes sociales es un fenómeno que ha existido desde el comienzo de las sociedades (Barabasi, 2002, p.27). Estas redes sociales se basan en la teoría de los seis grados, propuesta en 1929 por el escritor húngaro Frigyes Karinthy[1] en una historia llamada "Chains" (Cadenas). Esta teoría afirma que cualquier persona en la Tierra puede estar conectado a cualquier otra persona a través de una cadena de conocidos que no tiene más de seis intermediarios. El concepto está basado en la idea que el número de conocidos crece exponencialmente con el número de enlaces en la cadena, y sólo un pequeño número de enlaces son necesarios para que el conjunto de conocidos se convierta en la población humana entera.

Esta teoría se recoge también en el libro "Six Degrees: The Science of a Connected Age" del sociólogo Duncan Watts, donde se asegura que es posible acceder a cualquier persona del planeta en tan solo seis saltos. Según esta Teoría, cada persona conoce de media, entre amigos, familiares y compañeros de trabajo o escuela, a unas 100 personas. Si cada uno de esos amigos o conocidos cercanos se relaciona con otras 100 personas, cualquier individuo puede pasar un mensaje a 10.000 personas más tan solo pidiendo a un amigo que pase ese mensaje a sus amigos.

Estos 10.000 individuos serían contactos de segundo nivel, que un individuo no conoce pero que puede conocer fácilmente pidiendo a sus amigos y familiares que se los presenten. Este argumento supone que los 100 amigos de cada persona no son amigos comunes. En la práctica, esto significa que el número de contactos de segundo nivel será sustancialmente menor a 10.000 debido a que es muy usual tener amigos comunes en las redes sociales.

[1] Karinthy, Frigyes. Chains, 1929.

Si esos 10.000 conocen a otros 100, la red ya se ampliaría a 1.000.000 de personas conectadas en un tercer nivel, a 100.000.000 en un cuarto nivel, a 10.000.000.000 en un quinto nivel y a 1.000.000.000.000 en un sexto nivel. En seis pasos, y con las tecnologías disponibles, se podría enviar un mensaje a cualquier lugar individuo del planeta.

La primera red social reconocida como tal fue classmates, creada en 1995 por Randy Conrads. Esta red pretendía que los usuarios pudiesen recuperar o mantener el contacto con antiguos compañeros del colegio, instituto, universidad, etc.(Boyd, Danah., & Ellison, Nicole, 2007, p. 4).

Posteriormente, en 1997 se lanzó SixDegrees. Esta red permitía a los usuarios crear perfiles y listas de amigos. En 1998 añade una novedad entre sus aplicaciones, ya que es la primera red que permite navegar por las distintas listas de amigos. La finalidad que perseguía SixDegrees era la de convertirse en una herramienta que ayudase a las personas a conectarse con otras a través de mensajes. Aunque tuvo una expansión muy rápida, atrayendo a miles de usuarios, en el año 2000 dejó de existir. Una de las razones que pudieron justificar su desaparición estaba en el miedo a contactar con desconocidos a través de Internet.

De 1997 a 2001, aparecen varias comunidades que pueden ser entendidas como redes sociales. Al igual que las anteriores todas ellas partían de la creación de un perfil, con sus datos tanto personales como profesionales con el objetivo de hacer posible la comunicación con sus amigos. Entre estas redes encontramos a AsianAvenue, BlackPlanet, y MiGente. Aquí las personas registradas añadían información diferenciando entre datos personales, profesionales y los datos destinados a buscar pareja. AsianAvenue era una red centrada en la comunidad asiática-americana. El mayor número de usuarios que alcanzó fue los 2 millones de personas. BlackPlanet es un sitio web dedicado en exclusiva a la comunidad afro-americana. Comenzó como un lugar para buscar pareja y ofertas de trabajo, pero a medida que fue creciendo creó foros de debate sobre temas políticos y sociales. Los foros más populares eran el de Relaciones Personales, Patrimonio e Identidad, Actualidad, Sociedad y Cultura, y Feminismo. A diferencia del anterior alcanzó una masa social más amplia aunque, unos 20 millones de usuarios, aunque esta cifra no se puede comparar con las redes de hoy en día, era una cifra bastante elevada. MiGente.com estaba dirigido especialmente para la comunidad hispana. Su antigua compañía matriz, Community Connect Inc., afirmó que MiGente.com fue el sitio de más rápido crecimiento en inglés para la comunidad hispana con más de 3 millones de miembros registrados.

En 1999 nace LiveJournal que es la primera en integrar un sistema de mensajería instantáneo (chat) que podía ser utilizado solo por los mejores amigos de cada usuario. También en este año nace Cyworld, una red social coreana que hasta 2001 no añade los desarrollos propios de una red social. A su vez la red social sueca LunarStorm se reformuló como una red social en el año 2000, incluyendo listas de amigos, libros de visitas, y blogs.

Uno de los pasos más importantes en la historia de las redes sociales se produjo en el 2001 con la aparición de Ryze. Esta red pretendía ayudar a sus usuarios a clasificar a sus contactos de negocios. Según su fundador, lo que hizo fue presentar el sitio a sus amigos, que eran miembros de la comunidad empresarial y tecnológica de San Francisco. Siguiendo esta línea de contactos profesionales aparecen otras redes como Tribe.net, LinkedIn, y Friendster, donde se une lo personal con lo profesional.

Friendster se lanzó en el año 2002 como complemento social a Ryze. El objetivo principal era competir con Match.com, una red social creada para buscar pareja. La diferencia con esta última, era que Friendster ayudaba a encontrar amigos de amigos, llegando a un segundo nivel de contactos, ya que se pensaba que estos amigos de amigos podrían tener más en común que con personas totalmente desconocidas.

En un principio se diseño para que los usuarios solo pudieran ver los perfiles de las personas que no se localizasen a más de cuatro grados de distancia (amigos de amigos de amigos de amigos). Pero, con el fin de poder ver todos los perfiles, los usuarios comenzaron a agregar a gente desconocida. Debido a esto, Friendster se hizo muy popular rápidamente. Pero sus creadores no estaban preparados para un crecimiento tan rápido, por lo que fue perdiendo adeptos a la misma velocidad con la que se habían ido integrando en la red.

A partir del año 2003 van a surgir muchas redes sociales nuevas. Todas partían de una característica común, la necesidad de tener un perfil personal, y con un objetivo común, repetir el éxito que había tenido Friendster. De forma paralela continuaban con su labor las redes profesionales como LinkedIn, Visible Path y Xing, destinadas más a la parte profesional centrándose en la gente de negocios.

Las redes sociales adquieren cada vez más popularidad. En 2003 aparece MySpace, donde los usuarios pueden crear sus propias páginas personales. MySpace nació para competir con otras redes como Friendster, Xanga y AsianAvenue, siendo uno de los objetivos iniciales atraer a todos los usuarios que estaban insatisfechos con el funcionamiento de Friendster.

Otro hecho destacable es que en esta época comienzan a aparecer fenómenos que crecen con gran rapidez como son los medios de comunicación social y los contenidos generados por los usuarios, que llevan a la creación de plataformas que añaden características propias de las redes sociales convirtiéndose con el paso de los años ellas mismas en redes sociales. Es el caso de Youtube (para compartir videos), Flickr (para compartir fotos) y Last.FM (hábitos de escuchar música)

En el año 2004 Google lanza su propia red social Orkut, que no tuvo tanto impacto como sus creadores pensaban, a excepción de Sudamérica, siendo en Brasil donde más popularidad alcanzó. Al año siguiente Yahoo no quería quedarse atrás y lanzó Yahoo 360º pero tuvo menos éxito que Orkut.

En el año 2004 nace Facebook. Quizás esta red se convierte en el punto de inflexión de lo que eran las redes sociales y lo que serán después. Facebook se ha convertido en la red social con más usuarios registrados alcanzando a día de hoy 650 millones de usuarios, a pesar de haber nacido como una red para conectar a los usuarios de Harvard.

En estos años se han ido desarrollando redes sociales propias en cada país. En España tenemos el caso de Tuenti, que nace en el 2006 y está destinada principalmente para jóvenes; Mixi se adoptó en Japón de forma generalizada, LunarStorm en Suecia, los usuarios holandeses se unieron a Hyves, Grono conectó a los usuarios en Polonia, hi5 fue adoptado en los países más pequeños de América Latina, América del Sur y Europa y Bebo se hizo muy popular en el Reino Unido, Nueva Zelanda y Australia.

Además, estos últimos años han supuesto el despegue de las redes sociales basadas en el microblogging, donde destaca por encima de todas Twitter, que se está convirtiendo en un fenómeno social, y ha llegado ya a superar los 200 millones de usuarios, aunque en mi opinión nunca llegará a tener tantos usuarios como Facebook.

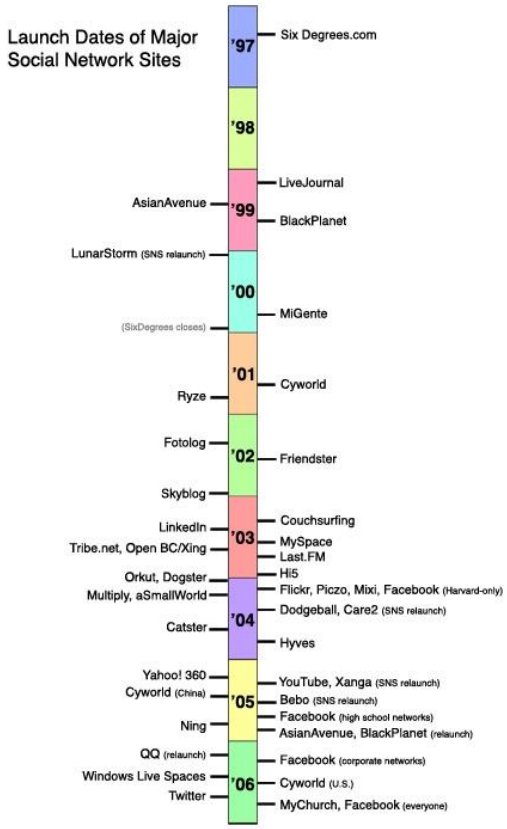


Fig.1 Evolución de las redes sociales según Ellison Boyd (2007)

En resumen, como hemos podido comprobar a lo largo de un corto espacio de tiempo han surgido muchas redes sociales, algunas de ellas han tenido éxito y se mantienen y otras, en cambio, no han tenido la misma suerte y han desaparecido. Las redes sociales pioneras creadas a finales del siglo XX abrieron un camino que en los años posteriores ha sido aprovechado por el resto de redes. Después de todos estos años, las redes sociales se han convertido en uno de los elementos de Internet más difundidos, ya que ofrecen a sus usuarios un lugar común para desarrollar comunicaciones constantes.

PARTE 2

LA REVOLUCIÓN DE LAS REDES SOCIALES: FACEBOOK

Capítulo 5
Orígenes y evolución de Facebook

El 4 de febrero de 2004 nacía en una habitación de Kirkland House, una de las residencias para estudiantes de Harvard, Facebook, probablemente la mayor red social online que ha aparecido hasta hoy. Creado por Marc Zuckeberg y fundado por Eduardo Saverin, Chris Hughes, Dustin Moskovitz y el propio Zuckerberg. El objetivo inicial con el que nació era conectar a los distintos estudiantes de universidades norteamericanas como Harvard, Columbia, Stanford y Yale.

Originalmente su nombre fue TheFacebook, pero éste no era el primer proyecto en el que se adentraba Marc Zuckeberg, sino que un año antes, en 2003, creó Facemash, un sitio en Internet donde podías calificar a los estudiantes de 1 a 10 según fuera su atractivo. Pero esta idea, no tan original, ya que era una copia de la web “Hot or Not”, no tuvo tanto éxito, quizás porque solo estaba destinada para los alumnos de Harvard. Además durante este periodo tuvo problemas con la administración de Harvard debido a que copió, sin autorización previa, las fotos de todos los estudiantes de Harvard de las bases de datos de la Universidad, por lo que la web quedó cerrada.

TheFacebook.com se desarrollo de una manera vertiginosa. En el primer día desde su lanzamiento ya había registrada cerca de 1200 personas. Visto que sólo estaba destinada a los estudiantes de Harvard, la cifra es importante.

En la pantalla inicial se podía leer el siguiente mensaje: «Thefacebook es un directorio online que conecta a la gente a través de las redes sociales universitarias. Hemos abierto Thefacebook para su uso popular en la Universidad de Harvard. Puedes utilizar Thefacebook para: buscar a gente en tu propia universidad, saber quién hay en tus clases, buscar a los amigos de tus amigos, ver una visualización de tu red social.».

Fig. 2 Página inicial Facebook 2004 (Blog de Facebook)

Para poder registrarte se necesitaba un perfil en el que tenías que añadir una fotografía junto con algunos datos personales. En este apartado indicabas tu estado sentimental, pudiendo elegir entre las distintas opciones que se te mostraban en el fichero desplegable (soltero, en una relación o en una relación abierta). Además podías añadir tu número de teléfono, tu número de usuario de Harvard y tu dirección de correo electrónico; indicar las clases a las que ibas a asistir; tus libros, películas y música favoritos; clubes a los que pertenecías; orientación política: muy progresista, progresista, moderado, conservador, muy conservador o indiferente; y una frase favorita.

Algo que distinguía a TheFacebook de todas las otras redes sociales que habían aparecido hasta entonces era la privacidad. Para poder registrarte era necesario tener una cuenta de correo Harvard.edu y la obligación de utilizar tu nombre real. En TheFacebook podías establecer tus opciones de privacidad para determinar exactamente quién podía acceder a tu información. Podías limitarlo a los estudiantes actuales, a sólo la gente de tu clase o a sólo los alumnos de tu residencia. Esto era lo que le hacía diferente de Friendster y MySpace.

Poco a poco se fue extendiendo. La siguiente universidad a la que abrieron el servicio fue a Columbia, el día 25 de febrero; el día siguiente se abrió en Standford y el día 29 en Yale.

El 30 de noviembre de 2004 alcanzó la cifra de 1 millón de usuarios registrados. Tan solo diez meses después de haberse creado.

En 2005 eliminan el artículo “The” para registrar el producto tal y como lo conocemos hoy en día “Facebook”. A finales de este año se inicia una expansión de Facebook, ya que abren la red social para colegios, llegando a alcanzar 5,5 millones de usuarios. En total un 85 % de los alumnos estadounidenses ya eran usuarios de Facebook, mientras que el 60 % lo consultaba diariamente. En este año se produce uno de los hechos que más caracterizan a la red social, el etiquetado de fotos. De esta forma, cualquier usuario registrado podía subir fotos a Facebook y etiquetarte en ellas. Entonces había dos maneras de demostrar si eras popular o no, la primera viendo los amigos que tenías, y la segunda, viendo las veces que te etiquetaban en sus fotos.

Fig 3. Perfil Facebook año 2005 (Blog de Facebook)

Probablemente el año que mayor cambio supuso para Facebook fue el 2006. En este año se produce la apertura definitiva. La red se expande, pasando de estar dirigida a una población académica a una población general. En agosto de 2006 Facebook abre sus puertas a toda la población, causando esta medida fuertes protestas debido a que perdía el principal motivo por el que fue creada, ser una plataforma con una base estudiantil.

También en este año aparecen aplicaciones importantes, como la opción de vincularse con amigos o conocidos a través de redes comunes, como redes de trabajo, colegio, universidades, etc. Más tarde esto se ampliaría a comunidades, ciudades, estados o países. De este modo podías ordenar a tus amigos en Facebook según la red o la

vinculación que tienes con ellos, separando a quienes son conocidos del trabajo, universidad o de tu pueblo.

Además se lanzó la opción News Feed, que permitía que los usuarios viesen, en su muro principal, qué es lo que sus amigos han dicho, hecho o publicado en Facebook recientemente.

Otro hecho importante ocurrido durante este año, es que se activa la opción para compartir contenido como, fotos, videos, blogs, y links de cualquier página web en tu perfil de Facebook.

El número de usuarios sigue creciendo llegando ya a los 12 millones de registrados.

Fig. 4 Página inicial Facebook año 2006 (Blog de Facebook)

A partir de 2007 los usuarios siguen creciendo a un ritmo vertiginoso. Para satisfacer las demandas de los usuarios se realizan una serie de mejoras en la web, como pueden ser la interfaz y plataforma electrónica para recibir y enviar mensajes a otros usuarios de Facebook. Además se desarrolla la plataforma para construcción de aplicaciones de terceros. Desde ese momento los programadores de todo el mundo

pueden desarrollar sus propias aplicaciones y juegos para que sean de libre uso para usuarios de Facebook.

Otra de las medidas que contribuyen la expansión de Facebook es que se lanza la interfaz para abrir Facebook en dispositivos móviles como móviles, PDA´s, etc.

También en este año se empieza a rentabilizar, todavía más, la marca. Presentan Facebook Ads o Anuncios Facebook. Mediante esto en el lateral derecho de la página de Facebook se despliegan anuncios comerciales de marcas y empresas. Los anuncios que son mostrados al abrir tu perfil dependen del lugar donde vivas, mostrando sólo anuncios relacionados a tus redes en Facebook.

El número de usuarios sigue creciendo y ya llega hasta los 50 millones de usuarios registrados.

Fig. 5 Perfil Facebook año 2007 (Blog de Facebook)

En el año 2008 los usuarios de habla hispana ven colmadas sus expectativas ya que se lanza la versión de la página en español. Sería la primera página en otro idioma distinto al inglés. Meses después se lanzarían las versiones en alemán y en francés.

También aparece en este año una de las aplicaciones más importantes de Facebook, el chat, que te permite mantener conversaciones en tiempo real, por medio de

mensajes de texto, con los usuarios que se encuentran usando su Facebook al mismo tiempo que tú.

Durante estos 365 días, los usuarios registrados en Facebook se duplican, llegando a los 100 millones de usuarios registrados.

Fig. 6 Página de inicio Facebook año 2008 (Blog de Facebook)

En el 2009 se produce el boom en relación a los usuarios registrados. Es el año que más crecimiento conlleva. Se pasa de 100 millones a 350 millones de usuarios en tan sólo un año. Parece que todo el mundo quiere pertenecer a Facebook, teniendo sus propios perfiles, compartiendo sus gustos, preocupaciones, etc.

Las empresas lo ven como una posibilidad de hacer llegar sus negocios a una cantidad importante de la población, por ello crean sus propias páginas donde mostrarán parte de sus productos, ofreciendo ventajas a aquellos usuarios amigos.

En este año se añade la opción de 'Me Gusta', por medio de la cual puedes comentar en las publicaciones de otros usuarios y hacerles saber que te gusta dicha publicación. Además, otra de las aplicaciones lanzadas durante este 2009 es la de nombres de usuarios, que permite que sea más fácil encontrar el perfil de cada usuario dándoles una dirección web. Ej.: www.facebook.com/usuario.ficticio.

Fig. 7 Página de inicio Facebook año 2009 (Blog de Facebook)

En el año 2010 lo más destacado en cuanto a aplicaciones es que se puso en marcha 'Lugares' que te permite saber qué actividades, espectáculos, restaurantes, clubes hay cerca de ti, basado en los datos de ubicación que proporciones a Facebook.

Por lo que respecta a usuarios, este pasado año se llegó a la nada despreciable cifra de 500 millones de usuarios registrados.

Fig. 8 Página de inicio Facebook año 2010 (Blog de Facebook)

En el año 2011 Facebook sigue creciendo de forma acelerada. En la actualidad cuenta con 650 millones de usuarios y se cree que pueda llegar a 700 millones a finales de este año.

Fig. 9 Página de perfil Facebook año 2011 (Blog de Facebook)

En palabras del propio Marc Zuckerberg, “Facebook es un servicio público. Tratamos de mejorar la eficiencia a través de la cual la gente pueda comprender su mundo. No tratamos de maximizar el tiempo pasado en nuestra página web; tratamos de ayudar a que la gente disfrute de una buena experiencia y a que saque el máximo provecho de esos instantes”. (Blog de Facebook, 2010)

Además de ser una red donde puedes contactar con amigos, se ha convertido en una herramienta más de marketing para que las empresas ya que éstas puedan interactuar de una forma más directa con los consumidores promocionando sus productos y servicios a través de una relación más cercana.

Algunos datos importantes sobre Facebook[23]:

- La media de amigos por usuario es de 130

[2] Confacebook.com, estadísticas sobre Facebook, 2011

[3] Estadísticas oficiales de Facebook: https://www.facebook.com/press/info.php?statistics

- En todo el mundo, la gente pasa más de 700 billones de minutos en Facebook al mes
- De media, los usuarios de Facebook están conectados a 80 páginas, grupos o eventos
- El 50% de los usuarios activos acceden a Facebook a cualquier hora del día
- Más de 30 billones es la cantidad de contenido generado y compartido cada mes en Facebook por sus usuarios, como contenido se entiende (enlaces web, notas, post en blogs, fotos, etc.)
- Facebook está traducido en más de 70 idiomas
- Alrededor del 70% de los usuarios de Facebook están fuera de USA
- Cada mes, más del 70% de usuarios utilizan aplicaciones de Facebook
- Dos tercios de las 100 principales webs americanas tienen integración con Facebook
- Más de 200 millones de usuarios acceden a Facebook a través de dispositivos móviles
- Los usuarios que tienen Facebook en sus móviles o smartphones son el doble de activos que los usuarios que no acceden a través de estos dispositivos
- Hay más de 200 operadores móviles, de 60 países, que trabajan en el desarrollo de aplicaciones y en la integración de sus servicios en Facebook
- Facebook roza los 2.000 empleados
- La valoración de Facebook está entre 7.9 y11 billones de dólares…y subiendo
- Hay más de 3 millones de páginas creadas, activas, en Facebook
- Las páginas de Facebook cuentan con más de 5.3 billones de seguidores
- La media de tiempo que empleamos en Facebook al día es de 55 minutos
- Las mujeres publican un 55% más (noticias, estados, fotos, etc…) que los hombres
- Más de 6 billones de minutos son empleados en Facebook cada día
- Más de 3 billones de fotos se suben a Facebook cada mes
- USA es el país con más usuarios de Facebook, con 150 millones
- El 26.22% de los usuarios de Internet lo son de Facebook

Los países que más usuarios registrados tienen en Facebook son:

- Estados Unidos (155,222,920 usuarios registrados)
- Indonesia (36,533,680 usuarios registrados)
- Reino Unido (29,745,780 usuarios registrados)
- Turquía (28,464,140 usuarios registrados)
- India (25,664,320 usuarios registrados)
- México (24,179,360 usuarios registrados)

- Filipinas (23,412,640 usuarios registrados)
- Francia (21,990,600 usuarios registrados)
- Italia (19,237,280 usuarios registrados)
- Alemania (18,642,320 usuarios registrados)

Fig.10 Países con más usuarios en Facebook (Blog de Facebook)

A principios del mes de julio de 2011 el número de usuarios activos en España (los que en los últimos días se han conectado al menos una vez) ha subido, situándose en 14.329.629. Casi un 4% más respecto al mes de mayo, cuando el número de usuarios se situó en 13.782.580. Destacar que el 31% de la población total de España, (según el Instituto Nacional de Estadística 46.148.605 personas) son usuarios de Facebook. (Estadísticas Cuéntame la red, julio 2011).

Otros datos que merecen ser reseñados en relación al uso de Facebook en España son los siguientes:

- Paridad en el reparto de usuarios de Facebook en España por sexo: el 49 % de usuarios son varones y el 50% mujeres. El 1% de usuarios no manifiesta su sexo.

- El grupo más común en Facebook está formado por mujeres y hombres de entre 25 y 34 años. En segundo lugar está el intervalo de 35 a 44 años y en tercer lugar el grupo de 19 a 24 años.

- El número de usuarios registrados en 5 de las principales ciudades (Madrid, Barcelona, Valencia, Sevilla y Bilbao) sigue creciendo, ya abarcan el 74 % de los españoles en Facebook.

En definitiva, Facebook ha crecido a un ritmo vertiginoso y se ha convertido en la red social con más usuarios del momento. Desde su creación en el año 2004 como un servicio exclusivo para estudiantes de Harvard, con el paso de los años ha ido ganando adeptos hasta alcanzar una cifra superior a los 650 millones de usuarios.Además, destacar que se ha asentado como la primera red social en cuanto a seguidores y a utilización.

Capítulo 6
Principios de Facebook

De las informaciones que se encuentran en su página web (www.facebook.com), podemos señalar que esta red social se basa sobre una serie de principios que definen los valores por los que fue creada. Facebook promueve la sinceridad y la transparencia ofreciendo a los individuos un mayor poder para comunicarse y compartir. Los 10 pilares sobre los que se asienta Facebook, que analizaremos a continuación, son claves para cumplir los objetivos que desde un principio diseñó Mark Zuckerberg. Lo más importante es que estos principios se deben adaptar a las distintas leyes de los países donde se encuentre Facebook. Son los siguientes:

1. Libertad para compartir y conectarse

   Este es el principio básico por el que se creó Facebook. Conseguir que cualquier persona pudiera comunicarse con amigos compartiendo toda la información que deseen. Entre las afirmaciones que se realizan se necesita como una condición primordial que las distintas partes que quieran mantener relación deben consentir la conexión.

2. Propiedad y control de la información

   Este principio establece una de las cualidades necesarias para el buen desarrollo de la red social. Según establece Facebook “las personas deben ser propietarias de su información. Deben tener libertad para compartirla con cualquiera que ellos decidan, llevarla consigo a cualquier lugar e incluso retirarla del servicio de Facebook. Las personas deben tener libertad para decidir con quién quieren compartir su información y para establecer los controles de privacidad que protejan sus decisiones”.

3. Flujo libre de información

   Desde una perspectiva ligada a la privacidad se puede poner una serie de matices a este principio. En teoría toda persona puede tener total libertad para

acceder a la información que los otros usuarios pongan a su disposición, siempre que estos no lo hayan configurado de otra forma, ya que las opciones básicas de configuración que predetermina Facebook se establecen en un nivel muy bajo de privacidad. Para ayudar a que se produzca este flujo es necesario contar con unas herramientas eficaces que lo hagan posible, pudiendo acceder a la información de una manera más fácil, rápida y eficaz.

4. Igualdad fundamental

   Todas las personas que están registradas en Facebook serán consideradas por igual independientemente de si se trate un individuo, anunciante, desarrollador, organización u otra entidad. Por ello existe una serie de principios, derechos y responsabilidades que se apliquen a todas las personas que utilicen el servicio de Facebook.

5. Valor social

   Cada persona creará su propia identidad con una absoluta libertad. Esta identidad no se podrá retirar de la red a no ser que no cumpla las distintas políticas que establece Facebook, como puede ser que atente contra el honor de cualquier ser humano.

6. Plataformas y estándares abiertos

   Todos los usuarios deben estar provistos de herramientas que les permita el acceso a la información que Facebook pone a su disposición. Además estas herramientas deben ser accesibles para todos.

7. Servicio fundamental

   Otro de los principios más importantes de Facebook. El servicio que presta Facebook es gratuito con el fin de que cualquier persona puede registrarse, conectarse con otros usuarios y compartir información con ellos. Además, se afirma que “toda persona tiene que poder utilizar el servicio de Facebook, independientemente de su nivel de participación o contribución”.

8. Bienestar común

   Facebook recoge que “los derechos y responsabilidades de Facebook y de las personas que lo utilizan deben describirse en una Declaración de derechos y responsabilidades, que tiene que ser coherente con estos principios”.

9. Proceso transparente

   Con el deber de ser un medio transparente, Facebook hará público cuáles son sus propósitos, planes, políticas y operaciones. Estos aspectos deberán ser comunicados de forma que todos los usuarios tengan acceso a ellos, creando mecanismos para que los usuarios puedan dar su opinión acerca de las modificaciones que se produzcan en la red.

10. Un mundo

    Facebook se ha creado con el objetivo de que todas las personas puedan estar comunicadas entre sí. Por ello, Facebook pretende romper las barreras nacionales y geográficas y estar a disposición de todo el mundo.

Destacar de estos puntos principales de Facebook, que a la hora de ponerlos en práctica, hay algunos de ellos que, o bien no se cumplen, o se cumplen a medias. El punto número dos, el usuario no tiene tanta libertad como predica ese principio, ya que cuando una persona quiere eliminar contenido de su perfil, aunque desaparezca de la vista pública, las copias de seguridad que Facebook realiza siempre mantendrán esa información eliminada.

También debemos mencionar el punto número 9, ya que no siempre han actuado de un modo transparente, puesto que ha ocurrido en ocasiones que Facebook ha hecho pruebas en el diseño o en el desarrollo de nuevas aplicaciones y los usuarios no habían sido previamente informados, como es el caso del lanzamiento de la nueva aplicación de reconocimiento facial por la que se reconoce automáticamente a los usuarios en las fotografías.

La filosofía de transparencia y sinceridad que se le ofrecía a los usuarios de Facebook en sus principios han quedado obsoletos. La red ha crecido tanto que hay algunos de estos principios que ya no se cumplen, porque a pesar de lo que predican el usuario cada vez tiene menos control sobre su información y el proceso de comunicación nos tan transparente como en un principio se detallaba, porque cada vez ocurre más que Facebook se preocupe por sus intereses y no preste atención a lo que realmente debería ser importante, la satisfacción de sus usuarios.

PARTE 3

EL DERECHO A LA PRIVACIDAD EN FACEBOOK

Capítulo 7
Intimidad y privacidad

El término privacidad tiene un origen reciente. De hecho, el Diccionario de la Real Academia Española (en adelante, DRAE) no lo aceptó como tal hasta el año 2001. La definición que nos ofrece es la siguiente: “ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión”.

Aunque en España tenga un inicio reciente, el origen del término privacidad se halla en la palabra anglosajona *privacy* y ha sido reconocido como derecho en el ordenamiento jurídico norteamericano.

En concreto, en los Estados Unidos de América el *right to privacy* o derecho a la privacidad fue desarrollado por primera vez en un conocido artículo jurídico de 1890 realizado por Warren y Brandeis y considerado por el juez Cooley como el derecho a ser dejado solo, a ser dejado en paz, como “The right to be alone”. (Warren y Brandeis “The Right to Privacy” Harvard Law Review, vol. IV, núm. 5 pp. 193 a 219; 15 Diciembre 1890 en López Jiménez, 2009, p. 239).

Basado en el citado artículo y siguiendo el peculiar sistema de creación de derecho anglosajón, basado tanto en el precedente judicial como en la propia ley, se fue reconociendo el citado derecho en el sistema norteamericano, incorporando principios como la inviolabilidad del domicilio, la correspondencia o, más recientemente, las telecomunicaciones (Salgado Seguín, 2010, p. 3)

Siguiendo con lo anterior, si realizásemos una traducción al castellano de la palabra *privacy* podíamos comprobar que hace referencia al concepto intimidad. Pero, el caso es que se creó esta palabra porque privacidad se refiere a algo distinto a intimidad.

El derecho a la intimidad se entendió inicialmente por doctrina y jurisprudencia como un bien ordenado a la protección de lo más interno y reservado de las personas.

Posteriormente la jurisprudencia y la evolución social han definido un derecho a la intimidad de contenido amplio y textura abierta cuyas manifestaciones son múltiples. En tal sentido, la relación de la intimidad con la propia imagen, los conflictos que se dan en el caso del ejercicio del derecho a la información y de la libertad de expresión, la práctica de pruebas corporales en el ámbito penal, la protección de la salud y la investigación genética, y la protección de la dimensión familiar han extendido la tutela de este derecho a un ámbito más amplio.

La regulación española de estos temas se inicia con la Constitución de 1978. El artículo 18 de la Constitución Española (en adelante, CE) se ordena a la protección de distintos bienes de la personalidad siendo su objeto garantizar una esfera de libertad individual que protege por una lado la vida privada de las personas y les otorga, de otro, facultades que permiten ejercer un control material sobre el tratamiento de su información personal. En el precepto conviven manifestaciones clásicas de los derechos de la personalidad, - derechos al honor, a la intimidad personal y familiar y a la propia imagen-, una esfera de protección frente a las injerencias en ámbitos específicos, -inviolabilidad del domicilio y secreto de las comunicaciones-, y un derecho de última generación definido por el Tribunal Constitucional como derecho fundamental a la protección de datos. Las tecnologías de la información no sólo se proyectan sobre el último derecho citado, sino que afectan también a la conformación constitucional de las dos primeras categorías.

Por el contrario, el derecho a la protección de datos, regulado en el artículo 18.4 de la Constitución, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley. De esta forma, supone el "derecho a controlar el uso que se realice de sus datos personales, comprendiendo, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención"[4]

La intimidad es, de estos dos conceptos, el que tiene un alcance menor. Es decir, el derecho a la intimidad protege la parte más íntima de una persona, esto es, esa esfera personal que define qué es y qué no es privado. Dicho de otra forma, hablar de intimidad es hablar de sentimientos, de creencias (políticas, religiosas), pensamientos o de una información –como la clínica o la relativa a la vida sexual- cuya difusión puede producir ciertas reservas al individuo. Se trata en definitiva de aquellos datos que bajo ninguna circunstancia proporcionaría un individuo de manera libre y consciente. Partiendo de este punto, nacen derechos como la inviolabilidad de las

[4] Extracto de la Sentencia del Tribunal Constitucional 292/2000 donde se reconoce el Derecho a la Protección de Datos, como un derecho fundamental absolutamente independiente del Derecho al Honor, Intimidad y Propia Imagen, otorgando así a la protección de datos de carácter personal, una entidad absolutamente independiente del resto de derechos.

comunicaciones o el derecho a la propia imagen; ambos muy relacionados con la parte más privada de la psicología del individuo.

La privacidad, sin embargo, es un término más amplio: se refiere a aquella parte del individuo que va más allá de lo íntimo, esto es, información que tomada por si misma puede no ser relevante, pero que analizada en un momento o contexto concretos puede llevarnos a la construcción de un perfil muy fiable del individuo. Así, si al hablar de intimidad poníamos como ejemplos los sentimientos o creencias, podríamos ilustrar el concepto de privacidad con los libros que se consultan, las películas que se alquilan, las asociaciones a las que se pertenece, etc. Por sí solos, estos datos no tienen excesivo valor; ahora bien, tomados en conjunto, en un ambiente determinado, pueden hablarnos de los gustos del individuo, de sus preocupaciones o necesidades. En cualquier caso, sin llegar a esa zona reservada que define la intimidad.

Podríamos concluir que los asuntos íntimos son privados, pero que no todos los asuntos privados son íntimos. Hecha esta distinción, es el momento en el que entra en juego el derecho a la protección de datos de carácter personal. (Battaner, 2006, p.2)

Según se recoge en la Sentencia 292/ 2000 emitida por el Tribunal Constitucional, el derecho a la privacidad atribuye a su titular la facultad de controlar el uso que se realice de sus datos personales, comprendiendo, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquél legítimo que justificó su obtención.

La privacidad sería así una nueva esfera, mucho más amplia que la de la propia intimidad, que contendría ni más ni menos que todos los datos vinculados a un individuo, sean éstos sensibles o no, los cuales deben ser controlados y protegidos en su tenencia y tratamiento por parte de terceros. (Salgado Seguín, 2010, p.5)

Todas estas ideas sentaron las bases de lo que el Tribunal Constitucional ha definido como un derecho fundamental autónomo: el derecho a la protección de datos de carácter personal, también conocido como derecho a la privacidad.

Según el Tribunal Constitucional el objeto del derecho a la protección de datos alcanza: "a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo". (Tribunal constitucional, Sentencia 292/2000).

Dado que una vez que nos registramos en una red social y comenzamos a interactuar con ésta, la cantidad de datos personales que añadimos a nuestros perfiles es enorme, esa información se convierte en una identidad digital que facilita un rápido conocimiento de datos de contacto, preferencias y hábitos del usuario. Entre los datos personales que añadimos estaría nuestro nombre, fecha de nacimiento, fotografías, opiniones acerca de nuestra tendencia política o creencias religiosas.

Además debe considerarse que durante la prestación de estos servicios se recopilan datos como la dirección IP, que se utilizan para segmentar la publicidad que se dirige a los distintos tipos de usuarios, así como aumentar el grado de contacto entre los usuarios registrados.

El marco legal en materia de protección de datos responde a la necesidad de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar, evitándose así que los datos sean utilizados de forma inadecuada o fraudulenta, o sean tratados o cedidos a terceros sin consentimiento inequívoco del titular (Agencia Española de Protección de Datos, 2009, p.94).

7.1 La regulación europea de la privacidad

A nivel europeo, la norma pionera en este sentido e inspiradora de todo el desarrollo legislativo posterior fue el Convenio 108 del Consejo de Europa (CoE), de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal. No en vano, desde el seno de esta institución venían desarrollándose iniciativas en este sentido desde finales de la década de 1960, a través de Resoluciones y Recomendaciones, tanto generales como sectoriales, aunque sin fuerza vinculante; o de la jurisprudencia del Tribunal Europeo de Derechos Humanos, que ha venido a dar acogida “constitucional” al derecho a la protección de datos de carácter personal a través del Convenio Europeo de Derechos Humanos (en adelante, CEDH) -concretamente, entendiéndolo comprendido en el derecho al respeto a la vida privada y familiar reconocido en su art. 8-. Pero fue, como ha quedado dicho, el Convenio 108 el primer instrumento que desplegó una eficacia jurídica efectiva en esta materia, convirtiéndose en “uno de los pilares jurídico-positivos de carácter internacional” sobre la protección de datos de carácter personal (Castillo, 2007, p. 87).

El Convenio fijó los principios básicos para la protección de datos, como el de calidad o el de seguridad; los derechos de acceso, rectificación y cancelación; la protección de los datos que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual; o la fijación de procedimientos de salvaguarda.

Guichot (2005, pp.36-39) ha destacado tres claves del Derecho del Consejo de Europa en esta materia, que marcarán además su impronta en nuestra normativa nacional. En primer lugar, no se encuentra claramente delimitada la relación entre derecho a la protección de datos y derecho a la intimidad. Para Guichot - que entiende como sinónimos las expresiones "vida privada" (que es la empleada en el Derecho del Consejo de Europa) e "intimidad"- se habría producido (o se está produciendo) una ampliación del ámbito de lo "íntimo" con respecto al reducto clásico, tanto desde un plano objetivo (lo que la Ley considera perteneciente al ámbito de la intimidad) como subjetivo (lo que cada individuo considera que forma parte de su intimidad).

La protección de datos es necesaria, primordialmente, frente a los tratamientos automatizados, que permiten un almacenamiento y cruce de información ilimitados, pero no sólo frente a este género de tratamientos, sino a cualquiera de ellos. A pesar de que "el Convenio reduce su ámbito de aplicación objetiva a los datos que sean sometidos a tratamiento automatizado" y por tanto, en sentido contrario, "niega su protección a los datos de carácter personal que no sean sometidos a un tratamiento automatizado" (Castillo, 2007, p. 89), al tratarse de una norma de mínimos, daba la opción a los Estados de ampliar o no su aplicación a los tratamientos "manuales".

Guichot (2008, p. 45) indica que resulta difícil precisar el contenido del derecho a la protección de datos en el Derecho del Consejo de Europa y el alcance de los posibles límites (recogidos en el art. 9). El contenido mínimo de este derecho podría articularse en tres ejes –que serán también los pilares de la normativa posterior:

- Regla de la calidad de los datos (art. 5), estructurada en los siguientes principios:
    - Principio de veracidad: los datos serán exactos y se actualizarán si fuera necesario.
    - Principio de seguridad: se establecerán las medidas de seguridad pertinentes para permitir la integridad de los datos y evitar los accesos, modificaciones y difusiones no autorizadas.
    - Principio de finalidad: los datos únicamente serán recogidos para fines determinados y legítimos, y no se utilizarán para finalidades incompatibles con aquéllas; serán adecuados, pertinentes y no excesivos con los mismos; etc.
- Facultades destinadas a garantizar a los ciudadanos el respeto de los principios anteriormente señalados (art. 8); singularmente, los derechos de acceso, rectificación y cancelación.

- Garantías institucionales: autoridad independiente de control, sistema sancionador, etc.

También dentro del marco de la Unión Europea el artículo 8 de la Carta Europea de Derechos Fundamentales reconoce de modo específico el derecho a la protección de datos como un derecho autónomo del derecho a la vida privada, donde se reconoce que:

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.

2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.

3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».

La Unión Europea publicó en el año 1995 la 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 éstos datos, con la finalidad de que los Estados miembros armonizasen y adaptasen sus legislaciones internas en materia de protección de datos de carácter personal.

Este texto constituye un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea (UE).

Los aspectos clave de la última normativa comunitaria en materia de protección de datos son:

- El establecimiento del principio de calidad de los datos, de tal forma que los datos personales deben ser adecuados, pertinentes y no excesivos, conforme a la finalidad para la que serán tratados.

- Se impone como principio básico y esencial para el tratamiento de datos personales, la existencia del consentimiento previo del titular de los datos.

- Se requiere a los Estados que establezcan la obligación de conciliar el derecho a la intimidad en el tratamiento de los datos personales con el derecho a la libertad de expresión.

- Se establecen como principios básicos de los ciudadanos los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) en relación a sus datos personales.

- Se incorpora como principio básico la garantía de confidencialidad, así como la obligación de implantar las medidas de seguridad oportunas que garanticen que el acceso a la información se encuentra limitado y controlado.

- Se enuncian los principios básicos para la creación de las Autoridades Nacionales de Protección de Datos.

- Se fijan las bases de las transferencias internacionales de datos personales.

- Se promueve la elaboración de códigos de conducta sectoriales, destinados a contribuir a la correcta aplicación de las disposiciones nacionales en materia de protección de datos personales.

- Se crea el Grupo de Trabajo del Artículo 29 institución de referencia en esta materia.

7.2 El ordenamiento jurídico español

A nivel nacional, en España la configuración del derecho a la protección de datos de carácter personal se produjo, como ya hemos señalado, sobre la base de una temprana previsión constitucional de una limitación legal del uso de la informática "para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos" (art. 18.4 CE) que, sin embargo, contrasta con el tardío desarrollo normativo.

En España, la regulación sobre protección de datos de carácter personal se articula en dos normas principalmente:

- La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).

- Real 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).

Aunque anteriores a éstas debemos hacer mención a la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (en adelante, LORTAD) para que nuestro país contara con su primera norma de protección de datos.

Podemos considerar que la LORTAD constituye el acta de nacimiento de un nuevo derecho en nuestro ordenamiento jurídico, aún insuficientemente definido, y ligado al derecho fundamental a la intimidad. Así, la Ley "presentaba a la vez su objeto como la protección de la intimidad ante los nuevos desafíos y como la garantía de un derecho distinto, el derecho a la privacidad" (Guichot 2005 p. 66).

La aprobación de la Directiva 95/46/CE hizo necesaria la adecuación de la normativa española a sus términos, a pesar de que, como hemos señalado, la LORTAD había tenido en cuenta el proyecto inicial de la norma comunitaria. De forma que se procedió a su trasposición –aunque con retraso con respecto al plazo de tres años establecido a tal efecto- mediante la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (LOPD). Esta Ley, "respetando el grueso de la LORTAD, se limitó a adaptar el texto a las diferencias existentes con la Directiva y a introducir algunas otras modificaciones" (Guichot, 2005, p. 64). En síntesis, las diferencias básicas que introduce con respecto a la LORTAD son (Guichot, 2005, pp. 170-171):

- Aplicación de la normativa a los ficheros no automatizados (contemplada por la Directiva 95/46/CE).

- Reconocimiento de nuevos derechos a los afectados: el derecho a la información en la recogida de datos y el derecho de oposición.

- Permite el tratamiento de datos para usos no incompatibles con la finalidad para la que fueron recabados.

- Se flexibiliza la aplicación de los principios y garantías respecto a determinados tratamientos privados (censo promocional a disposición de las empresas de marketing directo y publicidad, ficheros comunes de aseguradoras sin consentimiento del afectado, etc.)

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Siguiendo el análisis que la AEPD elaboró junto al INTECO (2009, pp. 104-107) sobre la LOPD podemos señalar que todo tratamiento de datos de carácter personal debe atender a una serie de principios básicos:

- Calidad de los datos: es esencial que los datos personales tratados sean adecuados, pertinentes y no excesivos, en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan

obtenido, no pudiendo usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recabados. Los datos deberán responder con veracidad a la situación actual del afectado debiendo rectificarlos si se constatan errores. Sólo podrán ser recogidos para el cumplimiento de finalidades determinadas, explícitas y legítimas del responsable del tratamiento, prohibiéndose la recogida de datos por medios fraudulentos, desleales o ilícitos. Por otra parte, el responsable debe conservar los datos personales mientras subsista la finalidad y cancelarlos cuando esta cese.

- Información en la recogida de datos: el afectado será informado, en el momento en el que se recaben sus datos, del alcance del tratamiento que se va a realizar. El art. 5 de la LOPD establece que "los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

  - ✓ De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
  - ✓ Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
  - ✓ De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
  - ✓ De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
  - ✓ De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante".

- Consentimiento del afectado o manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de sus datos personales.

- Datos especialmente protegidos, este principio hace referencia a datos de carácter personal que revelan la ideología, afiliación sindical, religión, creencias, -caso para el que el consentimiento debe ser expreso y por escrito-, origen racial, salud y vida, sexual, -para cuyo tratamiento se requiere consentimiento expreso-, y los relativos a la comisión de infracciones penales o administrativa.

- Seguridad de los datos, todas las empresas, organizaciones, asociaciones e Instituciones, públicas y privadas, que almacenen, traten y accedan a ficheros de datos de carácter personal, deben aplicar medidas de seguridad técnicas y organizativas que garanticen la confidencialidad, integridad y disponibilidad de la información.

- Deber de secreto, este principio recoge las obligaciones de secreto, confidencialidad y custodia que incumben a aquellas personas que traten los datos; y, de manera particular, a aquellos que en el desarrollo de sus funciones accedan a ficheros que contienen datos personales.

- Comunicación de datos, es "toda revelación de datos realizada a una persona distinta del afectado o interesado". Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero, para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

- Acceso a los datos por cuenta de terceros, supone la prestación de un servicio al responsable del fichero por parte de una tercera empresa denominada Encargado del Tratamiento, que accede a los datos del fichero para el cumplimiento de la prestación contratada; actuando en nombre, por cuenta y de acuerdo a las instrucciones establecidas y dadas por el Responsable del Fichero.

Por último, debemos tener en cuenta que la mayor parte de las redes sociales son propiedad de empresas ubicadas en los Estados Unidos de América, con todo lo que ello implica en cuanto a la normativa y a las medidas de protección en materia de privacidad. Por eso debemos analizar en qué medida es posible exigir a las plataformas el cumplimiento de la normativa comunitaria.

En este sentido, la normativa dispone que sea de aplicación en los siguientes casos:

- Cuando el tratamiento de datos se realice en España a través de un establecimiento del responsable del tratamiento.

- En el caso de que el responsable del tratamiento no se encuentre en territorio español, pero le sea de aplicación directa la normativa española mediante acuerdos internacionales.

- Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos, medios o elementos situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

En España, la normativa relativa a este aspecto admite la posibilidad de que las autoridades específicas de protección de datos nacional apliquen dicha normativa a los responsables de estos servicios, independientemente de donde se encuentre el lugar desde el que operan.

Por último, hemos de indicar que la normativa reguladora de este derecho se ha completado –necesariamente, ya que la LOPD remite en numerosas ocasiones a un desarrollo reglamentario de la misma- con la entrada en vigor del Real Decreto 1720/2007, de 21 de diciembre, por el se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Este reglamento no solo regula aquellas materias que la propia LOPD había dejado en manos del Gobierno para su desarrollo por vía reglamentaria (como es el caso de las medidas de seguridad), sino que también regula otros aspectos que, sin estar reservados por la ley para su desarrollo reglamentario, la práctica ha demostrado que necesitaban de una regulación normativa más detallada que la ofrecida por la LOPD.

En lo concerniente a redes sociales, el artículo que mayor impacto ha generado ha sido el número 13. Aquí se establecen las garantías específicas del tratamiento de datos de menores de edad que pueden expresar su consentimiento a partir de los 14 años por sí mismos. Pero existe la posibilidad de ampliar la edad de acceso a los 12 años con el permiso de los padres o tutores. Además se prohíbe recabar datos a menores sobre su grupo familiar.

7.3 El dato de carácter personal

La Constitución española sentó en el artículo 18.4 CE las bases de un nuevo derecho fundamental. Dicho derecho fue definido en su día como "Habeas Data", aunque resulta mucho más precisa y adecuada la denominación de derecho a la protección de datos. Se trata de un derecho de configuración jurisprudencial a través de un conjunto de sentencias que arrancan con la Sentencia del Tribunal Constitucional (en adelante, STC) 254/1993 y culminan con la STC 292/2000, cuyo fundamento jurídico quinto define un nuevo derecho fundamental dotándolo de plena autonomía respecto del derecho a la intimidad:

"La garantía de la vida privada de la persona y de su reputación poseen hoy una dimensión positiva que excede el ámbito propio del derecho fundamental a la intimidad (art. 18.1 CE), y que se traduce en un derecho de control sobre los datos relativos a la propia persona. La llamada "libertad informática" es así derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data) y comprende, entre otros aspectos, la oposición del ciudadano a que determinados datos personales sean utilizados para fines distintos de aquel legítimo que justificó su obtención (SSTC 11/1998, FJ 5, 94/1998, FJ 4). (AGPD, INTECO, 2009, p. 92)

Según el Tribunal Constitucional el objeto del derecho a la protección de datos alcanza: "a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el art. 18.1 CE otorga, sino los datos de carácter personal. Por consiguiente, también alcanza a aquellos datos personales públicos, que por el hecho de serlo, de ser accesibles al

conocimiento de cualquiera, no escapan al poder de disposición del afectado porque así lo garantiza su derecho a la protección de datos. También por ello, el que los datos sean de carácter personal no significa que sólo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo".

A efectos normativos, se entiende que un dato de carácter personal es "cualquier información concerniente a personas físicas identificadas o identificables"(Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, art. 3), lo que convierte en dato de carácter personal la mayor parte de la información sobre personas físicas, en la medida en que a través de escasos datos o informaciones sobre éstas y mediante la correcta aplicación de herramientas informáticas, es relativamente sencillo identificar a la persona concreta que se encuentra detrás de los datos de que se dispone.

Entre los datos personales que en el contexto de las redes sociales pueden llegar a identificar a las personas, se encuentra, entre otros, la dirección IP, tal y como ha sido definida por la Agencia Española de Protección de Datos y por el Grupo de Trabajo del Artículo 29 (en adelante, G29) en su "Dictamen sobre el concepto de datos personales".

El Grupo de Trabajo del Artículo 29 creado como organismo de carácter consultivo e independiente de protección de las personas en lo que respecta al tratamiento de datos, de conformidad con lo dispuesto en el artículo 29 de la Directiva 95/46/CE de protección de datos, ha explicitado los elementos principales de la definición de dato personal de la Directiva 95/46/CE, de la siguiente manera (Barriuso Ruiz, 2009, p. 320):

1.- “cualquier información”: de cualquier naturaleza o formato. Se diserta sobre los datos biométricos y las distinciones legales sobre las muestras humanas de las que pueden ser extraídos.

2º.-“relativo a”: determinándose con los elementos alternativos (contenido, finalidad y resultado) comprendida también la información que puede tener un claro impacto en la forma en que una persona es evaluada o tratada.

3º.- “identificada o identificable”: se centra especialmente en el empleo de medios razonables para identificarla.

4º.- “persona física”: se trata de personas vivas. Tratando los casos de los fallecidos, los nonatos y las personas jurídicas.

Dada la gran cantidad de datos personales que los usuarios publican en sus perfiles, éstos se convierten en auténticas "identidades digitales" que facilitan un rápido conocimiento de datos de contacto, preferencias y hábitos del usuario. Además debe considerarse que durante la prestación de estos servicios se recopilan datos como la dirección IP, que se utilizan para segmentar la publicidad que se dirige a los distintos tipos de usuarios, así como aumentar el grado de contacto entre los usuarios registrados.

Para finalizar este apartado hemos de hacer referencia a un tipo de datos de carácter personal a los que la normativa otorga una protección especial: se trata de los denominados “datos sensibles” o, de acuerdo con la terminología de la propia Ley, “datos especialmente protegidos” (art. 7 LOPD). Entre ellos se incluyen:

- Los llamados por algunos autores “datos ultrasensibles”, categoría bajo la que se incluyen los datos los que revelen la ideología, afiliación sindical, religión y creencias; así como los que hagan referencia al origen racial, a la salud y a la vida sexual. Su creación con la finalidad exclusiva de almacenar este tipo de datos (salvo los referidos a la salud) está prohibida, y su tratamiento, sometido a condiciones más estrictas que el resto de datos. Además, requieren unas medidas de seguridad especiales (medidas de nivel alto).

- El resto de datos sensibles está formado por los datos de carácter personal relativos a la comisión de infracciones penales o administrativas, que sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras (art. 7.4 LOPD) y a los que también se deben aplicar unas determinadas medidas de seguridad (medidas de nivel medio).

La principal conclusión es que hay un derecho emergente (privacidad) frente a otro en decadencia (intimidad) que protegen ámbitos parecidos pero diferentes. El derecho a la intimidad protege la parte más íntima de una persona, esa esfera personal que define qué es y qué no es privado. Por su parte, el derecho a la privacidad se refiere a aquella parte del individuo que va más allá de lo íntimo, esto es, información que tomada por si misma puede no ser relevante, pero que analizada en un momento o contexto concretos puede llevarnos a la construcción de un perfil muy fiable del individuo.

En relación a la protección de datos de carácter personal, se trata de un derecho ampliamente desarrollado legislativamente tanto en el ámbito europeo como en el nacional. A pesar de lo anterior, con el desarrollo de las redes sociales estás leyes han quedado en parte obsoletas porque han surgido nuevos problemas que no se tratan en las leyes promulgadas hasta el momento y que debido a la importancia que conllevan si deberían recogerse.

Capítulo 8
El largo camino para la protección de la privacidad en Facebook

Desde que se crease allá por el 2004, Facebook ha experimentado una gran transformación, tanto a nivel de diseño, de usuarios, y en relación a la privacidad. Con un afán donde se persigue hacer de lo social lo justo, en estos años se contabilizan hasta seis etapas distintas en las Facebook ha ido modificando progresivamente los términos de su servicio y haciendo públicos datos que en un principio eran privados (Morachimo Rodríguez, 2011, p.9).

Tanto ha cambiado la política de privacidad que, entre tantas opciones y términos legales que en ella se encuentra, resulta que tiene una longitud superior a la Constitución de los Estados Unidos de América. Como se puede comprobar en el siguiente cuadro, desde que se realizó la primera política de privacidad se ha multiplicado casi por seis la longitud de dichas políticas.

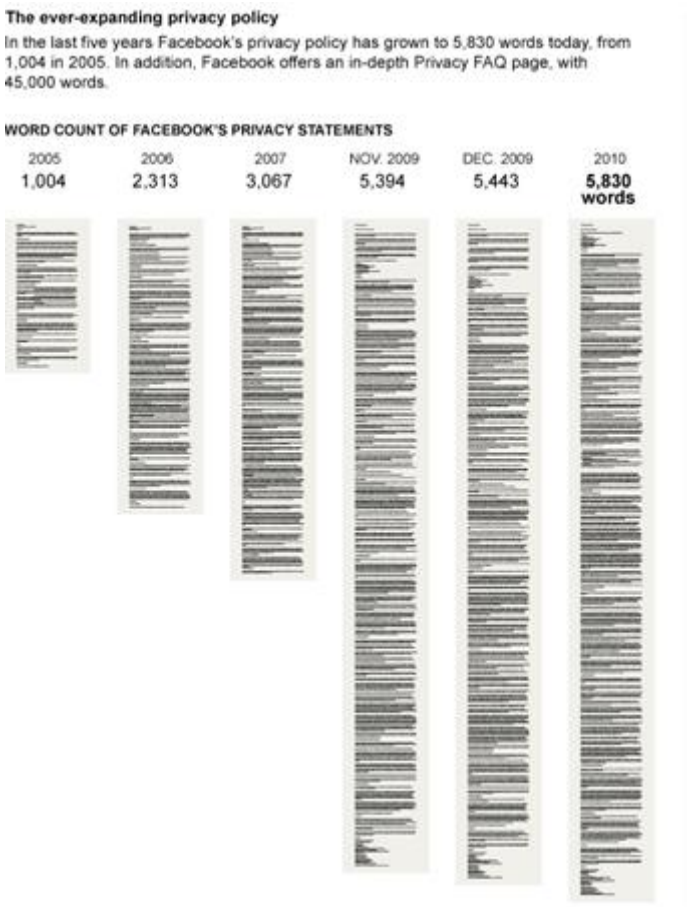


Fig. 11 Expansión política de privacidad según Bilton (2010, p.13)

Kurth Opshal (2010, p.1), a través de un artículo publicado en la Electronic Frontier Foundation(en adelante, EFF), explica que desde 2005 Facebook ha evolucionado de un espacio privado de comunicación entre gente seleccionada a una plataforma donde parte de la información personal es obligatoriamente pública, y puede ser comercializada para mostrar anuncios personalizados.

Basándonos en las opiniones realizadas por Kurth Opshal y apoyándonos en los magníficos gráficos que realizó Matt McKeon vamos a mostrar cómo ha ido cambiando la política de privacidad de Facebook a lo largo de sus distintas etapas. Para finalizar haremos una comparación entre cómo era la privacidad en el año 2005 y cómo es en el año 2010, con la última modificación.

La primera de ellas se corresponde con el año 2005. Se podía resumir de la siguiente forma:

"Ninguna información personal que envíe a TheFacebook estará disponible para usuarios del website que no pertenezcan al menos a uno de los grupos especificados por usted en sus opciones de privacidad."

Como podemos comprobar a la información más personal sólo podían acceder tus amigos o a lo sumo, las personas que pertenecieran a tu red. Desde un principio el nombre ha sido visible para todos los usuarios de Facebook para que se cumpla el objetivo principal por el que se creó la red, conectarte con los amigos. Todos los usuarios de Facebook podían ver las fotografías, saber a la red a la que perteneces, pero nadie que no fuera usuario de Facebook tenía acceso a ningún dato de esta red.

En el año 2006 apenas cambió pero algunos aspectos ya se fueron expandiendo**.** Por defecto, los nombres de perfil y las imágenes podían ser buscadas por todos los usuarios de Facebook, sin tener en cuenta su afiliación institucional, y que los perfiles completos son visibles para todos los usuarios de la misma institución. Aunque los usuarios tenían la posibilidad de ejercer un mayor control sobre sus perfiles, muy pocos lo hacían. Sólo el 1,2% de los usuarios hicieron uso de la opción que permitía controlar los límites de la búsqueda, mientras que menos aún (0,06%) optó por limitar su visibilidad dentro de la institución (Grude et al., 2006, p.5).

“Entendemos que usted no quiere que todo el mundo acceda a la información que cuelga en Facebook; por eso le damos control sobre su información. Nuestras opciones de privacidad por defecto limitan la información mostrada en su perfil a su escuela, su área de residencia y otras razonables limitaciones comunitarias de las que le informaremos.”

En este año Facebook introdujo una aplicación que causó más detractores que admiradores. Esta novedad, News Feed, mostraba en tu muro las actualizaciones que realizaban tus amigos. Por ejemplo, cuando subes una fotografía, cambias tu estado sentimental, actualizas tu perfil, aceptas las peticiones de amistad o cualquier otra acción que realizases se difundían a nuestros contactos a través de éste servicio de noticias. Aunque ninguna de la información que fue compartida en el News Feed había sido previamente ocultada, la agregación automática y la publicidad que se daba a la misma provocó indignación. Muchos usuarios creían que había una diferencia significativa entre el saber que alguien cambió su estado civil visitando regularmente el perfil de la persona a ver que aparece como una acción en el News Feed (Boyd, 2008, p 5).

Hasta la aparición de News Feed el pasatiempo favorito de los usuarios de Facebook era mirar cómo había cambiado el perfil de sus amigos, conocer las novedades, en fin, conocer aquellas cosas que todavía no sabían que habían sucedido. La idea que tenían en mente los diseñadores de Facebook era la de crear una herramienta para diseccionar la información que producen los usuarios de Facebook, seleccionar las acciones y cambios de perfil que serían más interesantes para sus amigos, y luego presentarlas a sus amigos en un orden cronológico inverso. De ahí que cada página de inicio de cada persona sería totalmente distinta dependiendo de quiénes fueran sus amigos (D. Kirkpatrick, 2011, p.216).

Pero esta novedad no tuvo el efecto que los diseñadores de Facebook pensaban y se crearon muchos grupos en contra de esta aplicación, de modo que los usuarios mostraron su desacuerdo. Realmente, lo que los usuarios reclamaban era que pudieran elegir ellos que información se mostraría y cual no en News Feed.

A partir del año 2007, la información que es pública en Facebook va aumentando de un modo considerable.

“La información de perfil que envíe a Facebook estará disponible para los usuarios que pertenezcan al menos a una de las redes que tienen permiso para ver sus datos a través de sus opciones de privacidad (ej: colegio, geografía, amigos de amigos). Su nombre, colegio y foto en miniatura serán visibles en las búsquedas en Facebook, a no ser que modifique sus opciones de privacidad.”. Las opciones de privacidad en Facebook siempre están predeterminadas para mostrar el máximo de información permitido.

En este año las quejas sobre la política de privacidad de Facebook llenaron bastantes líneas en los medios de comunicación. Esto se debió a la aparición de una herramienta complementaria a Facebook Ads (anuncios). Beacon, así se llamaba, tenía la peculiar característica de que cada vez que comprabas algo a través de Facebook lo anunciaba a tus amigos. Beacon fue un servicio de alertas mal diseñado. Ni siquiera tenía un interés publicitario, puesto que no generaba beneficios.

Fue un fracaso porque no se probó lo suficiente, fue un producto de última hora que salió mal. Cuando comprabas algo no te pedía que aprobaras explícitamente que se mandara la noticia a tus amigos. En vez de esto, aparecía un pequeño menú desplegable en el que se te pedía si querías que esa información fuera mandada o no. Si no frenabas la alerta de una manera activa, la alerta se mandaba. Según se dice en la jerga informática, eso se llama opt-out (optar por salir) en vez de opt-in (optar por entrar). Y en menú de salida sólo aparecía unos segundos antes de desaparecer de nuevo, por lo que a muchos usuarios esto se les escapaba (D. Kirkpatrick, 2011, p.294).

Beacon dio la sensación de ser un elemento invasivo y que hacía un mal uso de la información personal. El problema es que a mucha gente le pareció que Facebook quería ganar dinero pirateando los datos personales de sus usuarios.

La información que se comparte va aumentando gradualmente. Ahora también se comparte con toda la red otros datos del perfil, como son las creencias religiosas, las tendencias políticas y la fecha de tu cumpleaños.

Pero lo que podíamos llamar la gran revolución en el aspecto de la privacidad llegó en noviembre del 2009.

“Facebook está diseñado para hacer fácil compartir información con quien elija. Usted decide cuánta información se siente cómodo compartiendo en Facebook, y controla cómo se distribuye mediante sus opciones de seguridad. Debería revisar los parámetros predeterminados y cambiarlos si es necesario para ajustarlos a sus preferencias. También debería hacerlo cuando comparta información.

La información dirigida a ‘todo el mundo’ es pública, puede ser vista por cualquiera en Internet (sin necesidad de entrar en Facebook), puede ser indexada por buscadores

externos, puede ser asociada con usted fuera de Facebook y puede ser importada y exportada por nosotros sin limitaciones de privacidad. Por defecto, las opciones de privacidad para ciertos tipos de información que publica en Facebook están fijadas como “públicas”.

Los nuevos cambios realizados facilitarían que los más de 350 millones de usuarios que tenía Facebook en esos momentos controlasen quién ve sus actualizaciones**,** vídeos, fotografías y otra información personal, pero también les daría la oportunidad de mostrar su información a una audiencia más amplia, en concreto, a todo Internet.

Estos cambios se produjeron debido a una serie de denuncias , siendo la más importante de todas ellas la que dirigió la Canadian Internet Policy and Public Interest Clinic (en adelante, CIPPIC) de la Universidad de Ottawa (Hull et al, 2010, p. 8) , donde identificaban 22 prácticas de seguridad que violaban las leyes canadienses de protección de datos asegurando que Facebook no hacía lo suficiente para proteger la información personal que obtiene de sus miembros y da a los usuarios información incompleta y confusa sobre temas de privacidad**.**

La base de la queja presentada argumentaba que Facebook recolectaba información sensible sobre sus usuarios y la compartía con otros sin su permiso. También afirmaba que la compañía no alerta a los usuarios sobre cómo son utilizados esos datos o que no se elimina la información personal cuando se cierra una cuenta.

Phillipa Lawson, presidenta de CIPPIC, afirmó que "las redes de interacción social online están probando ser una poderosa herramienta para construir comunidades y promover el cambio social, pero al mismo tiempo son un campo minado en cuanto a invasión de la privacidad. Nos hemos concentrado en Facebook porque es el sitio más popular de interacción online en Canadá y porque apunta a jóvenes adolescentes que pueden no ser completamente conscientes de los riesgos que involucra el exponer sus datos personales en internet", explicó. (2009, p.2)

Esta queja fue presentada después de que estudiantes de la CIPPIC analizaran las políticas y prácticas de Facebook como parte de un curso e identificaran prácticas específicas que parecían violar la Ley de Protección de la Información Personal y los Documentos Electrónicos de Canadá (en adelante, PIPEDA).

Pero esta no fue la única modificación del año 2009. Quizás Facebook pensó que se había quedado corto con los cambios, asique en diciembre de ese mismo año hizo pública la nueva política de privacidad.

“Algunas categorías de información, como su nombre, foto de perfil, listas de amigos, páginas de las que es fan, género, región geográfica y redes a las que pertenece, se consideran disponibles públicamente para cualquiera, incluidas las aplicaciones desarrolladas en Facebook, y por tanto no tienen opciones de privacidad. Sin embargo, puede limitar la posibilidad de encontrar esa información mediante búsquedas modificando sus opciones de búsqueda privada”.

Las nuevas características de privacidad harán más fácil que un usuario de Facebook limite ciertos mensajes a una parte de sus amigos, como familiares, pero no colegas de trabajo. Así, cada vez que un internauta actualizaba su estado, podría indicar quién podría leer dicha actualización.

Además, los grupos con los que se podía compartir la información quedaban reducidos a tres, para simplificar las opciones: 'amigos', 'amigos de amigos' o 'todo el mundo'.

Pero pronto comenzaron a surgir las discrepancias. Varias asociaciones norteamericanas presentaron ante las autoridades de su país una denuncia contra Facebook para que le obligasen a corregir su nueva política de privacidad y dar más garantías de confidencialidad a sus miembros.

El Centre for Digital Democracy y el Electronic Privacy Information Center (El País, 18/12/2009) entre otros, sostenían que las nuevas reglas de privacidad perjudican a los miembros de esta red social. El problema principal era que, por defecto, los contenidos y datos del internauta son visibles para todo el mundo y es el propio interesado quien debe restringir este acceso. Estas organizaciones consideraban que esta fórmula favorece la visibilidad de los contenidos de la red a terceros y en los buscadores.

Entre las distintas peticiones que realizaron a la Comisión Federal de Comercio (en adelante, FTC) una de ellas era que "determinase el daño exacto que había causado la nueva política contra la privacidad y seguridad del usuario, y pedir a Facebook que restableciese las anteriores opciones de privacidad, obligando a la red social a que facilite el acceso a las opciones de privacidad y, por último, medidas compensatorias para resarcir al usuario".

Debido a todas las protestas surgidas, las críticas recibidas por parte de sus usuarios, incluyendo amenazas de cierre masivo de cuentas y la intervención de gobiernos y organismos encargados de la protección de datos personales, Facebook decidió modificar en abril del 2010 su política de privacidad.

“Cuando se conecte a una aplicación o website, ésta podrá acceder a su Información General. Este término incluye su nombre y el de sus amigos, fotos de perfil, género, IDs de usuario, conexiones (con páginas y aplicaciones externas) y el contenido compartido. Por defecto, las opciones de privacidad de cierta clase de información publicada en Facebook está señalada como “pública”: Dado que se necesitan dos para conectarse, sus opciones de privacidad sólo controlan quien puede ver su conexión en su página de perfil. Si no se siente cómodo porque su conexión esté disponible públicamente, debería considerar retirar (o no hacer) la conexión”.

Las nuevas modificaciones afectaban principalmente a tres aspectos:

La primera de ellas era que se simplificaban los procesos para asignar niveles de seguridad a la información, permitiendo a los usuarios de una forma más simple y sólo con un par de clicks el determinar si la información de su perfil es totalmente pública, sólo visible para sus amigos o también para los amigos de sus amigos y esto funcionará de forma automática; es decir que conservará las opciones de compartir

información asignadas por el usuario en las futuras actualizaciones de la aplicación, salvo que este los modifique, función que también estará disponible.

El segundo gran cambio planteado hacía referencia a la información contenida en el perfil del usuario y que por defecto actualmente queda abierta al público, condición que será modificada para reducir la cantidad de datos del usuario visibles en la red, salvo que la persona lo configure expresamente.

Por último, la tercera modificación presentada estaba relacionada con la polémica estrategia de Facebook planteada principalmente por la variación en la función del botón "me gusta" que compartía la información del usuario con otras webs o aplicaciones, sin que fuese necesario ni siquiera estar conectado a la red social. A partir de la introducción de este cambio, los usuarios tendrán la posibilidad de bloquear la entrega de información a terceras partes, incluyendo la opción de no activar las personalizaciones instantáneas para evitar, con todo esto, la transmisión de datos y preferencias del usuario a compañías de publicidad.

La finalidad de estos cambios propuestos por Facebook, según indicó Mark Zuckerberg, es la de completar el modelo de privacidad de datos de la red social y que prevé que con esto, el modelo será seguro durante varios años. Sus palabras textuales fueron**: "**"Cada vez que anunciamos un cambio tratamos de aprender de los errores pasados. Estamos lejos de la perfección, pero intentamos mejorar con todas nuestras fuerzas" (Europa Press, 3/6/2010).

Entre las diferencias más apreciables que podemos encontrar entre las distintas políticas de privacidad que ha desarrollado Facebook destacarían las siguientes:

- La principal diferencia que encontramos es que a día de hoy se comparte más información que en el origen de Facebook. En sus inicios ninguna persona que no estuviera dentro de la red no podía tener acceso a ningún dato. Era uno de los requisitos básicos, para poder ver el perfil de otro usuario era necesario formar parte de la Red. Hoy un usuario que navegue por Internet puede ver perfectamente tu nombre, las fotografías, los amigos, tus preferencias y gustos, etc. En el año 2005 tus contenidos estaban limitados para ser vistos solo por tus amigos. Hoy puede acceder cualquier usuario de Facebook.

- Otra diferencia muy importante es, que a pesar de tener una configuración de privacidad nada rigurosa, a lo sumo tu perfil podía ser consultado por unas 5 millones de personas. En 2011 simplemente si tienes la configuración por defecto de Facebook, parte de tu perfil puede ser consultado, no solo por los 650 millones de usuarios de Facebook, sino por la red entera.

- Además ha surgido un nuevo elemento, los amigos de amigos, que tienen casi los mismos privilegios que un amigo, a no ser que tú indiques lo contrario. Este nuevo elemento ha surgido en lugar de "network" es decir, a la red a la que pertenecías.

- Facebook consiguió su base principal de usuarios ofreciéndoles unos controles sencillos y de gran alcance sobre su información personal. Los cambios realizados año tras año se han traducido en una erosión gradual pero constante de la privacidad de los usuarios de Facebook, y de la capacidad de los usuarios para controlar su información privada. Los dos elementos claves que han cambiado son: 1) La tendencia a definir la información de Facebook como "pública" frente a "privada" , y 2) a quien se permite el acceso a la información pública o privada

- Ahora se tiene un control más granular sobre los datos que se hacen públicos en nuestro perfil de Facebook, en nuestras fotografías o en las fotografías donde hemos sido etiquetados y hasta en lo que publicas en el muro. Anteriormente, por defecto, Facebook ofrecía la posibilidad de que al menos los amigos de tus amigos tuvieran acceso a muchos datos tuyos que no tendrían por qué tener.

- Hoy en día, Facebook se ha convertido en una plataforma en la que un usuario no tiene otra opción que ver cómo parte de su información personal es pública y se encuentra disponible para "Todos" y que esta información puede ser compartida por Facebook con sus socios siendo utilizados estos datos con unos objetivos específicos como puede ser ofrecer una publicidad más personalizada según nuestros gustos.

- La transformación de Facebook en relación a su política de privacidad es indicativa de las maniobras de rentabilidad de la empresa en asociación con sus socios publicitarios aprovechando el valor de los datos personales y toda la información disponible de sus usuarios. A medida que Facebook creció y se hizo más importante, poco a poco fue convirtiéndose en una red más transparente con unos objetivos más comerciales a cambio de sacrificar parte de la política de privacidad y protección de datos con la que nació.

Para comprobar de una manera más visible los cambios producidos en estos años vemos cómo se han ido modificando las distintas partes a través de dos imágenes referentes a las características de la privacidad en el año 2005 y a la política de privacidad actual.

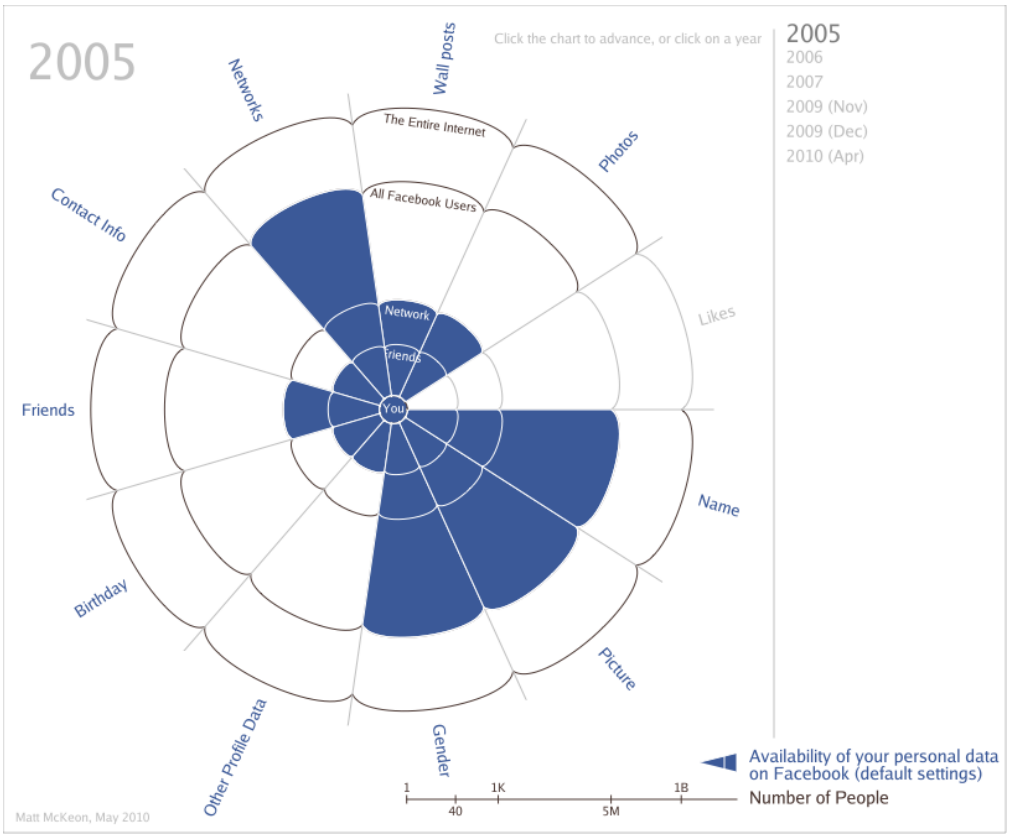


Fig. 12 Privacidad en Facebook año 2005

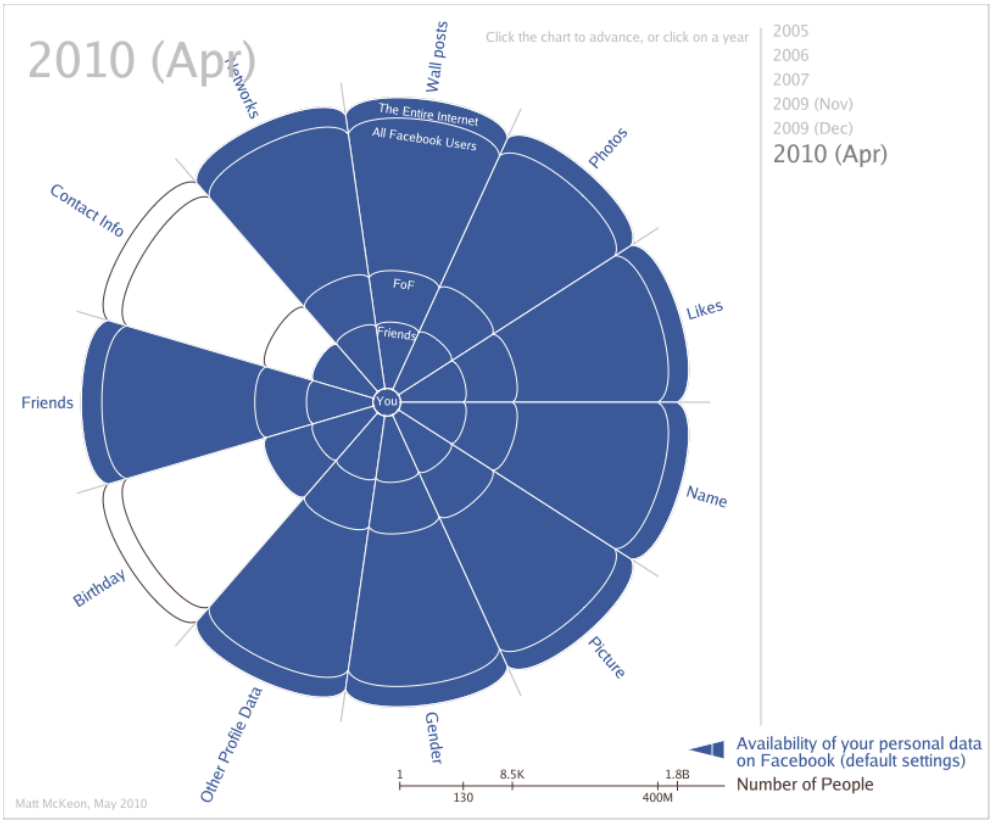


Fig. 13 Privacidad en Facebook año 2010

A día de hoy, Facebook acumula una gran cantidad de datos sobre sus 650 millones de usuarios. Esta información es tan diversa que va desde los intereses que uno tiene, pasando por su lista de amigos hasta saber cuál es tu tendencia política o creencia religiosa.

Si toda esta información fuese solo texto plano su valor se reduciría muchísimo. Lo que ocurre es que Facebook convirtió toda esta información en hipervínculos que, al seguirlos, activaban una búsqueda donde se nos mostraba a los usuarios que tenían los mismos intereses que nosotros. Pero esto conlleva también un valor importante para el usuario, ya que podrá entrar en contacto con otros usuarios que tengan los mismos intereses. Pero también es beneficioso para la publicidad de Facebook, ya que es más fácil destinar un producto específico si sabes las personas a las que les puede llegar a gustar. Recientemente, Facebook convirtió esa información en nodos de red con entidad propia (denominadas “Conexiones”), similares a las Páginas y a los Grupos. A la vez, modificó su política de privacidad para arrogarse el control de esa información y hacerla pública por defecto. Es decir, los datos que no tenían ningún valor ahora tienen un valor inmenso ya que acompañan tu identidad y se reflejan en el resto de páginas que visitas (Morachimo, 2011, p.7).

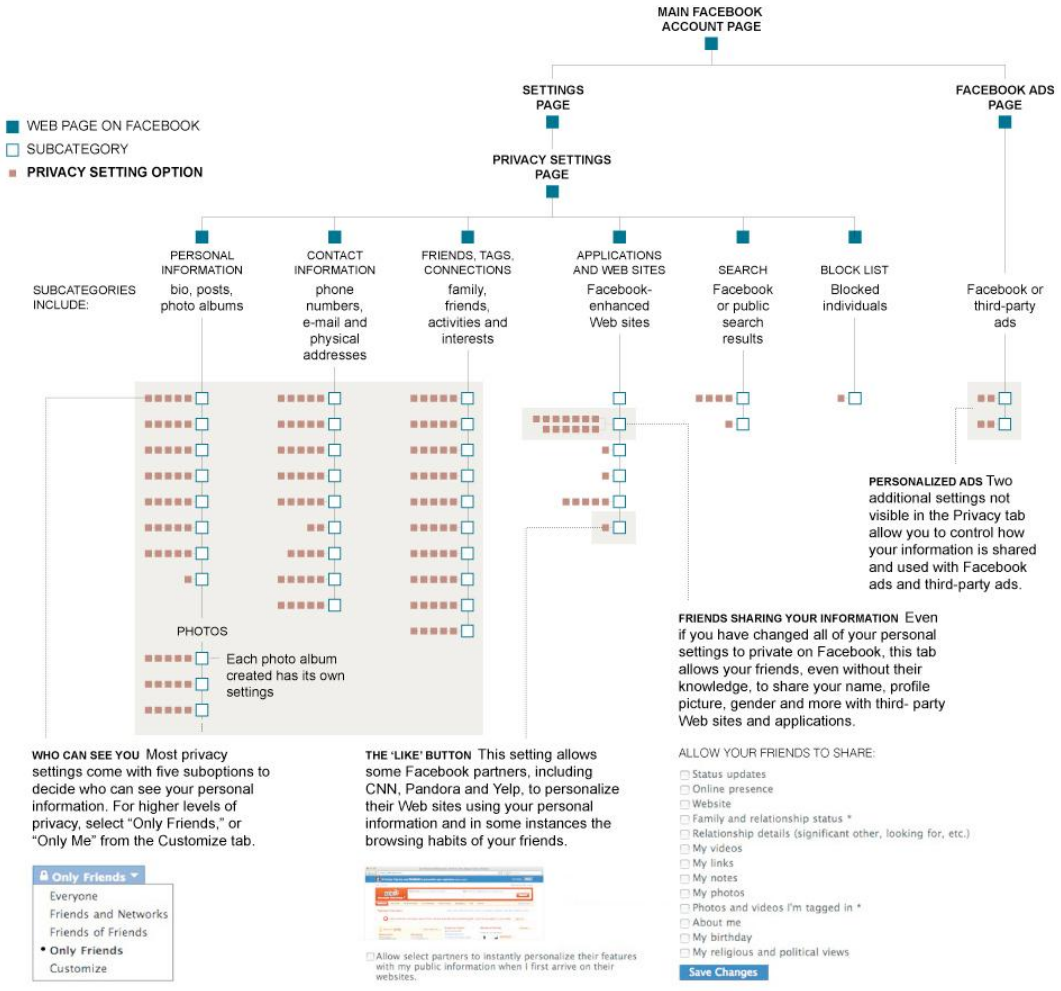


Fig. 14 Información que se recoge en Facebook según Bilson (2010)

De todas formas, a modo de consejo, quien no quiera correr el riesgo de que su información privada sea expuesta públicamente, que tenga precaución con lo que publique en Facebook. Cuando te registras en esta red social no renuncias al control sobre tus datos sino que te sometes a un contrato y aceptas todo lo que te va apareciendo en la pantalla sin prestar atención y leer esa información. El problema es que este contrato de adhesión viene siendo modificado unilateralmente por Facebook al punto de decir exactamente lo contrario de lo que decía cuando se creó.

En resumen, una vez analizada todas las políticas de privacidad que ha tenido Facebook a lo largo de los años hemos comprobado que la que ofrecía más seguridad a sus usuarios era la primera, ya que no tenía establecida una privacidad por defecto para “Todos”, sino que los perfiles de los miembros de la red solo podían ser consultados por miembros de la red. En los distintos cambios que ha ido sufriendo se ha convertido en una red cada vez más transparente, donde se muestran más datos personales de los usuarios que en ninguna de las políticas anteriores.

Capítulo 9
La política de privacidad de Facebook

A lo largo de su corta historia, Facebook ha variado considerablemente su política de privacidad. La última modificación se produjo en abril del 2010, motivada por las presiones recibidas por parte de los usuarios debido a las críticas generadas por la compleja configuración de las opciones de privacidad impuestas por Facebook, dado que hay muchos usuarios que no desean mostrar datos personales a todos los usuarios que componen la red.

El número de usuarios molestos por la exposición de sus datos personales incluso para personas o empresas que no están registradas en esta red social no han hecho más que aumentar y ha abierto el debate en el seno de una empresa donde no hay consenso en esta cuestión.

Entre los nuevos cambios producidos destaca por encima del resto la creación de una configuración más simple, más sencilla sin tanto lenguaje burocrático que hacía perderse a los pocos usuarios que leían la política de privacidad. Facebook siempre ha ofrecido una gran cantidad de controles, pero los usuarios veían una cierta dificultad a la hora de utilizarlos, por lo que se ha decidido simplificarlos para que los usuarios no tengan tantos problemas. Esta simplificación se ha llevado a cabo en tres aspectos: un único control para el contenido que publicamos en nuestro perfil, controles más efectivos para la información básica que compartimos y una forma más sencilla para desactivar todas las aplicaciones.

Con la creación de esta configuración más simple, el usuario va a decidir quién puede ver la información que publica. De esta forma el contenido puede quedar limitado a tres ámbitos: quedará abierto a todos, a los amigos de tus amigos o de una forma más restrictiva solo para tus amigos. La configuración que se elija aquí, será tomada como predeterminada en las futuras acciones que realices. Es una manera simple y efectiva de no tener que estar preocupado siempre por la configuración de la privacidad.

El aspecto que más molestaba a los usuarios se ha solucionado, en parte. Se ha reducido la cantidad básica de información que debía ser visible para todos los usuarios, eliminando además el modelo de privacidad de las conexiones. Ahora será el usuario quien decida quién puede ver tus amigos y tus páginas. Estos campos ya no serán públicos.

Quizás este sea uno de los mayores problemas que tiene Facebook en su lucha por defender la privacidad, el control de las aplicaciones y los sitios web. Se ha creado una opción que permita de una forma más sencilla y efectiva desactivar esa aplicación. Con esto se pretende que nada de nuestra información personal sea compartida con las aplicaciones o sitios web.

A continuación desgranaremos punto por punto en qué consiste la política de privacidad de Facebook.

La política de privacidad de Facebook se divide en nueve puntos diferentes.

1. Introducción
2. Información que recibimos
3. Compartir información en Facebook.
4. Información que compartes con terceros
5. Cómo utilizamos tu información
6. Cómo compartimos la información
7. Cómo puedes modificar o eliminar información
8. Cómo protegemos la información
9. Otras condiciones

En la primera parte, ya en las primeras líneas deja claramente definida cuál es su postura: “La presente política de privacidad incluye Facebook al completo. No obstante, no es aplicable a entidades que no sean propiedad o no se encuentren bajo el control de Facebook, incluidos los sitios web y aplicaciones que utilicen la plataforma. Si utilizas o accedes a Facebook, estarás aceptando las prácticas de privacidad aquí definidas”. (Facebook, 2010)

Es en este punto donde la mayor parte de los usuarios han mostrado su malestar criticando duramente el hecho de que plataformas y aplicaciones que interactúan con Facebook no tenga que asumir las políticas de privacidad que han de seguir todos los usuarios. Por este motivo, las distintas aplicaciones pueden recopilar toda la información personal que quieran sirviéndose de ellas para rentabilizarlas de una forma económica a través de la publicidad.

El punto 2 está dedicado a la información que recibe Facebook. Este punto se divide a su vez en cinco apartados bien diferenciados:

- Información que envías: el requisito principal para poder registrarte en Facebook es facilitar un nombre de usuario, una cuenta de correo, el sexo y la fecha de nacimiento. A medida que vas cumpliendo pasos en el registro debes ir añadiendo más información para que puedas conectarte con tus amigos, etc. Facebook contempla la posibilidad de necesitar más información que la que añades al principio cuando te registras por motivos de seguridad o para ofrecerte servicios específicos. Una vez registrado puedes proporcionar otra información sobre ti relacionada, por ejemplo, con tu ciudad de residencia, ciudad de origen, familia, relaciones, redes, actividades, intereses y lugares. También puedes indicar tu ideología política o tus creencias religiosas. Entre las distintas opciones que te ofrece la red están las herramientas de importación de contactos para ayudarte a cargar las direcciones de tus amigos para que puedas encontrarlos en Facebook e invitarlos a unirse a la red. La contraseña que añades para poder realizar esta búsqueda no será almacenada por Facebook, aunque la dirección de correo electrónico sí. En relación al contenido que añades, uno de los principios básicos de Facebook es que puedas compartirlo con los demás. Entre las opciones disponibles estarían actualizar tu estado, subir o hacer una foto, cargar o grabar un vídeo, compartir un enlace, crear un evento o un grupo, hacer un comentario, escribir algo en el muro de alguien, escribir una nota o enviar un mensaje. Si cuando subes una foto no deseas que los metadatos asociados a ella se guarden, debes eliminarlos antes de subir la foto a Facebook. Como bien sabemos, Facebook ofrece la posibilidad de comprar “contenido”, es decir, regalos o más cosas para los juegos o aplicaciones. Los datos que metes cuando realizas una compra quedarán guardados, a no ser que no quieras que almacenen el número de cuenta de origen de tu pago, pudiendo eliminarlo a través de la página de pagos.

- Información que recopilan cuando estás en Facebook: realizan un seguimiento de todas las acciones que realizas, desde cuando te unes a un grupo, añades un amigo**,** crear un álbum de fotos, enviar un regalo, dar un toque a otro usuario, indicar que "te gusta" una publicación, asistir a un evento o conectarte a una aplicación; todo lo que haces queda registrado. Además queda registrado desde donde te conectas. Cuando entras a consultar cualquier dato, por ejemplo tu perfil o alguna actualización de estado de un amigo desde un ordenador, teléfono móvil u otro dispositivo, Facebook tiene la potestad de obtener información de dicho dispositivo sobre tu tipo de navegador, ubicación y dirección IP, así como las páginas que visitas.
  Por otra parte nos explican también por qué utilizan las cookies (datos que almacenan en el ordenador, teléfono móvil o cualquier otro dispositivo desde el que te conectas). El objetivo principal de estas cookies es que Facebook sea más fácil de usar, para que la publicidad sea mejor y para proteger tanto a ti como a la propia red. Estas cookies guardan el nombre de usuario (pero nunca tu contraseña) con el fin de que te resulte más sencillo iniciar sesión cada vez que quieras entrar en Facebook. También utilizan las cookies para confirmar que estás conectado a Facebook, y para saber cuándo estás interactuando con aplicaciones y sitios web de la plataforma Facebook, nuestros widgets, botones

de compartir y nuestros anuncios. Las cookies se pueden configurar, pero esta configuración puede influir en la capacidad de uso de Facebook.

- Información que reciben de terceros: Las aplicaciones y sitios web que actúan dentro de Facebook suministran información, incluida la información acerca de las acciones que realizas. Además, se contempla la posibilidad de que Facebook reciba información previa a tu entrada en la aplicación con objeto de ofrecerte un servicio más personalizado.

- Información procedente de otros sitios web: Facebook establecerá programas con socios publicitarios y otros sitios web en los que éstos comparten información con ellos. A modo de ver cómo funcionan sus anuncios, nos utilizarán como cobayas para saber cómo han actuado los usuarios que han visto los anuncios y los que no lo han visto, con el fin de establecer comparativas, o como ellos lo llaman “seguimiento de conversión" que ayuda a medir la efectividad de la publicidad y a mejorar la calidad de los anuncios que nos muestran. Facebook recibirá información sobre si hemos visto o no, o si hemos interactuado con determinados anuncios de otros sitios, para medir la efectividad de dichos anuncios.

- Información procedente de otros usuarios: Facebook puede recopilar información sobre nosotros a partir de otros usuarios como cuando un amigo te etiqueta en una foto, un vídeo o un lugar. Con esos datos ya está dando detalles sobre nosotros referentes a gustos personales, intereses, etc.

El punto 3 trata sobre la información que compartimos en Facebook. En este apartado nos ofrece una nociones básicas sobre cómo debemos configurar la privacidad de nuestra cuenta junto a como se comparte nuestra información en Facebook. Entre las distintas secciones que comparten información encontramos:

- Nombre y foto del perfil: la foto que tienes de principal en tu perfil carece de privacidad, al igual que nuestro nombre. Esta afirmación tan contundente se debe a que estas dos características son básicas para poder conectarte a otros usuarios, pero en mi opinión me parece excesivo el derecho que Facebook se toma en este caso. La única forma que ofrece Facebook para no compartir tu fotografía de perfil es no teniendo ninguna, o en el caso de que tengas una, eliminarla. En este apartado también podemos controlar quien nos puede buscar tanto en Facebook como en los motores de búsqueda, aspectos que debemos configurar en nuestra cuenta.

- Información de contacto: es la información que ofrecemos para que los demás se puedan poner en contacto con nosotros, y también la información que pueden ver sobre nosotros (correo electrónico, número de teléfono). Estos aspectos se pueden regular a excepción del correo electrónico, cuyo dato es obligatorio para registrarte en Facebook pero que mediante la privacidad que elijas compartirás con el resto de los usuarios, con los amigos de tus amigos o solamente con tus amigos.

- Información personal: puedes controlar quién ve tu información personal, como puede ser tus tendencias políticas o creencias religiosas, en el caso que decidas añadir esa información a tu perfil. Facebook recomienda compartir esa información limitándola a la opción “amigos de amigos”.

- Mis publicaciones: a la hora de publicar contenido Facebook te ofrece la posibilidad de que puedas controlar exactamente quién puede verla en el momento de crearla. Cada vez que compartas algo, busca el icono del candado. Si haces clic en el candado se mostrará un menú que te permite elegir quién podrá ver tu publicación. Si por el contrario decides no seleccionar tu configuración en el momento de publicar el contenido, dicho contenido se compartirá en consonancia con la configuración de "Mis publicaciones".

- Sexo y fecha de nacimiento: estos dos datos son obligatorios cuando te registras en Facebook. La razón por la que se pide la fecha de nacimiento es para comprobar que se es mayor de 13 años, edad mínima para poder registrarse en Facebook, a excepción de España, cuya edad mínima es 14 años. Estos datos, a pesar de ser obligatorios puedes ocultarlos para que no los puedan ver otros usuarios.

- Otras indicaciones que debemos recordar:
  - ❖ Cuando actualizamos nuestro perfil, bien añadiendo contenido o cambiando datos, esta información se mostrará en las páginas de inicio de nuestros amigos y en otras páginas que visiten.

  - ❖ Cuando alguien te etiqueta en una fotografía tienes el derecho a eliminar esa etiqueta. Además, a través de la configuración de la privacidad, puedes limitar quién puede ver que has sido etiquetado.

  - ❖ A pesar de haber eliminado información de tu perfil o haber borrado, es posible que haya alguna copia de dicha información y que permanezca visible en algún otro lugar si ha sido compartida con otros, ha sido distribuida de algún otro modo o ha sido copiada o almacenada por otros usuarios.

  - ❖ Tu información puede ser compartida o copiada por otros usuarios.

  - ❖ Los mensajes que recibes o que envías a otros usuarios no pueden ser eliminados.

  - ❖ La información que publicas en el perfil de otro usuario o realizas algún comentario en su publicación se regirá por la configuración de la privacidad del otro usuario.

  - ❖ Cuando nos conectamos a la red a través de una fuente externa para publicar información, debemos comprobar la configuración de privacidad de dicha publicación, puesto que es la fuente externa quien la establece.

- Información de “Todos”: existe información que estará disponible para todos los usuarios de Facebook. Esta información como es nuestro nombre, foto de perfil

y conexiones permanecerá accesible y visible no sólo para los usuarios de Facebook, sino que también lo estará para todas aquellas personas que naveguen por Internet, estén o no registrados en Facebook. Lo peor de todo con respecto a nuestra privacidad es que está información queda sujeta a indexación por parte de motores de búsqueda de terceros y puede ser importada, exportada, distribuida y redistribuida por nosotros y otros sin limitaciones de privacidad. Dicha información puede asociarse contigo, incluido tu nombre y fotografía de perfil, incluso fuera de Facebook, por ejemplo, en motores de búsqueda públicos y cuando visites otros sitios de Internet. Facebook establece como predeterminada la opción "Todos". Esta opción puede ser modificada a través de la configuración de la privacidad de nuestra cuenta. Por último, si eliminas el contenido compartido con "Todos", se borrará de nuestro perfil, pero Facebook se excusa diciendo que ellos no pueden controlar el uso que se hace de esa información fuera de la red.

- Menores: Facebook se reserva el derecho de aplicar métodos de protección especial para menores y controlará la capacidad de interacción que se produce entre los adultos y los menores. Debido a esto, los menores pueden sufrir ciertas restricciones en el uso de la red.

El apartado 4 trata sobre la información que compartes con terceros. Éste es el punto más crítico y que más problemas ha dado a Facebook. Está relacionado con el uso que hacen de nuestra información las aplicaciones y sitios web que interactúan dentro de Facebook.

- Plataforma de Facebook: según afirman no operan con los sitios web y aplicaciones que utilizan Facebook. Debemos tener cuidado cuando utilizamos una aplicación ya que es una minoría quién lee atentamente qué pueden hacer con nuestra información personal. Esto significa que al utilizar estas aplicaciones y sitios web, tu información de Facebook no está sólo disponible para Facebook.

- Conexión a una aplicación o sitio web: cuando nos conectamos a una aplicación o sitio web, éstos podrán acceder a toda la información general que hemos añadido, ya por información general entiende nuestro nombre y los nombres de nuestros amigos, fotografías de perfil, sexo, identificador de usuario, conexiones y cualquier contenido compartido usando la configuración de privacidad "Todos". De todas formas, estos datos no parece que sean suficientes, ya que Facebook ofrece más información como datos técnicos, la localización de tu equipo informático o dispositivo de acceso, así como tu edad, para que puedan ofrecerte "medidas de seguridad" adecuadas para controlar el contenido que se te va a ofrecer para que sea el adecuado acorde a tu edad.

  A pesar de lo anterior, Facebook muestra también su "preocupación" y ofrece herramientas para controlar cómo compartes tu información con aplicaciones y sitios web que utilizan la red. De este modo, a través de la configuración de la privacidad puedes bloquear el acceso a todos tus datos por parte de los sitios web y las aplicaciones, o bloquear aplicaciones específicas.

Por último, Facebook nos aconseja leer siempre las políticas de los sitios web y las aplicaciones de terceros para que demos el visto bueno al modo en el que usan la información que compartes con ellos. Facebook se excusa afirmando que no puede garantizar que estos sitios web o aplicaciones cumplan sus normas.

- Cuando tus amigos utilizan la plataforma: si cualquiera de tus amigos se conecta a una aplicación o sitio web, éstos podrán acceder a tu nombre, fotografía del perfil, sexo, ID de usuario y aquella información que hayas compartido con "todos". También podrán acceder a tus conexiones, pero no podrán acceder a tu lista de amigos. Para poder acceder a ella necesitarán obtener tu permiso. Si, por ejemplo, tu amigo se conecta a una aplicación y ésta quiere acceder a contenido o información tuya tienen que obtener un permiso específico de nuestro amigo. Si nuestro amigo concede permiso a la aplicación sólo podrán acceder a contenido e información sobre ti a la que tu amigo pueda acceder. Además, sólo podrán utilizar dicho contenido y dicha información en conexión con ese amigo. Por ejemplo, si un amigo facilita a una aplicación acceso a una fotografía que sólo compartes con tus amigos, dicha aplicación puede permitir a tu amigo ver o imprimir la fotografía, pero no puede mostrársela a nadie más.

  Para que controlemos aspectos como el anterior contamos con una serie de opciones dentro de la configuración de la privacidad para limitar qué información pueden poner tus amigos a disposición de las aplicaciones y los sitios web, pudiendo bloquear el acceso a tu información de todas las aplicaciones y sitios web de la plataforma, o de aplicaciones o sitios web concretos, o en el caso más extremo eliminar a un amigo si no estás de acuerdo con el modo en que utiliza tu información.

- Sitios web y aplicaciones de terceros aprobados previamente: Facebook, eso sí, en ocasiones, facilita nuestra información a sitios web y aplicaciones de terceros aprobadas previamente que utilizan la plataforma cuando los visitas. Lo mismo ocurre cuando uno de nuestros amigos visite un sitio web o aplicación aprobada previamente, recibirá información general sobre ti para que podáis conectaros también a través de ese sitio web (si también dispones de una cuenta en dicho sitio web). Para permitir este intercambio de información, Facebook los somete a un proceso de aprobación y a la participación en diferentes acuerdos con el objetivo de proteger nuestra privacidad. Por ejemplo, estos acuerdos incluyen disposiciones relativas al acceso y eliminación de tu Información general, así como la posibilidad de rechazar la participación en la experiencia ofrecida.

  A través de la configuración de la cuenta puedes bloquear estas aplicaciones, o en el caso de que hayan recibido autorización previa haciendo clic en “No, gracias”. Además, si cierras la sesión de Facebook antes de visitar un sitio web o aplicación aprobados previamente, éstos no podrán acceder a tu información.

- Exportación de información: Facebook permite el uso de herramientas como fuentes RSS, aplicaciones de libretas de direcciones del teléfono móvil o funciones de copiar y pegar, para obtener y exportar (y en algunos casos, importar) información de Facebook, incluida tu propia información y todos los datos sobre tu persona.

- Publicidad: puedes anular el uso de cookies para que los anunciantes que presentan publicidad no puedan contar con tus datos a la hora de medir la efectividad de sus anuncios y personalizar el contenido publicitario. Facebook no comparte con los anunciantes información que te identifica personalmente salvo si obtenemos tu autorización.

- Enlaces: Facebook no se hace responsable de las políticas de privacidad que tiene los sitios web a los que accedes a través de los enlaces.

Es a partir de los siguientes puntos donde se centra en cómo se gestiona nuestra información. De hecho, el apartado 5 se llama “Como utilizamos tu información”. En palabras de Facebook recopilan información para ofrecernos una experiencia segura, eficaz y personalizada.

- Para gestionar el servicio: utilizan esta información para ofrecernos mejores servicios, hacerlos más funcionales, para poder evaluarlos y así mejorarlos. Además se utiliza para prestarnos un servicio técnico adecuado. Esta información se estudia para impedir actividades que podrían ser ilegales. Entre otro de los usos está el evitar que el correo basura en los usuarios, esto se realiza a través de sistemas tecnológicos que lo detectan. Estos esfuerzos pueden provocar, en ocasiones, el fin o la suspensión temporal o permanente de algunas funciones para algunos usuarios.

- Para ponerse en contacto contigo: en este caso se utilizaría nuestros datos para enviarnos anuncios relativos a servicios. Si quieres puedes evitar que lleguen estos mensajes, para ello debes desactivarlo en la página de notificaciones de tu cuenta.

- Para ofrecerte anuncios personalizados: lo primero de todo es dejar claro que no comparten nuestra información con los anunciantes a no ser que demos nuestro consentimiento. Eso sí, se permite a los anunciantes elegir las características de los usuarios que verán los anuncios y será Facebook quien decida que usuarios en concreto lo verán basándose en una serie de atributos que han analizado de nuestra información. Por ejemplo, podríamos utilizar tu interés por el fútbol para mostrarte anuncios de equipamiento de fútbol, pero no le dice a la empresa que vende el equipamiento quién eres.

  Por otra parte, aunque Facebook no comparte tu información con los anunciantes sin tu permiso, cuando haces clic en un anuncio o interactúas con

éste, se puede dar el hecho de que el propio anunciante coloque una cookie en tu navegador y tomar nota de que cumple los criterios que ha seleccionado.

- Para ofrecerte anuncios sociales: una vez que se analiza tu información, te ofrecerán los anuncios que más se adapten a tus condiciones e intereses y a los de tus amigos, con el fin de que los anuncios resulten más interesantes y se adapten mejor a ti y a tus amigos. Por ejemplo, si te conectas a la página de tu grupo de música favorito, podemos mostrar tu nombre y la foto de tu perfil al lado de un anuncio de dicha página que verán tus amigos. Pero esa información solo se comparte con el amigo que puede ver el anuncio. Si no quieres que tu información sea utilizada con este fin, puedes desactivar esta opción editando tu cuenta.

- Para complementar tu perfil: Facebook puede utilizar información sobre ti recogida de otros usuarios para completar nuestro perfil. De todas formas se nos permite eliminar el contenido o limitar la visibilidad de nuestro perfil.

- Para hacer sugerencias: se utilizará nuestra información, incluidas las direcciones que importas a través de las herramientas de importación de contactos, para hacerte sugerencias a ti y a otros usuarios de Facebook. Es el caso de que si un amigo cuelga una foto donde apareces, Facebook le sugerirá que te etiquete en ella. Para hacer esto, comparan las fotos de nuestro amigo con la información que han recogido de las fotos donde se nos ha etiquetado. Podemos controlar si queremos o no que otros usuarios nos etiqueten en las fotos personalizando nuestra configuración. Otro ejemplo sería cuando un usuario importa la misma dirección de correo que nosotros, Facebook nos sugerirá hacernos amigos. Para controlar si podemos sugerir o no a otro usuario que te añada como amigo, ve a la opción "Buscarte en Facebook" de tu configuración de privacidad.

- Para ayudar a nuestros amigos a que nos encuentren: otros usuarios pueden utilizar información de contacto que tengan sobre ti (como tu dirección de correo electrónico) para encontrarte, incluso a través de herramientas de importación y búsqueda de contactos

- Software descargable: algunas aplicaciones de software descargables y applets que Facebook ofrece, como las barras de herramientas del navegador y las herramientas para cargar fotos transmiten datos. Facebook se reserva el derecho de no realizar ninguna declaración formal si creen que la recopilación y uso de información por su parte es el fin obvio de la aplicación, por ejemplo, el hecho de recibir fotografías cuando se utiliza la herramienta para cargar fotos. Si creen que no resulta obvio que estén recopilando o utilizando dicha información, nos avisarán la primera vez que facilitemos información, de tal manera que podamos decidir si queremos utilizar esa función.

- Cuentas in memoriam: cuando un usuario muere, su cuenta se convierte en una cuenta conmemorativa. Sólo podrán acceder al perfil los amigos ya

confirmados y se permite a éstos y a los familiares que escriban en el muro del usuario en recuerdo suyo. También se puede cerrar la cuenta si se recibe una solicitud formal un pariente del usuario u otra solicitud legal pertinente para hacerlo.

Quizás sea este sexto apartado el más importante de todos, ya que Facebook nos muestra cómo comparte nuestra información, y lo que más nos interesa, con quién la comparte. Uno de los pilares sobre los que se sujeta Facebook es compartir información con otros, bien sean nuestros amigos o personas de nuestro entorno. Facebook nos ofrece una serie de herramientas para que, a través de la configuración de la privacidad, decidamos quién queremos o no que vea nuestra información. En el caso de que compartan información con terceros, se realizará cuando crean que esta acción esté permitida por nosotros, bien porque sea necesaria para ofrecer su servicio o cuando se exige legalmente que esto se haga.

- Cuando realizas un pago: cuando efectúes un pago en Facebook o realices una transacción con un tercero, sólo se compartirá la información de la transacción con los terceros que sean necesarios para completar la transacción, previo acuerdo con los terceros para que respeten la privacidad de la información.

- Cuando invitas a un amigo a que se una a Facebook: se enviará a nuestro amigo un mensaje de nuestra parte, utilizando nuestro nombre, siendo enviados, como máximo, dos recordatorios. Además este mensaje puede contener información sobre otros usuarios que nuestro amigo pueda conocer. Si quieres conocer quiénes han aceptado tus invitaciones, enviar recordatorios o eliminar las direcciones de correo electrónico de nuestros amigos lo podemos hacer a través de la página del historial de invitaciones.

- Cuando eliges compartir información con comerciantes: Facebook no suministrará información sin nuestra previa aceptación.

- Para ayudar a nuestros amigos a encontrarnos: Facebook, de forma predeterminada, nos obliga a incluir información personal que facilita a nuestros amigos la búsqueda. Sin embargo, podemos controlar quién puede ver esta información, así como quién nos puede encontrar en búsquedas. A su vez Facebook colabora con proveedores de mensajería instantánea y correo electrónico para ayudar a sus usuarios a identificar cuáles de sus contactos son usuarios de Facebook, de forma que podamos promocionar Facebook a dichos usuarios.

- Para dar a los motores de búsqueda acceso a la información disponible públicamente: Facebook restringe el acceso de los motores de búsqueda. Sin embargo se les puede permitir acceder a la información que se encuentra configurada con la opción “Todos” (fotografía y nombre) además de la

información de nuestro perfil que hayamos configurado para que la vean todos. En el caso de que queramos restringir la visibilidad de parte de nuestro perfil o impedir que los motores de búsqueda indexen nuestro perfil lo podemos llevar a cabo a través de la configuración de la privacidad de nuestra cuenta.

- Para ayudar a mejorar o promocionar Facebook: en ocasiones se comparten datos con terceros con el fin de mejorar los servicios que presta la red. En estos datos no se puede identificar a ningún usuario en particular ni vincularse a éste con ninguna información o acción específica.

- Para prestarte servicios: Facebook puede ofrecer información a los proveedores de servicios con el fin de facilitar el uso de los servicios que pone a nuestra disposición. El acceso a nuestra información para que los proveedores la utilicen tendrá un carácter temporal, pero este uso que hagan de ella siempre estará restringido a la ayuda que prestan para ofrecer el servicio.

- Para publicitar sus servicios: Facebook puede pedir a anunciantes externos que muestren anuncios para promocionar sus servicios. Esto se realizará a través de la presencia de una cookie, pero no se compartirá más información con el anunciante.

- Para ofrecer servicios conjuntos: Facebook presta servicios de forma conjunta con otras empresas, como con Marketplace. En el caso de que utilices estos servicios tus datos serán utilizados para mejorar el servicio. Sin embargo, antes de que empieces a utilizar el servicio, se mostrará la política de privacidad del servicio que vas a utilizar.

- Para responder a requerimientos legales y evitar daños: se puede revelar información con arreglo a citaciones, órdenes judiciales u otros requerimientos (incluidos asuntos civiles y penales) si creemos de buena fe que la ley exige dicha respuesta. Esto también tiene vigor en las jurisdicciones ajenas a los Estados Unidos, donde tiene la sede Facebook, para cumplir con las leyes propias de cada país. También podrá compartir información para evitar que se cometa un fraude u otra actividad ilegal, evitar un daño físico inminente o proteger tanto a Facebook como al usuario de personas que infrinjan la Declaración de derechos y responsabilidades. Esto puede incluir compartir información con otras empresas, abogados, tribunales u otras entidades gubernamentales.

El apartado 7 trata sobre cómo podemos eliminar o cambiar la información que previamente habíamos añadido.

- Edición de nuestro perfil: podemos realizar las operaciones que queramos, bien eliminando o modificando la información de nuestro perfil desde el apartado "Editar mi perfil". Cualquier cambio que hagamos se mostrará de inmediato.

- Eliminar los contactos cargados: se puede eliminar la lista de los contactos cargados mediante las herramientas que utiliza Facebook para importar contactos con el fin de cargar direcciones a través de las páginas de ayuda. Si también queremos eliminar las direcciones de correo de amigos que hemos invitado a unirse a Facebook lo podemos hacer a través de la página del historial de invitaciones.

- Desactivación o eliminación de la cuenta: este es otro punto donde se ha generado más controversia. Existen dos opciones para darte de baja en Facebook. La primera de ellas es desactivándola. El problema reside en que cuando la desactivas, ningún usuario podrá ver tu cuenta, pero no será eliminada. El hecho es que Facebook mantendrá todos tus datos, incluidos fotografías, contenido que hayas agregado, etc. por si en un futuro decides volver a activarla. Según explica Facebook, muchos usuarios desactivan sus cuentas por motivos temporales y al hacerlo, piden que se mantenga su información hasta que vuelvan a Facebook. Por ello, si quieres volver a reactivar tu cuenta, al hacerlo mantendrás todos los datos, pareciendo que nunca te has ido. El segundo caso que se puede dar ese el de eliminar la cuenta. Ésta es la única manera de borrar tu cuenta de forma permanente. Facebook avisa que una vez eliminada nunca podrás reactivarla. Para poder dar de baja tu perfil lo puedes hacer desde la configuración de tu cuenta.

- Limitaciones sobre la eliminación: como decíamos antes, éste es uno de los motivos que más preocupan a los usuarios de Facebook en relación a la privacidad. A pesar de que has eliminado tu cuenta, Facebook puede tener copias de dicha información visibles en otro lugar en la medida en que se haya compartido con otros, se haya distribuido de otro modo conforme a tu configuración de la privacidad, o haya sido copiada o almacenada por otros usuarios. Sin embargo, tu nombre dejará de estar asociado con dicha información en Facebook. Es el caso de que si mientras tenías tu cuenta, publicaste algo en el perfil de un amigo, esa información se mantendrá pero no aparece tu nombre, sino que aparecerá usuario anónimo. También Facebook se reserva el derecho a conservar cierta información para evitar el robo de identidades y otras conductas inadecuadas, incluso si se ha solicitado la eliminación.

  En relación a las aplicaciones y sitios web, éstos pueden conservar tu información hasta el límite permitido por sus condiciones de servicio o políticas de privacidad. Sin embargo, una vez que te has borrado de su servicio, ya no podrán acceder a nuestra información.

- Copias de seguridad: la información eliminada y borrada puede permanecer en copias de seguridad hasta un máximo de 90 días, pero no estará disponible para los demás.

- Información de contacto de no usuarios: si ya no eres usuario de Facebook, y otro usuario nos facilita tu dirección de correo electrónico y quieres que esa información sea eliminada puedes hacerlo a través de las distintas páginas de ayuda de Facebook. Sin embargo, esa solicitud sólo se aplicará a las direcciones que tengamos en el momento de la solicitud y no a ninguna dirección que los usuarios nos faciliten posteriormente.

El penúltimo apartado hace referencia a como gestionan nuestros datos y a cómo protegen nuestra información.

- Medidas que toman para mantener a salvo nuestra información: la información que Facebook toma de nosotros se encuentra en un servidor protegido con un firewall. Quizás no sea el método más seguro, ya que a día de hoy, los hackers pueden atravesar cualquier cortafuego. Cuando introducimos información confidencial como contraseñas y números de tarjeta de crédito, esa información se cifra usando tecnología de capa de socket seguro (SSL). A su vez, Facebook aplica medidas para aumentar la seguridad, como el análisis de la actividad de la cuenta por si hubiera algún comportamiento fraudulento o anómalo de otro tipo, o limitan el uso de funciones del sitio web en respuesta a posibles signos de abuso, pudiendo eliminar contenido inadecuado o enlaces a contenido ilegal, y pudiendo suspender o desactivar cuentas si incumplen los derechos y responsabilidades que se aceptan cuando uno se registra en la red.

- Riesgos inherentes a compartir información: Facebook acepta que ninguna medida de seguridad es perfecta ni impenetrable, por lo que la por más opciones de privacidad que añadas tu cuenta es vulnerable si hay un ataque informático. Facebook no puede garantizar que sólo vayan a ver tu información personas autorizadas ni pueden garantizar que la información que compartas en Facebook no pase a estar disponible públicamente, ni se hacen responsables de las acciones que hagan otros usuarios con los que compartes información. Ni se responsabilizan si alguien burla las medidas de seguridad de Facebook o tu configuración de la privacidad. Para reducir estos riesgos debemos emplear métodos de seguridad adecuados como serían elegir una contraseña segura, utilizar contraseñas diferentes para servicios diferentes y emplear software antivirus actualizado.

Por último, el noveno apartado, es el punto que cierra definitivamente la política de privacidad de Facebook y hace referencia a otra serie de condiciones que se deben cumplir.

- Cambios: Facebook se reserva el derecho a cambiar la política de privacidad cuando ellos quieran, pero, eso sí, siempre conforme a los procedimientos señalados en la Declaración de derechos y responsabilidades. Esta política de privacidad se aplica a toda la información que tienen sobre nosotros y sobre nuestra cuenta. Cuando se produzca modificaciones considerables en la privacidad, Facebook lo hará

público de tal modo que la información donde se reflejen los cambios llegue a todos los usuarios registrados.

- Consentimiento para la recopilación y procesamiento en Estados Unidos**.** Al utilizar Facebook, das tu consentimiento para que tus datos personales sean transferidos y procesados en Estados Unidos.

Esta política de privacidad está verificada por TRUSTe. Esta organización independiente lleva el programa de garantía de privacidad más importante del mundo. Certifica a más de 3.500 páginas web, entre las cuales se encentran portales y marcas como Yahoo, Microsoft, Apple Inc., IBM, Oracle, Intuit, eBay y, como ya hemos mencionado, Facebook.

Facebook también cumple el marco Safe Harbor de la Unión Europea (en adelante, UE) desarrollado por el Departamento de Comercio de Estados Unidos en cuanto a recopilación, uso y retención de datos pertenecientes a la UE. Como parte de la participación en Safe Harbor, Facebook se compromete a resolver todos los posibles conflictos que puedan surgir en relación con sus políticas y prácticas a través de TRUSTe**.**

Una vez analizada la actual política de privacidad de Facebook debemos comprobar si esta política se adapta a las prescripciones normativas que regulan el tratamiento de datos personales en el ámbito español. En concreto analizaremos si estas medidas cumplen los principios básicos que todo tratamiento de datos de carácter personal debe atender como hemos mencionado anteriormente en el apartado donde se estudia la LOPD.

Respecto a la información en la recogida de datos que según establece que el afectado será informado de modo expreso, preciso e inequívoco, en el momento en el que se recaben sus datos, del alcance del tratamiento que se va a realizar (art. 5 de la LOPD) constatamos que Facebook cumple con este principio debido a que en las primeras líneas de su política de privacidad informa detenidamente a los usuarios sobre los datos que va a recabar y cómo van a ser tratados.

En relación al artículo 5 de la LOPD, señalaremos algunos aspectos que completan el punto anterior:

- Facebook no especifica sobre la existencia de un fichero o tratamiento de datos de carácter personal, pero si nos indica la finalidad de la recogida de estos datos y de los destinatarios de la información. Concretamente destina un apartado completo, el número 5 para referirse a lo anterior. Aquí nos señala que esos datos se recopilan para tratar de ofrecer un uso seguro, eficaz y personalizado de la red, y a qué se destina esa información, como puede ser

para ponerse en contacto con nosotros, complementar nuestro perfil, hacernos sugerencias, etc.

- Facebook no hace mención al carácter obligatorio de las respuestas a las preguntas que les sean planteadas.

- Al igual que el punto anterior, Facebook tampoco señala las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

- Por contra, dedica todo el capítulo 7 a como podemos ejercitar los derechos de acceso, rectificación, cancelación y oposición, aunque, como señalaremos posteriormente, hay algunos de estos derechos que no se cumplen como es el derecho de cancelación.

- Por último, en relación a la identidad y dirección del responsable del tratamiento o, en su caso, de su representante, Facebook no indica claramente quien es el responsable, pero se da a entender qué es la propia red social la que se hace responsable de los datos.

La cantidad de datos que añadimos a Facebook cuando nos registramos en su red es excesiva, ya que debemos facilitar el nombre, correo electrónico, sexo y fecha de nacimiento. A medida que vamos avanzando en el registro, podemos proporcionar otra información sobre nosotros relacionada con nuestra ciudad de residencia, ciudad de origen, familia, relaciones, redes, actividades, intereses y lugares. Según se recoge en el artículo 4 de la LOPD los datos personales tratados deben ser adecuados, pertinentes y no excesivos, en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido, no pudiendo usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recabados.

En relación al artículo 7 de la LOPD, donde se recoge que, de acuerdo a los datos especialmente protegidos, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Facebook cumple con este artículo ya que en ningún momento dice que esos datos sean obligatorios, si no que queda en la voluntad del usuario añadirlos o no.

El artículo 9 de la LOPD indica que todas las organizaciones deben contar y aplicar medidas de seguridad técnica y organizativa que garanticen la confidencialidad, integridad y disponibilidad de la información. A pesar de lo anterior, Facebook se ha visto en varias ocasiones sorprendido en temas de seguridad, ya que debido a aplicaciones que estaba implementando, sufrió el robo de datos personales. Esto ha provocado que las medidas de seguridad que tenían haya aumentado para evitar posibles actos como los anteriormente mencionados.

Los responsables de custodiar nuestros datos, según se recoge en el artículo 10 de la LOPD, tienen la obligación de guardar secreto, mantener la confidencialidad y custodiar los datos que en la red se recogen. A pesar de lo que dice la Ley, Facebook no ha mantenido la confidencialidad y ha comercializado con esos datos, ya que se ha demostrado que ha vendido datos de carácter personal a empresas con el objetivo de que éstas pudieran ofrecer un servicio publicitario más personal. Esto señalado anteriormente incumple también con otro de los artículos que se recogen en la LOPD, ya que según se señala en el artículo 11 los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero, para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado, y en ningún momento Facebook nos indica en su política de privacidad que los datos que se recogen serán utilizados con fines comerciales.

Relacionado con el artículo 11, Facebook cumple con uno de los puntos que se indica en el citado artículo, ya que según indica en la política de privacidad si es necesario podrá revelar datos personales cuando así lo exija la normativa española en relación a citaciones, órdenes judiciales u otros requerimientos (incluidos asuntos civiles y penales). También podrá compartir información para evitar que se cometa un fraude u otra actividad ilegal, evitar un daño físico inminente o proteger tanto a Facebook como al usuario de personas que infrinjan la Declaración de derechos y responsabilidades.

Uno de los problemas de Facebook relacionados con el cumplimiento de la LOPD viene por parte de las fotografías. La imagen se considera un dato de carácter personal y por tanto, según lo establecido en el artículo 6.1 de la Ley Orgánica de Protección de Datos (LOPD), se debe obtener el consentimiento si queremos realizar un tratamiento sobre una fotografía en la que aparezca una persona cualquiera. Es decir, si queremos etiquetar a otro usuario, deberíamos contar con su consentimiento.

Otro de los problemas que tiene Facebook es que no cumple con el artículo 16 de la LOPD, el derecho de rectificación y cancelación. Según se recoge en su política de privacidad, Facebook hace una declaración de principios ya que explica claramente que cuando desactivas una cuenta, ningún usuario podrá verla, pero no será eliminada. La red guarda la información del perfil por si más tarde nos decidimos a volver a activarla. En el caso de que queramos eliminar la cuenta, Facebook puede tener copias de dicha información visibles en otro lugar en la medida en que se haya compartido con otros, se haya distribuido de otro modo conforme a tu configuración de la privacidad, o haya sido copiada o almacenada por otros usuarios, por lo que realmente nunca desaparecerás de la red.

A modo de conclusión, y una vez desmenuzada la política de privacidad de Facebook, vemos que hay una serie de aspectos que todavía no quedan del todo claro. El primero de ellos hace referencia a las aplicaciones y a los sitos web. Como se ha

repetido en varias ocasiones, es, de largo, el aspecto que más problema ha causado a Facebook. Cuando queremos utilizar una aplicación, la cantidad de información personal que debemos dar es exagerada. Papadopoulos y Kaponi (2010, p. 7) ponen un ejemplo que explica con claridad lo que ocurre con las aplicaciones "si yo me apunto a un gimnasio, espero que me pidan mi nombre y mi dirección. Y quizás como mucho, algo de información sobre mi estado físico, el nombre de mí médico o cuando es mi cumpleaños. Lo que no espero es que me pidan que libros y películas me gusta, a qué escuela fui cuando era un niño, donde trabajo, ni cuáles son mis creencias religiosas e ideologías políticas, o cual es mi orientación sexual ni responder a ningún tipo de pregunta, sea directa o indirecta. Ni mis amigos esperan que revele nada de información sobre ellos en el gimnasio".

Otro de los aspectos que llaman la atención es la configuración de la privacidad que Facebook toma como predeterminada. De esta forma, la información se divide en tres partes. En la parte "Todos" se incluyen actualizaciones de estado e información que los usuarios quieren compartir con un mayor grupo de personas. En "Amigos de amigos" se incluyen fotos y vídeos de ti, que suelen ser relevantes para los amigos de tus amigos. En "Sólo amigos" se incluye toda tu información de contacto y las cosas que sólo son relevantes para las personas con las que interactúas directamente.

También, el lugar en el que tu información es más transparente de todos es la aplicación de fotos de Facebook (D. Kirkpatrick, 2010, p.249). Es aquí donde nos resulta más difícil mantener un cierto nivel de privacidad sobre nosotros mismos. No tienes manera de controlar si otra persona cuelga una fotografía tuya. Lo único que puedes hacer es eliminar la etiqueta que te identifica y que provoca que esta información se distribuya por nuestra lista de amigos, pero en general, cuando la eliminas, la noticia del etiquetado ya ha aparecido en el canal de noticias. Existe la posibilidad de ajustar la configuración para que no podamos ser etiquetados nunca. Pero, por defecto, las fotografías son visibles. Todo el mundo puede verlas, a menos que ajustes deliberadamente los controles de privacidad, lo que la mayor parte de los usuarios no hacen.

El propio Mark Zuckerberg ha reconocido que si tuviera que volver a crear Facebook hoy, los datos de los usuarios serían por defecto públicos y no privados**,** como lo han sido durante años.

Concluyendo a modo de resumen, ante los distintos problemas que venía padeciendo últimamente por la privacidad, Facebook decidió simplificar la configuración de los perfiles evitando utilizar un lenguaje tan técnico que hacía que muchos de sus usuarios renegaran de la privacidad y dejasen su configuración como predeterminada. Para la creación de esta nueva política de privacidad, Facebook se ha basado en tres premisas. La primera es la necesidad de que el contenido sea fácil de entender incluso cuando los conceptos son complicados. Para ello la red social ha tratado de eliminar parte de los conceptos jurídicos y sustituirlos por otros más sencillos. En segundo lugar Facebook ha considerado que la nueva explicación debe ser visual e interactiva porque es lo que se utiliza en las páginas web de hoy. En lugar de disponer varias hojas de texto sin más, la nueva fórmula de Facebook incorpora elementos visuales y hace uso de diferentes tipografías para facilitar y orientar la lectura. Por último, Facebook ha tratado de configurar la información en relación a las preguntas

realizadas por los usuarios. El desarrollo del documento sobre privacidad de la red social se estructura respondiendo a las preguntas más importantes planteadas al servicio de ayuda por parte de los usuarios.

Capítulo 10
Las opciones para configurar la privacidad en Facebook

La última modificación que llevó a cabo Facebook con la intención de mejorar su privacidad fue a finales del año 2010.

Según Paula Ortiz (2010) habitualmente las plataformas de redes sociales se configuran en tres niveles de privacidad: amigos, que sería el primer grado de relación; amigos de amigos, el segundo grado de relación y toda la red, es decir, interactuar con todos los miembros de la red, independientemente de la relación que exista.

Facebook siempre ha supuesto que tenía una política de privacidad bastante rigurosa. Lo que la mayor parte de sus usuarios no conocen, es que si no configuran correctamente la privacidad, ésta queda predeterminada en el nivel más bajo, o lo que es lo mismo, que cualquier usuario pueda ver perfectamente todos tus datos.

La privacidad en Facebook ha sido un tema de continuo debate. De hecho, desde que la red apareció han sido varias las veces que se ha cambiado con el objetivo de que los usuarios puedan configurar a su gusto quién puede acceder a sus datos personales.

A continuación vamos a explicar cómo debería ser una correcta configuración de la privacidad. En primer lugar, y dando por hecho que se es usuario de Facebook, se debe ir a la parte superior derecha, y dentro del apartado “Cuenta” elegir la opción “Configuración de la privacidad”. Dentro de todas las secciones que podemos encontrar, la más importante de todas es “Compartir en Facebook”.

En esta sección se controla quién puede ver todo el contenido que publicas diariamente (como actualizaciones de estado, fotos y vídeos). También se incluye parte de lo que compartes sobre ti (fecha de nacimiento e información de contacto), así como el contenido que otros comparten sobre ti (comentarios en tus publicaciones y las fotos y los vídeos en los que estás etiquetado).

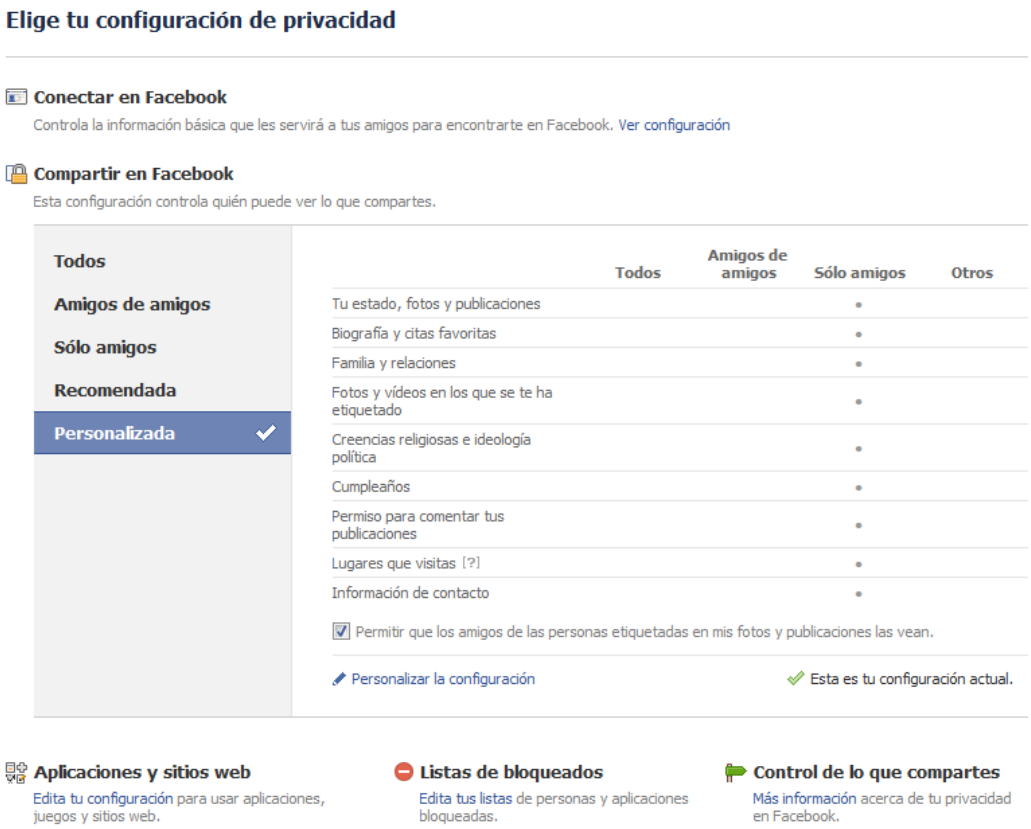


Fig. 15 Pantalla configuración de la privacidad

Como podemos comprobar esta sección se divide en dos partes. En la columna de la izquierda hay cinco opciones: Todos, Amigos de Amigos, Sólo Amigos, Recomendada, Personalizada.

Ahora dependerá de la elección que hagamos para saber quién podrá acceder a nuestra información (perfil, fotos, etc.). Si elegimos “Todos” cualquier persona podrá ver todo lo que tenemos en nuestro perfil, desde la información más básica hasta las fotografías que hayamos subido. Si por el contrario elegimos "Sólo Amigos", entonces solamente las personas que hayamos aceptado como amigos en la red, podrán acceder a nuestro contenido.

Facebook como opción predeterminada elige la opción “Recomendada”. Siguiendo la información que la propia red tiene en su web nos señala que “los conceptos "Todos", "Amigos de amigos" y "Sólo amigos" se pueden considerar como grandes

contenedores que constan de distintos grupos de información. Con la configuración recomendada, tu información se distribuye en los tres contenedores. En "Todos" se incluyen actualizaciones de estado e información que los usuarios quieren compartir con un mayor grupo de personas. En "Amigos de amigos" se incluyen fotos y vídeos de ti, que suelen ser relevantes para los amigos de tus amigos. En "Sólo amigos" se incluye toda tu información de contacto y las cosas que sólo son relevantes para las personas con las que interactúas directamente". Si nos decantamos por esta opción cualquier persona podrá ver nuestras fotos, leer nuestras actualizaciones de estado y ver nuestra biografía. Los amigos de nuestros amigos verían las fotografías y videos en los que hemos sido etiquetados, conocer cuando es nuestro cumpleaños, y sólo nuestros amigos podrán comentar en nuestro muro, y ver la información que tenemos de contacto (dirección, correo electrónico, etc.)

Por último encontramos la opción "Personalizada". En mi opinión es la opción más recomendable para aquellos usuarios que quieren controlar completamente su privacidad.

Para poder configurar la privacidad según nuestras preferencias debemos ir al vínculo que aparece en la parte inferior de donde están las cinco opciones de privacidad de Facebook. Este vínculo aparece junto a un lápiz y se llama "Personalizar la configuración".

Cuando hacemos clic sobre el vínculo aparecerá una nueva página donde elegiremos las opciones que más se adecuen a lo que queremos proteger. Esta página se divide en tres partes: Cosas que comparto, Cosas que otros comparten e información de contacto. Los ajustes que se pueden hacer a cada uno de ellos son básicamente los mismos.

En "Cosas que comparto" controlamos quien puede ver lo que publicamos. También quien puede enterarse de quienes forman parte de nuestra familia, nuestras relaciones sentimentales, nuestros intereses, biografía, creencias religiosas y políticas y hasta de nuestro cumpleaños.

En la pantalla, a cada lado hay un cuadro con un candado. Es ahí donde debemos señalar la opción que queremos aplicar. Al igual que en la configuración anterior podemos escoger entre "Todos", "Amigos de amigos", "Sólo amigos" o "Personalizar".

Fig. 16 Pantalla "Cosas que comparto"

Aunque a simple vista puede parecer poco importante, pero justo al final de este apartado encontramos una de las opciones más importantes a la hora de la configuración de la privacidad "Editar la configuración de la privacidad de álbumes de fotos y vídeos actuales". Aquí podemos controlar quién puede ver los álbumes de fotos que hemos subido a Facebook. Una vez dentro vemos que aparece una imagen por cada álbum que tenemos. Al igual que en los otros casos, podemos editar la opción de privacidad que queramos.

De vuelta a la página principal, el siguiente apartado que podemos modificar es "Cosas que otros comparten". Este apartado hace referencia a lo que los otros pueden escribir y publicar sobre nosotros, y cómo vamos a controlarlo. Aquí editaremos opciones como: "Fotos y videos en los que estoy etiquetado", "Pueden realizar comentarios en las publicaciones", "Mis amigos pueden publicar en mi muro", y "Pueden ver las publicaciones de amigos en el muro". En el caso de que queramos modificar la configuración para que mis fotos sólo puedan verlas mis amigos, debemos asegurarnos de que está opción esta seleccionada en la categoría ""Fotos y videos en los que estoy etiquetado". De no hacerlo la gente podrá ver fotos que hayan subido nuestros amigos en las que aparezcamos nosotros.

Fig. 17 Pantalla "Cosas que otros comparten"

Por último, en el apartado "Información de contacto" nos permite escoger a qué usuarios queremos mostrar nuestros datos de contacto, como son el número de teléfono, la dirección o el correo electrónico. Como opción más recomendada, ya que se trata de datos personales, elegiríamos la opción "Sólo amigos".

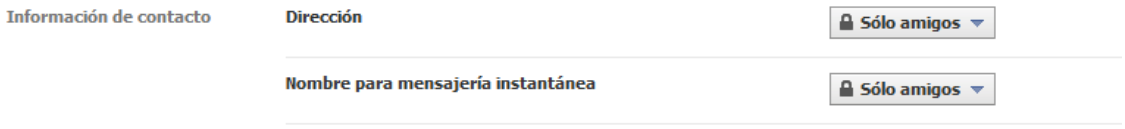


Fig. 18 Pantalla "Información de contacto"

Dentro del apartado referente a la privacidad en Facebook, además de lo anteriormente analizado, podemos llevar a cabo la configuración de otras secciones distintas.

En primer lugar vamos a hablar de **"**Conectar con Facebook**"**. De forma predeterminada Facebook da por hecho que queremos aparecer en el directorio que ellos manejan. Este directorio se trata de un listado en el que aparece nuestro nombre, junto a nuestra imagen de perfil, lo que hace que podamos ser vistos por cualquier usuario de la red. De hecho, Facebook dice que nuestro nombre, la foto de tu perfil, el sexo, las redes a las que pertenecemos y el nombre de usuario son datos que están accesibles a todo el mundo porque son necesarios para que tus amigos y familiares puedan conectar contigo. Para llevar a cabo una correcta configuración debemos modificar las distintas opciones que se nos muestran. Estas opciones son:

- Buscarme en Facebook: es lo que hace posible que cualquier usuario pueda buscarnos en la red.
- Enviarme solicitudes de amistad: depende de la opción de privacidad que elijas, pero en este caso es recomendable poner "Todos" porque si no sería una opción que quedaría muy restringida.

- Envío de mensajes: tú decides de quién quieres recibir mensajes. Como se dice en la página de configuración, esto te ayuda a comprobar que conoces a alguien antes de agregarlo a tus amigos.

- Ver mi lista de amigos: se trata de una herramienta útil ya que te puede poner en contacto con amigos de tus amigos. Lo peor de todo son las últimas palabras que añade Facebook para describir esta opción, ya que nos informa de que la lista de amigos siempre está a disposición de las aplicaciones y las conexiones a tus amigos pueden estar visibles en otras partes.

- Ver tu formación académica y trabajo: te posibilita la conexión con antiguos compañeros de clase y de trabajo, así como la posibilidad de descubrir nuevas oportunidades profesionales.

- Ver mí ciudad actual y ciudad de origen: al igual que la anterior opción, te permite volver a retomar el contacto con personas que a lo mejor hace años que no sabes nada de ellas.

- Ver mis intereses y otras páginas: te permite conectar con personas que tienen unos intereses comunes a los tuyos.

A continuación vamos a analizar **"**Aplicaciones, juegos y sitios web**"**. En esta sección podemos se controla qué información se comparte con las aplicaciones y los sitios web, incluidos los motores de búsqueda (las aplicaciones y los sitios web que tú y tus amigos utilizáis ya tienen acceso a tu nombre, la foto de tu perfil, tu sexo, las redes a las que perteneces, tu lista de amigos, tu identificador de usuario, tu nombre de usuario y a cualquier otra información que compartes con todos). En esta sección no tenemos la posibilidad de modificar muchas opciones, ya que la información que compartes depende de la aplicación o juego que hayas instalado. La mayor parte de estas aplicaciones para poder instalarlas te obligan a compartir todos tus datos personales, teniendo acceso completo al perfil, a las fotos, videos, etc. No es de extrañar que sea con estas aplicaciones con las que más problemas y denuncias ha sufrido Facebook en relación a la privacidad, ya que son las propias aplicaciones las que filtran información personal de los usuarios, ya que como he comentado antes, la mayor parte de ellas te obligan a compartir toda tu información.

Entre las nuevas características que ha añadido Facebook a la privacidad, hay una que destaca por encima del resto. Esta novedad consiste en que cada vez que publiquemos algo en la red, seamos nosotros mismos quienes elijamos quien puede verlo. Para ello debemos hacer ir al vínculo "Amigos", que aparece en la parte izquierda de nuestro perfil. Entonces se cargará una nueva página y dentro de ella, en la parte superior hay un botón llamado "Crear una lista". En esta lista añadiremos el nombre de los amigos que queramos que vean nuestras actualizaciones.

En palabras del propio Mark Zuckerberg recogidas en el diario El País ha explicado que "esta función se plantea ante el escaso uso que los miembros de la red social hacen de las listas (sólo un 5%). La propuesta permite acotar el número de amigos a los que se quiere dejar acceder a una determinada información. Hasta ahora, las opciones eran: amigos, amigos de los amigos o todo el mundo. Facebook considera

que la categoría "amigos" es demasiado genérica y no es del todo privada ya que algunos miembros cuentan con miles de ellos. Ahora, por ejemplo, podrá seleccionar a los componentes de su familia como receptores de determinados mensajes".

En definitiva, Facebook, de forma predeterminada, configura su privacidad en la opción " Recomendada". El problema principal que conlleva tener esta configuracion es que se muestran demasiados datos públicos, ya no solo a los usuarios de Facebook sino a todo Internet. Entre la información que se compartiría, además de la fotografía de perfil y el nombre del usuario, datos siempre visibles, estaría las actualizaciones de estado que el usuario realice.

Para conseguir que no se muestren más datos de los ya por sí visibles, entre las distintas opciones que nos ofrece Facebook es recomendable elegir la opción "Personalizada". A través de esta opción es el propio usuario quien elige lo que se muestra y quién lo puede ver. Además, realizar la configuración según esta opción no es nada complejo, ya que es el propio usuario quien elige lo que quiere que se muestre y lo que no quiere mostrar.

Capítulo 11
Los riesgos y peligros de la privacidad en Facebook

Desde el momento en el que te registras en una red social te encuentras con la posibilidad de sufrir una serie de riesgos que pueden surgir en diferentes momentos. Estos peligros pueden llegar, como hemos dicho antes, desde el momento en que te registras, cuando forma parte de ella o cuando quieres darte de baja de la red.

Los usuarios deben valorar siempre qué tipo de datos proporcionan a la plataforma y publican en su perfil, ya que no tiene la misma trascendencia el tratamiento por parte de la plataforma de los datos de carácter personal de nivel básico (nombre, dirección, teléfono, etc.), que otras información de contenido más sensible (nivel de renta, solvencia, recibos, afiliación sindical o política, salud, vida sexual, etc.), donde el nivel de protección y concienciación por parte del usuario deberá ser mucho mayor, dado que se trata de derechos pertenecientes a la esfera más íntima de su vida.

El primer momento donde se puede correr riesgo con la protección de datos es en la fase inicial de registro. Tiene cierto peligro debido a que en este momento debes añadir toda la información personal necesaria para poder operar en la red social.

En este momento, los datos se pueden ver sometidos a varios riesgos:

- Que los datos que te pidan para poder registrarte sean excesivos (alguno de los cuales pueden calificarse de sensibles): cuando estamos completando los datos iniciales se nos pide una serie de datos como pueden ser datos referentes a nuestra ideología política, orientación sexual y tendencia religiosa. De todas formas estos datos tiene un carácter voluntario y todo usuario es libre de publicar el contenido que deseé respecto a sí mismo, debe considerar las

implicaciones que ello puede conllevar para su vida y las personas de su entorno, ya que estos datos serán visibles por todos sus contactos y, dependiendo de la configuración del perfil, por todos los usuarios de la red. Es por ello que los usuarios y los responsables de las redes deben limitar y controlar en todo momento que el grado y la trascendencia de los datos publicados no sea extrema. Debe tenerse en cuenta que el artículo 7 LOPD obliga a contar con un consentimiento expreso y por escrito en lo que se refiere a datos relativos a ideología, religión o creencias, y expreso en el ámbito de la salud, origen racial y vida sexual.

- Que el grado de publicidad del perfil de usuario sea demasiado elevado: para poder mantener tus datos a salvo, debes realizar una adecuada configuración de la privacidad. Esto es importante porque así determinas quién quieres que vea tus datos. El caso que estamos estudiando, Facebook tiene activado por defecto el mayor grado de publicidad, resultando el perfil de acceso completamente público lo que supone un grave riesgo para la seguridad de los datos personales de los usuarios, en la medida en que éstos serán accesibles por parte de cualquier usuario de la plataforma.

- Información relativa a la política de privacidad: La información es poco clara y no se especifica suficientemente el uso que puede hacerse de los datos, como, por ejemplo, la cesión a terceros para poder realizar publicidad. Además, la identificación del responsable del tratamiento es a menudo confusa.

- Ausencia de mecanismos para controlar la edad mínima para registrarse: en Facebook la edad mínima para poder registrarse es de 13 años, aunque en España la edad es más elevada, estando el límite en los 14 años. De todas formas, no hay una manera clara de controlar el acceso, debido a que cuando añades tus datos, a la hora de decir tu edad, es muy fácil mentir en este sentido, poniendo más años de los que realmente tienes, y a no ser que Facebook reciba una denuncia de que un menor está en su red no hace nada para evitarlo.

Esta segunda etapa hace referencia al desarrollo de la actividad del usuario en la red. En este momento los aspectos que pueden poner en riesgo la seguridad y protección de datos personales de los usuarios son:

- La publicación excesiva de información personal (propia o de terceros) y la falta de control que hay sobre lo que se publica. En esta fase se mantiene el posible riesgo que conlleva la publicación excesiva de información personal por parte de los usuarios. Aquí debemos hacer mención a la posibilidad que existe de que otros usuarios publiquen también datos respecto de terceros, lo que puede conllevar el tratamiento y la cesión pública de datos de personas que no han prestado el consentimiento para ello. En definitiva se trata de una falta de control respecto de la publicación de información, entendida en un sentido amplio. En relación a estas cuestiones, se plantean otras dudas respecto al uso de etiquetas y metadatos que permiten identificar e insertar información relativa a terceros ajenos a la red social.

- Uso de cookies sin permiso del usuario: a menudo utilizan este tipo de ficheros que tienen la posibilidad de almacenar determinada información sobre el usuario y su tipo de navegación a través de un sitio web. Estos ficheros se instalan en los equipos de los usuarios, de forma que resulta posible detectar el lugar desde el que accede el usuario, el tipo de dispositivo empleado (móvil o fijo) para el acceso, el tipo de contenidos accedidos, los lugares más visitados y las acciones habituales realizadas durante la navegación, así como el tiempo empleado en cada una de las páginas, entre otras muchas funcionalidades. Este modo de recabar los datos funciona de forma automática, al contrario que en el caso de los formularios.

- Perfil indizado de manera automática por los buscadores de internet: algunas redes sociales permiten por defecto que los perfiles de los usuarios sean indexados por los motores de búsqueda de forma pública en la Red. Esto supone una amenaza para la protección de datos personales de los usuarios, en la medida en que sus datos básicos y principales contactos se exponen públicamente en la Red, accesibles por parte de cualquier usuario, pudiendo llegar a ser empleadas esas informaciones de forma descontrolada por terceros.

Los usuarios ponen a disposición de la red mucha información, ya sea de forma consciente o de forma inconsciente. Esta última forma de proporcionar datos está ligada a que la navegación por Internet deja un rastro vinculado a la dirección IP.

También se pone de relieve que las redes sociales constituyen un entorno en qué fácilmente puede producirse la suplantación de la identidad. De hecho, no es nada extraño que uno encuentre en una red social varias personas que reivindican la misma identidad, sobre todo cuando se trata de personas famosas.

Por último, la tercera etapa más crítica para la protección de datos personales se sitúa en la fase en la que el usuario pretende darse de baja del servicio. Es aquí donde debemos tener en cuenta los siguientes problemas:

- La imposibilidad de realizar la baja efectiva del servicio: darse de baja en una red social es una tarea difícil. Cuando este proceso debería ser más sencillo que el darse de alta, se ha comprobado que al solicitar la baja siguiendo las pautas que marcan las redes, la baja no se hace efectiva, manteniéndose los datos personales de los usuarios a disposición de los responsables de la red social. Debido a este problema, la Unión Europea va a garantizar el derecho al olvido en la red, objetivo es que los ciudadanos puedan exigir a las empresas que borren sus datos personales o fotos cuando se den de baja de sus servicios. Este punto quedará más detallado en el capítulo “Derecho al olvido”.

- La conservación de datos y el cumplimiento del principio de calidad de los datos: las redes mantienen los datos generados por los usuarios con vistas publicitarias, ya que les sirven como herramienta a través de las cuales ofrecer un servicio más personal ya que conocen las preferencias y perfiles de los usuarios, lo que hará posible realizar una publicidad más contextualizada.

Para concluir, debemos señalar que existe un problema derivado de la falta de toma de conciencia real por parte de los usuarios de que sus datos personales pueden ser accesibles por cualquier persona y del valor que éstos pueden llegar a alcanzar en el mercado. En muchos casos, los usuarios hacen completamente públicos datos y características personales que en ningún caso expondrían en la vida cotidiana como ideología, orientación sexual y religiosa, etc. Pero no debemos obviar el hecho de que las redes sociales son herramientas públicas y accesibles para cualquier tipo de persona, con independencia de que las intenciones con las que se accede sean negativas o ilícitas. De hecho, es habitual que los usuarios de redes sociales no sean conscientes o descuiden la privacidad de sus perfiles.

Entre los riesgos más importantes que debemos tener en cuenta se encuentra que no se dé de baja la información cuando eliminamos nuestra cuenta.

Capítulo 12
Conductas lesivas

Una buena manera de entender los riesgos a los que nos enfrentamos en el mundo de las redes sociales es aproximarnos desde el punto de vista de los conflictos que comienzan a plantearse.

Por tanto, en el ámbito de las redes sociales podemos identificar distintos tipos de conductas relevantes desde el punto de vista de la protección de datos. Como se va a observar en los casos que se van a analizar, la causa principal consiste en la publicación de algún tipo de dato personal o de documentos o archivos que lo contengan. Esto a su vez desde la perspectiva de su repercusión en los derechos de los afectados plantea distintos escenarios alternativos en función de la configuración de la red:

- Si tu perfil sólo está disponible para que solo pueda ser consultado por tus amigos, los problemas que se pueden producir son (Martínez, 2009, p.97):
  - Un usuario puede oponerse a algo que se ha publicado en nuestra cuenta, bien publicado por nosotros o por terceros con permiso.
  - Un usuario se apropia de determinada información y/o la utiliza o publica más allá del grupo cerrado y sus finalidades.
  - Un usuario publica información con oposición de otro u otros de ellos.
- Si tu perfil se encuentra abierto, existe una voluntad manifiesta de que los contenidos sean accesibles a todos los usuarios. El grado de apertura no dependerá del usuario, sino de la configuración de la red social.

Para mostrar los conflictos más habituales que se suelen producir, para conocer los casos que ya han sido juzgados hemos recurrido tanto a periódicos de tirada nacional e internacional, agencias de prensa o a través de los informes que presenta la AEPD.

Los conflictos más habituales suelen ser:

a) Suplantaciones de identidad: al darse de alta en una red social se descubre que otro usuario ha asumido nuestra identidad. Se trata de un comportamiento muy obvio, en cuanto a sus fines, en redes sociales en las que se buscan relaciones de negocios o profesionales. Por otra parte, en los casos de acoso a menores se suele suplantar la identidad de otro menor para conseguir ganar la confianza de la víctima.

- Ésta ha sido uno de los conflictos que más causas judiciales ha provocado. El concepto de "suplantación de identidad" está recogido como delito en nuestra normativa penal, adopta una nueva trascendencia en el mundo online, dado que cualquier usuario puede contar en Internet-y normalmente así sucede- con varias "identidades digitales". Uno de los casos más emblemáticos que corresponden a este tipo es el de un empleado despedido por crear un perfil falso de su jefe en Facebook. Un trabajador del hospital Nuestra Señora del Perpetuo Socorro de Cartagena ha sido despedido por crear una cuenta en la red social Facebook a nombre del director del centro con expresiones "objetivamente injuriosas". El acusado creó una cuenta en la red a nombre del director gerente del hospital, sin conocimiento de éste y utilizando sus datos personales, así como una cuenta de correo electrónico. El Juzgado afirma que los hechos, tanto por la suplantación de personalidad que implican como por la gravedad de las expresiones objetivamente injuriosas atribuidas al acusado, "con referencia a la empresa en la que presta servicios y con intención de difundirlas revisten la gravedad suficiente para justificar la imposición de la sanción de despido". Para el juez, "constituyen faltas muy graves de trasgresión de la buena fe contractual y abuso de confianza, así como injurias a un superior jerárquico".[5]

b) Difusión no consentida de fotografías con variantes diversas:

    - Casos en los que por pura experiencia un usuario incluye en su espacio fotografías de amigos o conocidos, y las etiqueta sin su consentimiento. Las consecuencias que puede acarrear este acto pueden ser variadas, aunque las más difundidas son las que se refieren al acceso posterior por las empresas a estas fotografías influyendo en sus decisiones de contratar o despedir a un empleado.

    - Existen fotografías que se publican con la clara intención de hacer daño. Los entornos escolares suelen ser prolíficos en este tipo de

[5] Otros casos destacados fueron la condena por crear un perfil falso con el objetivo de chantajear a sus compañeros, la pena de 13 años de cárcel al conocido como “violador de Facebook”

supuestos en los que se pretende ridiculizar o vejar a compañeros o profesores incluyendo fotografías tomadas con móviles o comentarios despectivos. También se suelen utilizar las fotografías con un ánimo de venganza, como cuando una pareja deja de ser tal y uno de los dos implicados cuelga fotos íntimas del otro. Este es uno de los casos más habituales. De hecho, ya hay condenados por este tipo de actos. Es el caso de Joshua Simon Ashby que fue condenado por publicar fotos de su ex pareja desnuda. Se trata de la primera persona en recibir una condena por publicar en una red social contenidos que puedan violar el derecho al honor y a la propia imagen de terceros. La imagen iba acompañada con comentarios subidos de tono variedad de insultos. Fue sentenciado a cinco semanas de cárcel.

c) Por último, el otro gran grupo se corresponde con los comentarios lesivos en las publicaciones. Por ejemplo, cuando un usuario de la red social utiliza su muro para insultar o difamar a otra persona, bien sea anónima o conocida. Debido a este tipo de actos encontramos algunas condenas significativas, como es la condena a un vecino de Pamplona por verter injurias contra la alcaldesa, Yolanda Barcina, en una página de Facebook. El acusado ha sido condenado a indemnizar a Barcina con 500 euros y a una multa de 180 euros, y requiere a Facebook que clausure la página "este año tenemos sequía por la puta Barcina"[6]

Si consideramos estos supuestos podemos valorar como una misma conducta, como puede ser publicar una fotografía sin consentimiento, puede verse amplificada dependiendo en el escenario en el que nos situemos.

Con el desarrollo de las redes sociales han aparecido una serie de peligros que anteriormente no eran comunes. Como hemos podido comprobar en los párrafos anteriores, el delito que más casos ha provocado es el de la suplantación de la identidad. Entrar en la cuenta o el perfil de otra persona es una conducta que de por sí puede comportar graves consecuencias jurídicas. Al acceder a una cuenta ajena se puede estar cometiendo un delito de lesión de privacidad considerado por la normativa española como una forma de descubrimiento y revelación de secretos.

[6] Otra de las condenas más significativas ha sido la de un joven francés que fue condenado por insultar a un policía a través de su muro en Facebook.

Capítulo 13
Derecho al olvido

Desde que aparecieron las redes sociales online, se ha notado una creciente preocupación en relación a la privacidad de los datos personales. El problema que a todos nos preocupa es la pérdida de control sobre nuestra información personal. Hasta el momento no existen fórmulas precisas ni claras que faciliten eliminar nuestros datos si decidimos hacerlo, dependiendo en gran medida de la voluntad del sitio donde los alojamos.

Pero parece que esto va a cambiar. La Comisión Europea (en adelante, CoE) ha anunciado que regulará el “derecho al olvido”, es decir, el derecho en virtud del cual los usuarios pueden exigir a los proveedores de servicios de Internet que borren sus datos completamente cuando dejen de ser necesarios para los fines para los que se recabaron o cuando el cliente se dé de baja.

Además de la Ley del Olvido, la vicepresidenta del Ejecutivo comunitario ha desvelado también que junto a esta propuesta, también se exigirá que la configuración de redes sociales como 'Facebook' garantice la "privacidad por defecto", de forma que los datos de los usuarios no puedan procesarse salvo si éstos han dado su permiso expreso.

La Comisión Europea ha publicado un Eurobarómetro (Comisión Europea, 2011) sobre la protección de datos, donde se muestran datos que confirman que los usuarios estaríamos más que contentos con esta nueva directiva, algunos de los datos más representativos son:

- El 75 % de los internautas de la UE quieren poder borrar sus datos personales en línea siempre que lo deseen.

- Casi un 90 % de los ciudadanos revelan datos personales que incluyen información biográfica.

- Por ello, un 70% de los encuestados señala su preocupación sobre el uso que las empresas hacen de sus datos.

- También revela que el 74% quiere que sea necesario su consentimiento expreso antes del proceso de obtención y procesamiento de sus datos personales en internet.

La vicepresidenta de la Comisión y responsable de Justicia, Viviane Reding (Público, 16/3/2011), ha anunciado durante este año presentará una propuesta legislativa para proteger el 'derecho al olvido' en las redes sociales. El objetivo principal que se busca con esta medida es obligar a sitios como Facebook y otras redes sociales a que eliminen completamente nuestra información personal cuando nos demos de baja.

La iniciativa quedará incluida en la propuesta legislativa que la Comisión Europea (CE) presentará en 2011 para reforzar las normas de protección de datos de la Unión Europea (UE) y adaptarlas a los cambios provocados por las nuevas tecnologías. "La protección de los datos personales es un derecho fundamental", destacó la vicepresidenta de la CE y responsable de Justicia, Viviane Reding.

"Al modernizar la legislación, quiero clarificar específicamente que las personas deben tener el derecho, y no sólo la posibilidad, de retirar su consentimiento al procesamiento de datos", ha explicado Reding.

La nueva legislación tendrá como prioridad reforzar los derechos de las personas. Para ello, se les facilitará un mayor nivel de protección y control sobre sus propios datos, sobre todo en Internet, añadió. Estas medidas se aplicarán especialmente a las redes sociales, aunque también a los proveedores de servicios de Internet y buscadores, quienes tendrán que limitar la recogida de datos al mínimo necesario y deberán informar a los usuarios de forma transparente sobre quién recoge y usa sus datos y sobre cómo, con qué fines y por cuánto tiempo lo hace.

Por otro lado, las compañías estarán obligadas a notificar a sus clientes cualquier acceso ilegal a sus datos personales por parte de personas no autorizadas**.** La Comisión quiere que los clientes estén informados de cómo se está controlando su uso de Internet para dirigirles publicidad. “Los usuarios deben saber cuándo los comercios ‘on-line’ usan las páginas web consultadas con anterioridad como base para hacer sugerencias de productos”*,* aseguró la vicepresidenta del Ejecutivo comunitario. (La Vanguardia, 7/3/2011)

Pero Facebook ha criticado esta medida. En palabras del responsable de privacidad de Facebook en Europa, Richard Allan, se mostró contrario a la intención de la Unión

Europea de garantizar el derecho al olvido en Internet. Richard Allan explicó que la privacidad se puede mejorar, pero crear una ley genérica en función de casos concretos es un error. Además, aseguró que los usuarios de Facebook están más preocupados por que se garantice la permanencia de sus fotos e informaciones que por su eliminación.

Según Allan, la creación de la ley de derecho al olvido se está produciendo en función a denuncias concretas, no a una necesidad común. "Es un error cambiar leyes de protección de datos en base a casos excepcionales", explicó.

Allan ha declarado que la gente puede borrar cualquier cosa de la red social, sin restricciones**.** Según el directivo, los casos concretos que han generado polémica en relación al derecho al olvido tienen su origen en contenidos indexados por los buscadores, almacenados como caché. Allan ha confirmado que desde Facebook trabajan continuamente para mejorar la privacidad de sus usuarios y ha reiterado que una ley como la que planea la Unión Europea no es la solución.

"La regla de la "privacidad por defecto" evitaría, de esta manera, la recogida de datos a través de aplicaciones de software, por ejemplo. El uso de los datos para cualquier otro objetivo que vaya más allá de los que estén especificados sólo se permitirá con el consentimiento explícito del usuario", ha explicado Reding.

Debido a esto, desde los organismos de la Unión Europea se exigirán una mayor transparencia a las redes sociales, que estarán obligadas a informar a los usuarios sobre los datos que recogerán, con qué objetivos, cómo pueden ser usados por terceras partes y cuáles son los riesgos para que no pierdan el control sobre su información personal.

Las declaraciones de la propia Reding lo dejan bastante claro: "Quiero garantizar que quien se inscribe en una red social goce de una mayor claridad. A menudo, condiciones desfavorables como restringir el control de los usuarios sobre sus datos personales o hacer los datos públicos de manera irreversible no se mencionan claramente".

Para lograr estos objetivos, la Comisión obligará a que las empresas situadas fuera de la UE que procesen datos de ciudadanos comunitarios cumplan también estas reglas.

Por último, deberíamos señalar otro aspecto que ha cobrado una gran importancia en los últimos tiempos ¿Qué ocurre con los datos de una persona cuando ha fallecido?.

En el caso de las personas fallecidas, nada se dice en la normativa de protección de datos, pero atendiendo a la normativa civil, se considera que no pueden ser titulares de derechos. Por lo tanto, no tiene sentido hablar de su derecho a la protección de de sus datos personales y de su poder de disposición, plasmado en el consentimiento. Pero no podemos dejar de lado el hecho de que en muchas ocasiones se tratan datos

de personas fallecidas, y en el caso de las redes sociales, sus usuarios pueden publicar datos de personas fallecidas.

La Agencia Española de Protección de Datos ha señalado que, aunque el derecho a la protección de datos personales es un derecho personalísimo que se pierde con el fallecimiento, los familiares de la persona fallecida podrán ejercer bien un derecho de acceso, bien un derecho de cancelación. Pero, para ello, debe estar previsto en alguna Ley. Esta sería la vía alternativa de la que dispondrían terceras personas distintas al usuario de las redes sociales para garantizar los derechos del familiar fallecido, sin que se pudiera hablar del ejercicio de un derecho de protección de datos personales, ni por parte de dichos herederos ni, mucho menos, por parte del usuario.

De momento, Facebook ha creado un espacio donde se mantienen los perfiles de los usuarios fallecidos como homenaje hacia ellos. Estos 'perfiles conmemorativos' pretenden ser como un lugar donde la gente puede guardar y compartir los recuerdos de aquellos que han fallecido".

Los perfiles son privados y, para evitar bromas pesadas, hay que suministrar a Facebook una prueba de que conocemos realmente a la persona. Paralelamente, Facebook se compromete a retirar la información personal del difunto disponible en el portal para evitar a sus seres queridos el mal trago de ver regularmente su foto o sus antiguos mensajes.

A modo de conclusión, debido al problema que supone la dificultad de darse de baja de una red social, y lo que ocurre con esos datos, la Comisión Europea prevé llevar a cabo un proceso legislativo referente a la protección de datos de los ciudadanos europeos. Con esta nueva legislación lo que se pretende es resolver las situaciones que se dan en el entorno digital respecto al almacenamiento de datos personales por parte de las empresas, como poder exigir que cuando un usuario abandone una red social, todos los datos se borren de forma completa, algo que hoy en día pocas plataformas sociales permiten.

PARTE FINAL

Conclusiones

Las conclusiones de este trabajo se han ido presentando en relación con las diferentes cuestiones abordadas. Ahora, no se trata de reproducir todas las ideas que se han expuesto, sino de destacar aquellas que son más importantes y que hemos intentado subrayar en esta investigación sobre la regulación de la valoración y selección de documentos. La recapitulación se ha organizado atendiendo a los diferentes objetivos que se planteaba el trabajo.

La información que está disponible para todos los usuarios de Internet es excesiva. Entre los datos que se ofrecen están nuestro nombre, foto de perfil y conexiones permanecerá accesible y visible no sólo para los usuarios de Facebook, sino que también lo estará para todas aquellas personas que naveguen por Internet, estén o no registrados en Facebook. Como se ha analizado en los puntos anteriores del trabajo, el mayor problema que esto provoca es que esa información puede ser indexada por los motores de búsqueda de terceros y puede ser importada, exportada, distribuida y redistribuida por nosotros y otros sin limitaciones de privacidad. Dicha información puede asociarse contigo, incluido tu nombre y fotografía de perfil, incluso fuera de Facebook, por ejemplo, en motores de búsqueda públicos y cuando visites otros sitios de Internet

Las distintas políticas de privacidad que ha tenido Facebook en su historia destacan por ser poco claras, confusas. Una enorme cantidad de usuarios de esta red social no sabe cómo configurar las opciones de seguridad o las encuentra sumamente confusas y muchos se están cuestionando si darse o no de baja. El problema es que por defecto, siempre están configuradas las mínimas opciones de privacidad y la utilización de la mayoría de las aplicaciones de terceros implica la transferencia de los datos particulares. Para aumentar el descontento de los usuarios, se suman los fallos de seguridad en el sistema como el que se presentó en el chat y obligó a cerrarlo durante unas horas. Aunque Facebook se ha esforzado en comunicar estos cambios

en forma sencilla, probablemente estos usuarios encuentren engorroso leer las Políticas de Privacidad o no lleguen a comprenderlas.

Una vez analizadas todas las políticas de privacidad se puede llegar a la conclusión que, de todas ella, la más segura para el usuario era la primera, la del año 2005. Facebook tiende a ser cada vez más transparente, y como hemos podido ver, con el paso de los años los datos que están accesibles a los demás son cada vez mayores. En la política de privacidad del año 2005 había un elemento que le hace diferente a la actual, para poder ver cualquier perfil de Facebook debes estar registrado en la red. En la política actual no hace falta. Aunque tengas una configuración de tu cuenta correcta, cualquier usuario de Internet puede ver, como mínimo, tu nombre y tu fotografía de perfil. En el año 2005 ninguna información personal que enviases a Facebook estaría disponible para los usuarios de la página que no pertenezcan a alguno de los grupos especificados por ti en tus ajustes de privacidad.

La política de privacidad que siguen las aplicaciones presentes en Facebook deja mucho que desear. A pesar de que las normas de la red social prohíben a estos la transmisión de datos de sus usuarios a empresas publicitarias, incluso si el usuario lo permite cuando configura sus exigencias de privacidad en la red, se han demostrado que algunas aplicaciones transmitieron los nombres de decenas de millones de usuarios y, en algunos casos, los de sus 'amigos', a compañías de publicidad y otras de rastreo en internet. Si Facebook, como pretende, quiere ser un ejemplo para todas las redes sociales debería aplicar una política más restrictiva a las aplicaciones que en esta red social encontramos, debido a que cuando aceptamos las condiciones de uso de estas aplicaciones cedemos la posibilidad de que puedan consultar toda la información que tenemos en nuestro perfil.

Las redes sociales, como ya hemos visto, no escapan a la normativa sobre protección de datos, por lo que los usuarios, titulares de la información, deben verse dotados de las facultades que confiere el derecho fundamental a la protección de datos, esto es, los conocidos derechos ARCO (acceso, rectificación, cancelación y oposición) y se deben cumplir con los requisitos o principios para que el tratamiento de esa información sea lícito, tales como el consentimiento libre y la información.

Los derechos ARCO son el conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales. Estos derechos se regulan en el Título III de la Ley Orgánica de Protección de Datos (LOPD) y en el Título III de su Reglamento de Desarrollo.

Se trata de derechos cuyo ejercicio es personalísimo, es decir, que sólo pueden ser ejercidos por el titular de los datos, por su representante legal o por un representante acreditado, de forma que el responsable del fichero puede denegar estos derechos cuando la solicitud sea formulada por persona distinta del afectado y no se acredite que actúa en su representación.

El ejercicio de estos derechos se debe llevar a cabo mediante medios sencillos y gratuitos puestos a disposición por el responsable del fichero y que están sujetos a

plazo, por lo que resulta necesario establecer procedimientos para su satisfacción. Si la persona reclamante cree que sus derechos no han sido atendidos en forma y plazo según la LOPD y su reglamento, puede acudir a la tutela de la Agencia Española de Protección de Datos (AEPD).

Facebook incumple con los puntos de mayor importancia, ya que no se trata de una red tan segura como parece, puesto que en varias ocasiones ha sufrido ataques que han conllevado la copia de datos de carácter personal de sus usuarios. También incumple con el artículo 16, ya que no se cumple con el derecho de rectificación y cancelación, puesto que aunque elimines tu cuenta siempre habrá restos de tus datos en la red, bien a través de copias de seguridad o por la información que queda recogida en otros usuarios. Otro de los puntos débiles es que se pide muchos datos de carácter personal cuando nos registramos.

La configuración predeterminada de la privacidad de Facebook ofrece más datos de los necesarios. Facebook, en el camino de hacer cada vez más públicas las cuentas de los usuarios, ha establecido como configuración predeterminada la opción "Recomendada". Este es el nivel más bajo de todos los que podemos encontrar en Facebook, a no ser que uno mismo establezca su configuración en abierta para todos. Con la opción recomendada, la cuenta de cualquier usuario puede ser vista por cualquiera que navegue por Internet. Los datos que estarían disponibles para todos serían "Mis datos", "Fotos", "Publicaciones", "Biografía", "Citas favoritas", "Familia" y "Relaciones". Demasiados datos para compartir. La configuración de la cuenta para delimitar la privacidad no es un aspecto en el que los usuarios se centren demasiado, no llegando a conocer muchos de ellos los datos que realmente pueden llegar a compartir.

Facebook ha tenido varios problemas con la Unión Europea debido a la privacidad. Si ya con la penúltima modificación de la política de privacidad fue "llamado a orden" debido a la gran cantidad de datos personales de los usuarios que quedaban expuestos, ahora se le ha vuelto a abrir un frente pero con dos vertientes. Por un lado estaría una de las nuevas características incorporadas por Facebook, el reconocimiento facial automático. Los encargados de la protección de datos de la Unión Europea han preguntado a Facebook sobre qué criterios tomó en cuenta para activar esta facultad en los perfiles sin consulta previo del usuario. Otra de las preocupaciones es que el reconocimiento facial podría relacionar información personal con las imágenes en la base de datos. La Unión Europea está preocupada porque el reconocimiento facial esté activado por predeterminado; y también ha cuestionado sobre los riesgos potenciales de esta herramienta para los usuarios.

El otro frente abierto con la Unión Europea está relacionado con el Derecho al olvido. La Unión Europea está presionando para que se adopten medidas más estrictas de protección de la privacidad, en un esfuerzo para conceder a los usuarios de Internet más control sobre los datos personales que recopilan, almacenan y explotan, en ocasiones, con fines comerciales. Las nuevas normas, que en principio entrarán en vigor este año, sitúan a la UE a la vanguardia de las leyes de privacidad en Internet y podrían influir en otros países, ahora que la ley sobre Internet se ha convertido en un terreno cada vez más apremiante y polémico. Con esta nueva ley, las redes sociales como Facebook se verán obligadas a demostrar que necesitan recopilar los datos que

piden y a permitir que los usuarios eliminen cualquier rastro personal de los sitios en los que se registren.

Para bien o para mal, Facebook está provocando una reconfiguración masiva de los límites de la privacidad. A día de hoy si eres amigo de alguien en Facebook, puede que te enteres de más cosas sobre él de las que te ha contado en los últimos diez años de amistad en la vida real.

La cantidad de datos personales que se alojan en Facebook también plantean cuestiones de políticas públicas sobre la privacidad. David Kirkpatrick (2010, p. 240) se pregunta si una empresa puede acumular y controlar tantos datos personales dentro de su infraestructura. La gente quiere estar al mando de su identidad digital. Por muchas promesas que nos haga Facebook sobre cómo tratará nuestros datos, ¿podemos estar seguros de que esos datos se utilizarán de una forma correcta?

La realidad es que en Facebook no hay nada que sea del todo confidencial. Es más, hasta la propia normativa de la empresa lo señala: cualquiera de tus datos personales pueden hacerse públicos. No podemos garantizar que el contenido que cuelgas en tu muro no será visto por personas no autorizadas.

Según Morachimo (2010, p.12) la gran pregunta es si Facebook está cambiando nuestros límites entre lo privado y lo público, imponiéndonos la apertura que conviene a su modelo de negocio, o si somos nosotros los que estamos desarrollando nuevas formas de relación en las que entendemos que estos datos ya son públicos y Facebook simplemente se adapta a esto.

Facebook va a seguir presionando para lograr mayor apertura porque eso conviene a su negocio y dejará de hacerlo cuando sus usuarios empiecen a abandonar su servicio o cuando el sistema legal se lo prohíba. Por eso es importante que, en la situación en la que nos encontramos, los usuarios comprendan a qué estamos renunciando cuando compartimos información en Facebook y pensemos si nos sentimos cómodos con ello.

A continuación ofrecemos una serie de recomendaciones que permitirán que nuestra cuenta de Facebook sea más segura:

- Controlar la información que compartimos: debemos asegurarnos que nuestra configuración no se encuentra en la opción "Recomendada" sino en "Personalizada", puesto que a través de las opciones que nos ofrece, podemos elegir con quién compartimos nuestra información.

- Organizar a nuestros amigos en listas: esta herramienta es parte de las opciones de privacidad en Facebook. Es probable que tengas compañeros de trabajo, amigos íntimos, familiares, conocidos, etc., todos mezclados en la

misma lista. Lo adecuado sería hacer grupos y a partir de ahí definir qué es lo que queremos mostrar a cada grupo.

- Establecer niveles de privacidad en tus álbumes de fotos: es elemental realizar la función anterior con el objetivo de que nuestras fotografías solo puedan verlas quien nosotros queremos.

- Proteger la privacidad de las aplicaciones que instalemos: las aplicaciones de terceros en Facebook (juegos, test y similares) son el principal agujero de seguridad de la red social. Sugerimos la eliminación de todas las aplicaciones que no estén en uso, y revisar cuidadosamente los permisos que ha dado a cada aplicación individualmente. Por ejemplo, algunas aplicaciones pueden publicar en su muro a pesar de que no requieren la opción para funcionar.

- Controlar la función "sitios": a menudo pasa desapercibida, y puede ser muy importante, ya que permite que tus amigos te marquen en lugares. Tener a alguien diciéndole al mundo donde estás en cada momento puede resultar peligroso en algunos casos. Si queremos evitarlo, debemos desactivar esta función.

- Desactivar la opción de búsqueda pública: cuando alguien los busca en un motor de búsqueda, pueden obtener una vista previa de su perfil público que, en algunos casos, puede ser muy revelador. Si no queremos que eso ocurra, debe desactivar esta opción.

Por último, para proteger la privacidad, tenemos que partir del hecho de que es el propio titular de la misma el que tiene que protegerla. Por ello, el usuario de las redes sociales tiene que partir de una correcta configuración de su perfil en la red. Y para que esto parta del propio sujeto, el mismo debe estar concienciado de la problemática existente.

Bibliografía

ACQUISTI, A.; GROSS, R.(2006) Imagined communities: awareness, information sharing, and privacy on the Facebook [en línea]. Proceedings of Privacy Enhancing Technologies Workshop (PET), Lecture Notes in Computer Science , 2006, no. 4258, pp. 36-58. Disponible en: http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf [Consultado el 25/07/2011].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; INTECO (2010). Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online [en línea]. [S.l.] : [s.n.], 2010. Disponible en: http://www.inteco.es/file/vuiNP2GNuMinSjvyZnPW2w [Consultado el 25/07/2011].

AREITO, Javier (2010). Identificación y análisis en torno a la privacidad de la información: amenazas a las redes sociales [en línea]. *Revista Española de electrónica,* Octubre 2010, vol. 671, no. 10, p. 50-67. Disponible en: http://www.redeweb.com/index.php/articulos/19-seguridad-en-redes/755-identificacion-y-analisis-en-torno-a-la-privacidad-de-la-informacion-amenazas-a-las-redes-sociales [Consultado el 25/07/2011]

BARRIUSO RUIZ, Carlos (2009). Las redes sociales y la protección de datos hoy [en línea]. Anuario de la Facultad de Derecho de Alcalá de Henares, 2009, no.2, p. 301-338. ISSN 1888-3214. Disponible en: http://hdl.handle.net/10017/6447 [Consultado el 25/07/2011]

BOYD, Danah; ELLISON, Nicole (2007). Social network sites: definition, history, and scholarship [en línea]. Journal of Computer-Mediated Communication, 2007, vol. *13,* no. 1. Disponible en*:* http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html [Consultado el 25/07/2011]

BOYD, Danah; HARGITTAI, Eszter (2010). Facebook privacy settings: who cares? [en línea]. First Monday, 2010, vol. 15, no. 8. Disponible en: http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589 [Consultado el 25/07/2011]

COLLINS, JC (2010). Fortify your Facebook privacy settings [en línea]. Journal of Accountancy, 2010, vol. 206, no. 6, pp.42-48. Disponible en: http://www.journalofaccountancy.com/Issues/2010/Jun/20102502.htm [Consultado el 25/07/2011].

COMISIÓN EUROPEA (2011). Attitudes on Data Protection and Electronic Identity in the European Union: Special Eurobarometer survey 359 [en línea]. Disponible en: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf [Consultado el 25/07/2011].

COTINO HUESO, Lorenzo (Ed.)(2011). Libertades de expresión e información en Internet y las Redes Sociales: ejercicio, amenazas y garantías [en línea]. Valencia: Servei de Publicacions de la Universitat de Valencia, 2011. 515 p. ISBN 978-84-694-0081-4. Disponible en: http://www.uv.es/cotino/elibertades2010.pdf [Consultado el 25/07/2011]

DEBATIN, Bernhard; LOVEJOY, Jennette P. et al. (2009). Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences [en línea]. Journal of Computer-Mediated Communication , 2009, no. 15, pp. 83–108. Disponible en: http://dx.doi.org/10.1111/j.1083-6101.2009.01494.x [Consultado el 25/07/2011].

DUMORTIER, Franck (2009). Facebook y los riesgos de la "descontextualización" de la información [en línea]. En: Congreso Internet, Derecho y Política (IDP) (5º.2009.Barcelona). IDP. Revista de Internet, Derecho y Política. Barcelona: Universitat oberta de Catalunya, 2009. Pp. 25-41. ISSN 1699-8154. Disponible en: http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_dumortier/n9_dumortier_esp [Consultado el 25/07/2011]

ESCALANTE GONZALBO, Fernando (2008). El derecho a la privacidad [en línea]. 6ª ed. México: Instituto Federal de acceso a la información pública, 2008. 47 p. Cuadernos de transparencia, n. 02. ISBN: 968-5954-08-9. Disponible en: http://www.bibliojuridica.org/libros/libro.htm?l=1798 [Consultado el 25/07/2011]

ESPAÑA. Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. *Boletín Oficial del Estado*, 14 de diciembre de 1999, no. 298, pp. 43088-43099.

ESPAÑA. 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. *Boletín Oficial del Estado*, 19 de enero de 2008, no. 17, pp. 4103-4136.

FAERMAN, Juan (2010). Faceboom: Facebook, el nuevo fenómeno de masas. 1º ed. Barcelona: Alienta, 2010, 124 p. ISBN 978-84-92414-14-7

FERNÁNDEZ BURGUEÑO, Pablo (2009). El Peligro de las Redes Sociales y sus principales consecuencias jurídicas [en línea]. Economist & Jurist, Junio 2009, vol. 131, p.54 -58. Disponible en: http://www.pabloburgueno.com/wp-content/uploads/2009/06/El-peligro-de-las-redes.pdf [Consultado el 25/07/2011]

FERNÁNDEZ, Peter (2009). Balancing outreach and privacy in Facebook: five guiding decision points [en línea]. Library Hi Tech News , 2009, no. 3/4, pp. 10-12. ISSN: 0741-9058 Disponible en: http://dx.doi.org/10.1108/07419050910979946 [Consultado el 25/07/2011].

FLETCHER, Dan (2010). How Facebook Is Redefining Privacy [en línea]. Time Magazine, 2010**.** Disponible en: http://www.time.com/time/magazine/article/0,9171,1990798,00.html [Consultado el 25/07/2011].

FOGEL, Joshua; NEHMAD, Elham (2009). Internet social network communities: Risk taking, trust, and privacy concerns [en línea]. Computers in Human Behavior, 2009, vol.25, no. 1, pp. 153–160. Disponible en: http://dx.doi.org/10.1016/j.chb.2008.08.006 [Consultado el 25/07/2011].

FONG, P.W.L.; ANWAR, M.; ZHAO Z. (2009). A Privacy Preservation Model for Facebook-Style Social Network Systems [en línea]. Lecture Notes in Computer Science, 2009, vol.5789, pp. 303-320. Disponible en : http://dx.doi.org/10.1007/978-3-642-04444-1_19 [Consultado el 25/07/2011].

FUCHS, Christian (2011). An alternative view of privacy on Facebook [en linea]. Information, 2011, no. 2, pp. 140-165. ISSN 2078-2489. Disponible en: http://www.mdpi.com/2078-2489/2/1/140/pdf [Consultado el 25/07/2011].

GRIMMELMAN, James (2008). Facebook and the Social Dynamics of Privacy. [S.l.] : [s.n.], 2008. Disponible en: http://es.scribd.com/doc/9377908/Facebook-and-the-Social-Dynamics-of-Privacy [Consultado el 25/07/2011].

GRIMMELMANN, James (2009). Saving Facebook [en línea]. Iowa Law Review, 2009, no. 94, pp. 1137-1206. Disponible en: http://works.bepress.com/james_grimmelmann/20/ [Consultado el 25/07/2011]

GRUBBS HOY, Mariea; MILNE; George (2010). Gender differences in privacy-related measures for young adult Facebook users [en línea]. Journal of Interactive Advertising, 2010, vol. 10, no. 2, pp. 28-45. ISSN: 1525-1029. Disponible en: http://jiad.org/article130 [Consultado el 25/07/2011]

GRUBBS, Amelia (2011). Privacy Law and the Internet using Facebook.com as a Case Study [en línea]. University of Tennessee Honors Thesis Projects, 2011. 65 p. Disponible en: http://trace.tennessee.edu/cgi/viewcontent.cgi?article=2397&context=utk_chanhonoproj [Consultado el 25/07/2011]

GRUDE, Amy; SCHOLL, Matt; THOMPSON, Robert (2006). Privacy on Facebook [en línea]. SI689 Computer Supported Cooperative Work, 2006, 17 p. Disponible en: http://www.amygrude.com/documents/689.pdf [Consultado el 25/07/2011]

GUICHOT REINA, Emilio (2005). Derecho a la Protección de Datos y Actividad Administrativa. Revista Vasca de Administración Pública, 2005, no.71, pp. 81-120.

GUICHOT REINA, Emilio (2007). Derecho a la privacidad, transparencia y eficacia administrativa: un difícil y necesario equilibrio. Revista catalana de dret públic, 2007, no. 35, pp. 43-74.

HASHEMI, Yasamine (2009). Facebook's privacy policy and its third-party partnerships: lucrativity and liability [en línea]. Boston University Journal of Science & Technology Law, 2009, vol. 15, no. 1, pp. 140- 164. Disponible en: http://www.bu.edu/law/central/jd/organizations/journals/scitech/volume151/documents/Hashemi_WEB.pdf [Consultado el 25/07/2011]

HOADLEY C.M. et al. (2010). Privacy as information access and illusory control: The case of the Facebook News Feed privacy outcry [en línea]. Electronic Commerce Research and Applications, 2010, vol. 9, no. 1, pp. 50-60. ISSN: 1567-4223. Disponible en: http://dx.doi.org/10.1016/j.elerap.2009.05.001 [Consultado el 25/07/2011].

HULL, Gordon; LIPFORD, Heather Richter; LATULIPE, Celine (2009). Contextual gaps: privacy issues on Facebook [en línea]. Ethics and Information Technology, 2010, no. 2009, pp. 1-37. Disponible en: http://dx.doi.org/10.1007/s10676-010-9224-8 [Consultado el 25/07/2011].

KIRKPATRICK, David (2011). El efecto Facebook: la verdadera historia de la empresa que está conectando al mundo. Traducido por Mar Vidal. Barcelona: Gestión 2000, 2011. 443 p. ISBN 978-84-9875-091-1

KRASNOVA, Hanna (2009). Privacy concerns and identity in online social networks [en línea]. Identity in the Information Society , 2009, vol. 2, no. 1, pp. 39-63. Disponible en: http://dx.doi.org/10.1007/s12394-009-0019-1 [Consultado el 25/07/2011].

KRIVAK ,T (2008). Facebook 101: Ten things you need to know about Facebook [en línea]. Information Today, 2008, vol. 25, no. 3, pp. 42-44. Disponible en: http://search.proquest.com/docview/214802296/fulltextPDF?accountid=17252 [Consultado el 25/07/2011].

LÓPEZ JIMÉNEZ, David (2009). La protección de datos personales en el ámbito de las redes sociales electrónicas: el valor de la autorregulación [en línea]. Anuario de la Facultad de Derecho de Alcalá de Henares, 2009, no.2, p. 237-274. ISSN 1888-3214. Disponible en: http://hdl.handle.net/10017/6445 [Consultado el 25/07/2011]

MCKEON, Matt (2010). The Evolution of Privacy on Facebook[en línea]. Disponible en: http://mattmckeon.com/facebook-privacy/ [Consultado el 25/07/2011]

MEZRICH, Ben (2010). Multimillonarios por accidente: el nacimiento de Facebook. Una historia de sexo, dinero, talento y traición. 1º ed. Barcelona: Alienta, 2010. 304 p. ISBN 978-84-92414-20-8

MITJANS PERELLÓ, Esther (2009). Impacto de las redes sociales en el Derecho a la protección de datos personales [en línea]. Anuario de la Facultad de Derecho de Alcalá de Henares, 2009, no.2, p. 107-129. ISSN 1888-3214. Disponible en: http://hdl.handle.net/10017/6439 [Consultado el 25/07/2011]

MONSORIU FLOR, Mar (2009). Manual de Redes Sociales en Internet. 1º ed. Barcelona: Creaciones Copyright, 2009. 250 p. ISBN: 978-84-96300-75-0

MORACHIMO RODRÍGUEZ, Miguel (2011). La privacidad después de Facebook [en línea]. Gaceta Constitucional, 2011, no. 40, pp. 343-355. Disponible en: http://www.blawyer.org/docs/morachimo_privacidad_facebook.pdf [Consultado el 25/07/2011]

OPSAHL, Kurt (2010). A bill of privacy rights for social network users [en línea]. Electronic Frontier foundation, 2010. Disponible en: http://www.eff.org/deeplinks/2010/05/bill-privacy-rights-social-network-users [Consultado el 25/07/2011]

OPSAHL, Kurt (2010). Facebook´s eroding privacy policy: a timeline [en línea]. Electronic Frontier foundation, 2010. Disponible en: https://www.eff.org/deeplinks/2010/04/facebook-timeline [Consultado el 25/07/2011]

PAPADOPOULOS, Marinos; KAPONI, Alexandra (2010). Privacy in the nook of Facebook [en línea]. Disponible en: http://www.marinos.com.gr/bbpdf/pdfs/msg87.pdf [Consultado el 25/07/2011]

PEKÁREK, Martin; PÖTZSCH, Stefanie (2009). A comparison of privacy issues in collaborative workspaces and social networks [en línea]. Identity in the Information Society, 2009, vol. 2, no. 1, pp. 81-93. Disponible en: http://dx.doi.org/10.1007/s12394-009-0016-4 [Consultado el 25/07/2011].

PESET, Fernanda; FERRER-SAPENA, Antonia; BAIGET, Tomàs (2008). "Evolución social y networking en la comunidad biblio-documental". El profesional de la información, 2008, nov.-dic., vol. 17, no. 6, pp. 627-635.

RALLO LOMBARTE, Artemi (2009). La protección de datos en España: análisis de actualidad [en línea]. Anuario de la Facultad de Derecho de Alcalá de Henares, 2009, no.2, p. 15-30. ISSN 1888-3214. Disponible en: http://hdl.handle.net/10017/6431 [Consultado el 25/07/2011]

RALLO LOMBARTE, Artemi; MARTÍNEZ MARTÍNEZ, Ricard (coord.) (2010). Derecho y Redes Sociales. 1º ed. Pamplona: Civitas, 2010. 380 p. ISBN 978-84-470-3462-8

RAYNES-GOLDIE, Kate (2010). Aliases, creeping and wall cleaning: understanding privacy in the age of Facebook [en línea]. First Monday, 2010, vol. 15, no. 1 – 4. Disponible en: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432 [Consultado el 25/07/2011].

ROIG, Antoni (2009). E-privacidad y redes sociales [en línea]. En: Congreso Internet, Derecho y Política (IDP) (5º.2009.Barcelona). IDP. Revista de Internet, Derecho y Política. Barcelona: Universitat oberta de Catalunya, 2009, pp. 42-52. ISSN 1699-8154. Disponible en: http://idp.uoc.edu/ojs/index.php/idp/article/view/n9_roig/n9_roig_esp [Consultado el 25/07/2011]

SÁNCHEZ VIGIL, Juan Miguel; MARCOS RECIO, Juan Carlos; VILLEGAS TOVAR, Ricardo; OLIVERA ZALDUA, María (2009). Aspectos legales y documentales de las redes sociales: el modelo Facebook [en línea]. Ibersid, 2009, p. 187-195. Disponible en: http://www.ibersid.eu/ojs/index.php/ibersid/article/view/3739 [Consultado el 25/07/2011]

STRAND, JL (2011). Facebook: Trademarks, Fan Pages, and Community Pages [en línea]. Intellectual Property and Technology Law Journal, 2011, no. 23, pp. 10-13. Disponible en: http://www.wolfgreenfield.com/files/strand_facebook.pdf [Consultado el 25/07/2011].

TILLY, Charles; WOOD, Lesley J (2010). Los movimientos sociales, 1768-2008: desde sus orígenes a Facebook. Traducido por Ferrán Esteve. 2ª ed. Barcelona: Editorial Crítica, 2010. 366 p. Libros de historia. ISBN 978-84-9892-045-1

VANDER VEER, E.A (2010). Facebook. Traducido por Margarita Fernández. 2ª ed. Madrid: Anaya Multimedia, 2010. 304 p. ISBN 978-84-415-2815-4

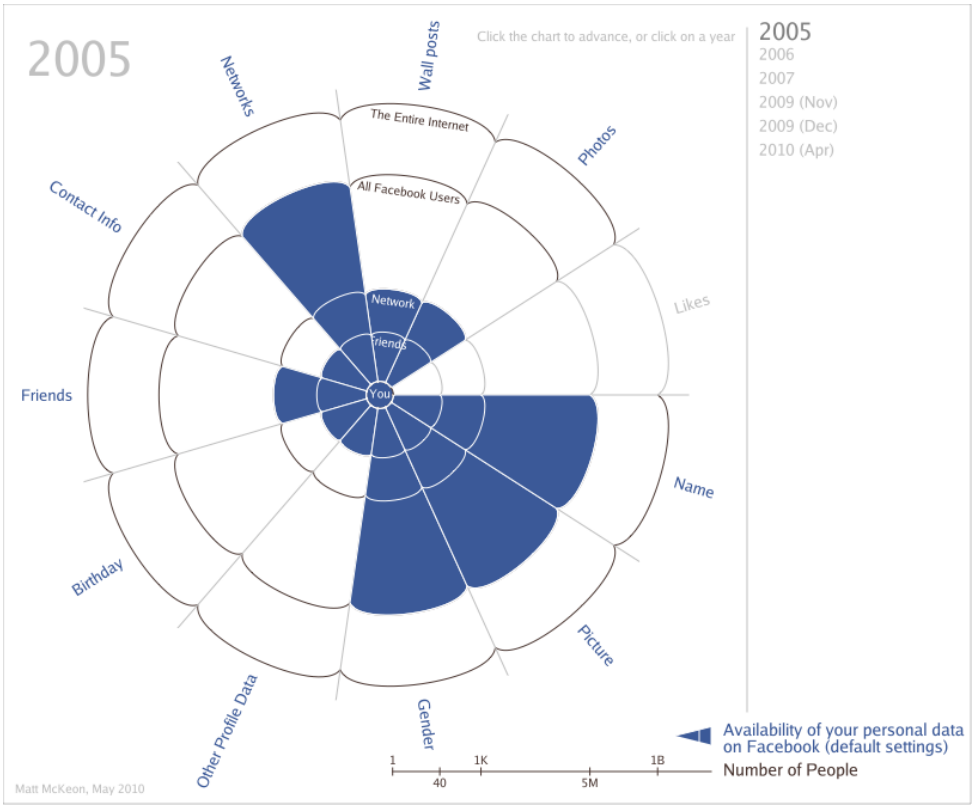
ZIMMER, Michael (2010). **"**But the data is already public": on the ethics of research in Facebook [en línea]**.** Journal Ethics and Information Technology, 2010, vol. 12, no. 4, pp. 313–325. Disponible en: http://dx.doi.org/10.1007/s10676-010-9227-5 [Consultado el 25/07/2011].

ZUCKERBERG, Mark (2010). An open letter from Facebook founder Mark Zuckerberg [en línea]. Facebook Blog, 2010. Disponible en: http://blog.facebook.com/blog.php?post=190423927130 [Consultado el 25/07/2011]

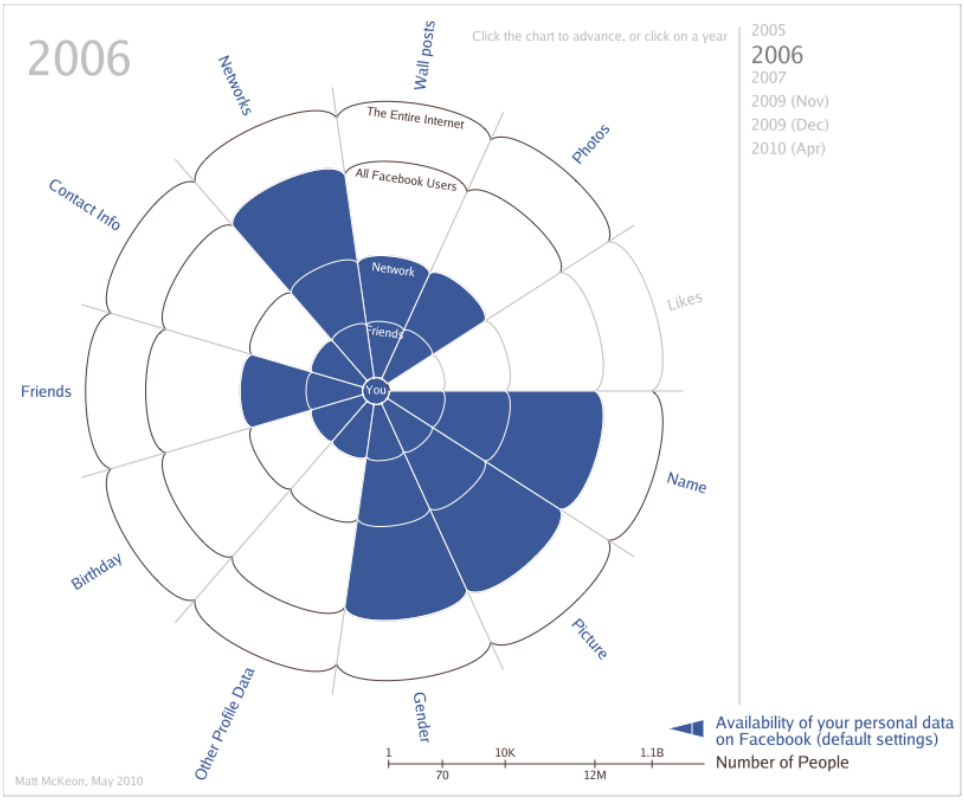
ZUCKERBERG, Mark (2010). Making controls simple, [en línea]. Facebook Blog, 2010. Disponible en: http://blog.facebook.com/blog.php?post=391922327130 [Consultado el 25/07/2011]

Anexos

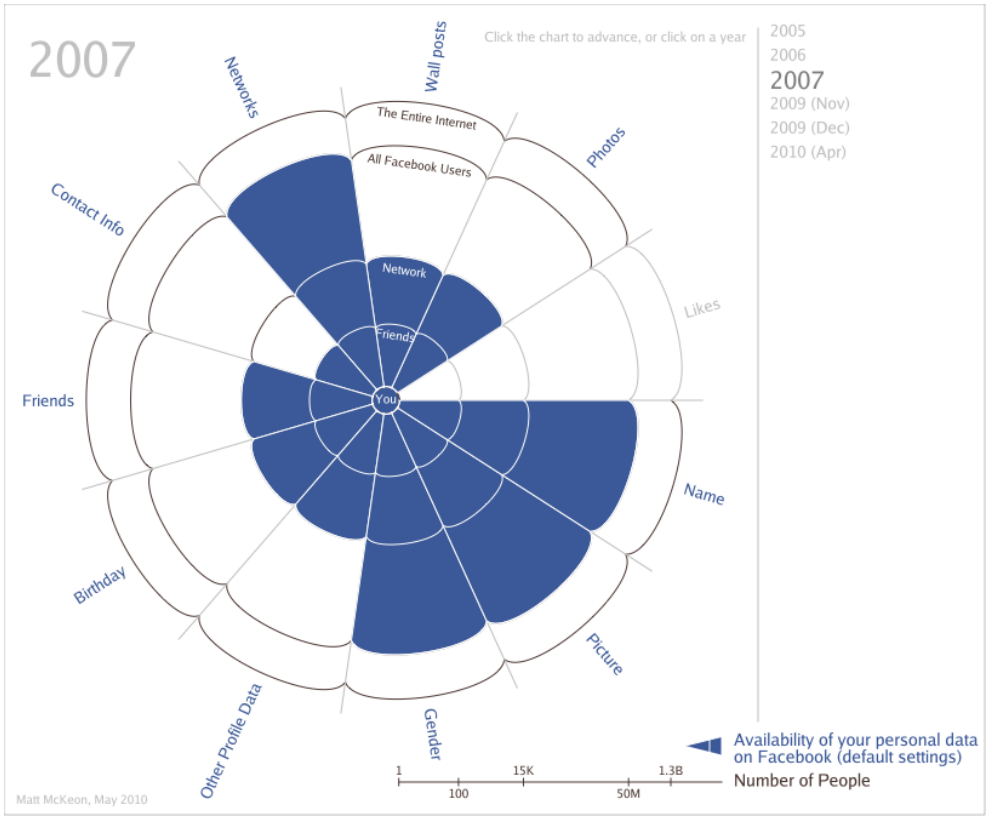
- Privacidad en el año 2005



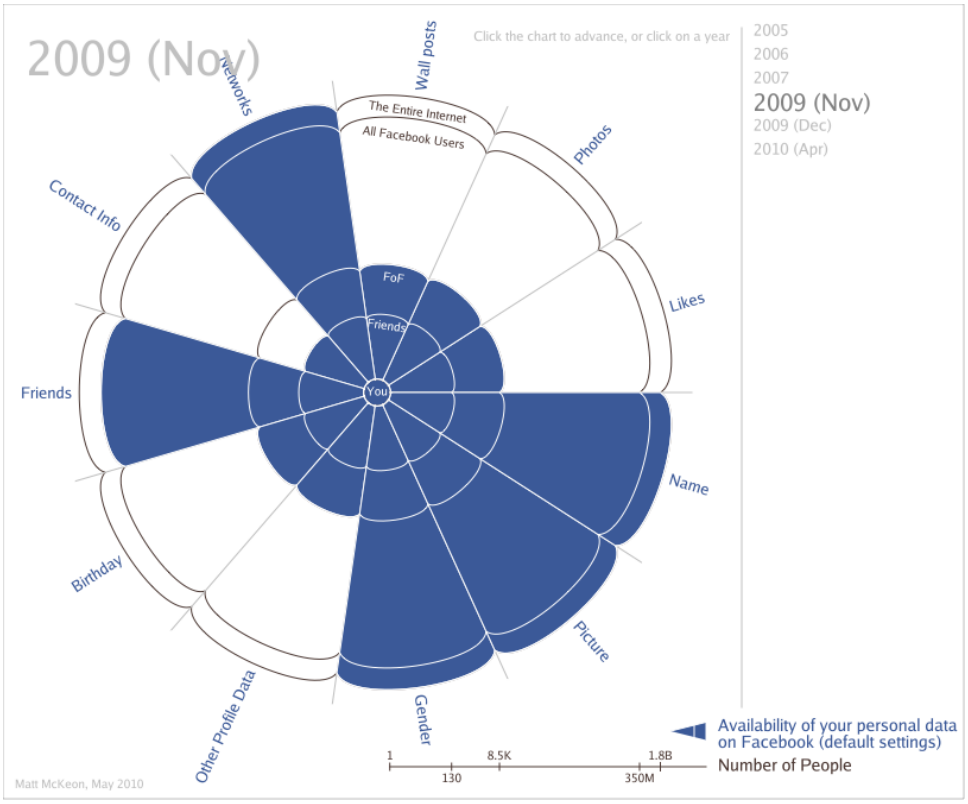
- Privacidad en el año 2006



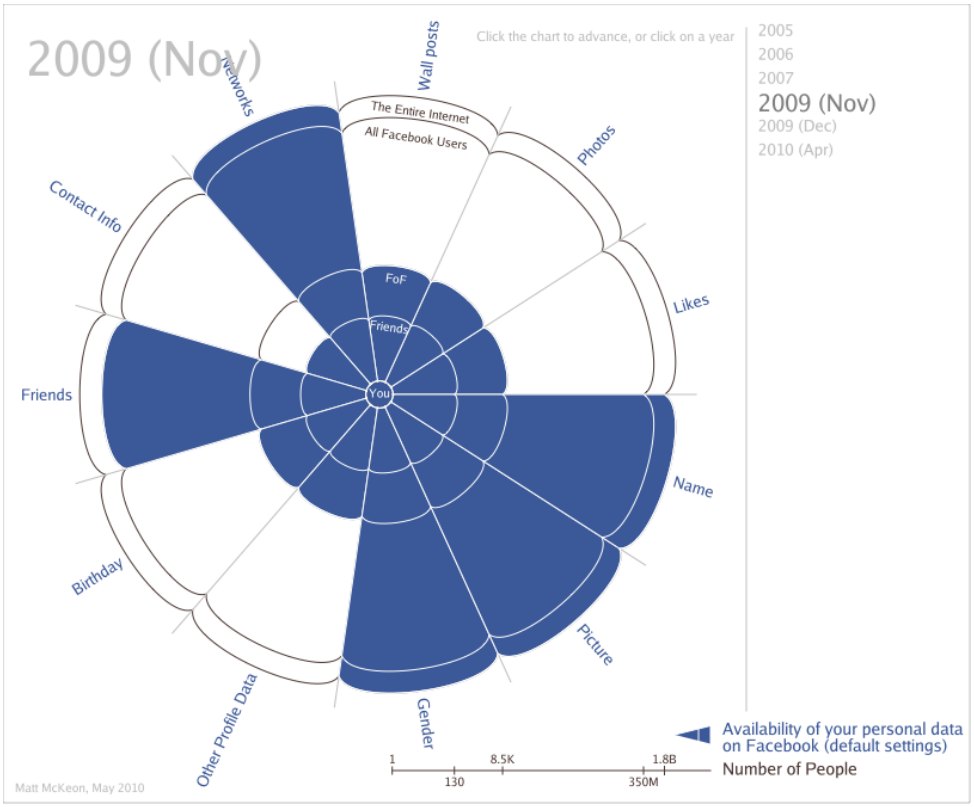
- Privacidad en el año 2007



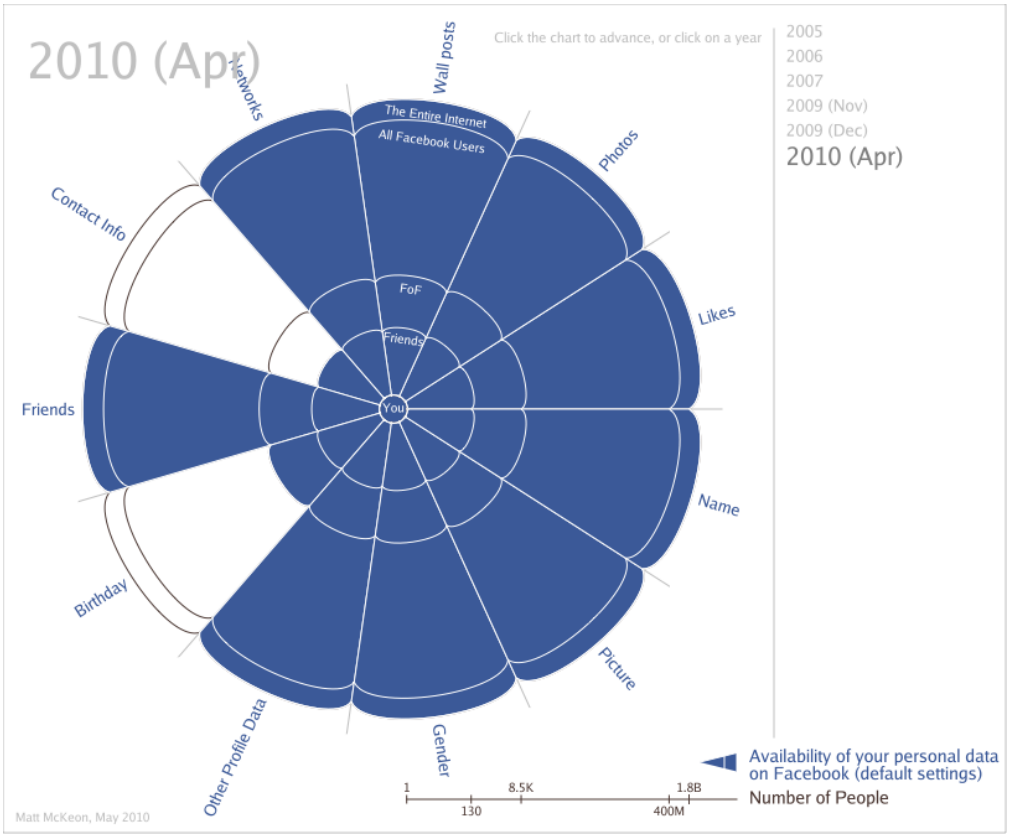
- Privacidad en el año 2009 (Noviembre)



- Privacidad en el año 2009 (Diciembre)



- Privacidad en el año 2010 (Abril)



Política de privacidad de Facebook (2011)

Fecha de la última revisión: 22 de diciembre de 2010.

Este documento consta de nueve secciones, y puedes ir directamente a cada una de ellas seleccionando los enlaces siguientes:

1. Introducción
2. Información que recibimos
3. Compartir información en Facebook.
4. Información que compartes con terceros
5. Cómo utilizamos tu información
6. Cómo compartimos la información
7. Cómo puedes modificar o eliminar información
8. Cómo protegemos la información
9. Otras condiciones

1. **Introducción**

Preguntas. Si tienes alguna pregunta o duda sobre nuestra política de privacidad, ponte en contacto con nuestro equipo de privacidad a través de esta página de ayuda. También puedes contactar con nosotros por correo ordinario en 1601 S. California Avenue, Palo Alto, CA 94304.

Programa TRUSTe. Facebook ha obtenido la certificación TRUSTe Privacy Seal. Esto significa que TRUSTe ha verificado que esta política de privacidad y nuestras prácticas cumplen los requisitos del programa TRUSTe. Si tienes alguna duda o queja sobre nuestra política de privacidad o nuestras prácticas, contáctanos por correo ordinario en la siguiente dirección: 1601 S. California Avenue, Palo Alto, CA 94304 o a través de esta página de ayuda. Si no te satisface nuestra respuesta, puedes ponerte en contacto con TRUSTe aquí. Esta política de privacidad se aplica al sitio web www.facebook.com. El programa TRUSTe sólo incluye la información recopilada a través de este sitio web, y no comprende otros datos, como información que pudiera recopilarse a través de software descargado de Facebook.

Safe Harbor. Facebook también cumple el marco Safe Harbor de la Unión Europea desarrollado por el Departamento de Comercio de Estados Unidos en cuanto a recopilación, uso y retención de datos pertenecientes a la Unión Europea. Como parte de nuestra participación en Safe Harbor, nos comprometemos a resolver todos los posibles conflictos que puedan surgir en relación con nuestras políticas y prácticas a través de TRUSTe. Asimismo, responderemos a las solicitudes de acceso dentro de un plazo de tiempo razonable. Para ver nuestra certificación, entra en el sitio web del programa Safe Harbor del Departamento de Comercio de los Estados Unidos.

Ámbito. La presente política de privacidad incluye Facebook al completo. No obstante, no es aplicable a entidades que no sean propiedad o no se encuentren bajo el control de Facebook, incluidos los sitios web y aplicaciones que utilicen la plataforma. Si utilizas o accedes a Facebook, estarás aceptando las prácticas de privacidad aquí definidas.

No se acepta información de niños menores de 13 años. Si tienes menos de 13 años, no intentes registrarte en Facebook ni nos facilites ningún dato personal. Si descubrimos que hemos recibido información de un niño menor de 13 años, borraremos esa información lo más rápido posible. Si crees que podría obrar en nuestro poder información procedente de un niño menor de 13 años, ponte en contacto con nosotros a través de esta página de ayuda.

Participación de los padres. Recomendamos encarecidamente que los menores de edad, a partir de los 13 años, pidan permiso a sus padres antes de enviar información sobre sí mismos a través de internet, y animamos a los padres a que enseñen a sus hijos prácticas seguras para el uso de internet. Encontrarás material de ayuda acerca de cómo los padres pueden hablar con sus hijos sobre un uso seguro de internet en esta página de ayuda.

2. Información que recibimos

Información que nos envías:

Información sobre ti. Cuando te registras en Facebook, nos facilitas tu nombre, correo electrónico, sexo y fecha de nacimiento. Durante el proceso de registro, te ofrecemos la posibilidad de conectarte a tus amigos, centros educativos y empleados. También podrás añadir una foto. En algunos casos podríamos pedirte información adicional por motivos de seguridad o para ofrecerte servicios específicos. Una vez registrado puedes proporcionar otra información sobre ti relacionada, por ejemplo, con tu ciudad de residencia, ciudad de origen, familia, relaciones, redes, actividades, intereses y lugares. También puedes indicar tu ideología política o tus creencias religiosas.

Contenido. Una de las finalidades principales del uso de Facebook es compartir contenido con los demás, por ejemplo, actualizar tu estado, cargar o hacer una foto, cargar o grabar un vídeo, compartir un enlace, crear un evento o un grupo, hacer un comentario, escribir algo en el muro de alguien, escribir una nota o enviar un mensaje. Si no deseas que guardemos los metadatos asociados al contenido que compartes en Facebook (como las fotografías) elimina los metadatos antes de cargar el contenido.

Información sobre transacciones. Podemos guardar los datos de las transacciones o pagos que realices a través de Facebook. Si no deseas que almacenemos el número de cuenta de origen de tu pago, puedes eliminarlo a través de la página de pagos.

Información sobre amigos. Te ofrecemos herramientas de importación de contactos para ayudarte a cargar las direcciones de tus amigos para que puedas encontrarlos en Facebook e invitar a unirse a aquellos contactos que todavía no usen Facebook. Si no deseas que almacenemos esta información, entra en esta página de ayuda. Si nos das tu contraseña para obtener estos contactos, no la guardaremos una vez cargada la información de los contactos.

Información que recopilamos cuando interactúas con Facebook:

Información sobre la actividad en el sitio web. Realizamos un seguimiento de las acciones que llevas a cabo en Facebook, como añadir conexiones (incluido unirte a un grupo o añadir un amigo), crear un álbum de fotos, enviar un regalo, dar un toque a otro usuario, indicar que "te gusta" una publicación, asistir a un evento o conectarte a una aplicación. En algunos casos, también estás llevando a cabo una acción cuando nos proporcionas información o contenido. Por ejemplo, si compartes un vídeo, además de almacenar el contenido real que has actualizado, podemos registrar el hecho de que lo hayas compartido.

Acceso a la información del dispositivo y del navegador. Cuando accedes a Facebook desde un ordenador, teléfono móvil u otro dispositivo, podemos obtener información de dicho dispositivo sobre tu tipo de navegador, ubicación y dirección IP, así como las páginas que visitas.

Información sobre cookies. Utilizamos "cookies" (datos que almacenamos en tu ordenador, teléfono móvil u otro dispositivo durante un período de tiempo prolongado) para que Facebook sea más fácil de usar, para que nuestra publicidad sea mejor y para proteger tanto a ti como a Facebook. Por ejemplo, las empleamos para guardar tu nombre de usuario (pero nunca tu contraseña) de modo que te resulte más sencillo iniciar sesión cada vez que quieras entrar en Facebook. También utilizamos las cookies para confirmar que estás conectado a Facebook, y para saber cuándo estás interactuando con aplicaciones y sitios web de la plataforma Facebook, nuestros widgets, botones de compartir y nuestros anuncios. Puedes eliminar o bloquear las cookies mediante la configuración de tu navegador, pero en algunos casos puede influir en tu capacidad de uso de Facebook.

Información que recibimos de terceros:

Plataforma de Facebook. No poseemos ni operamos las aplicaciones o sitios web que utilizas a través de la plataforma de Facebook (como juegos y otros programas). Cuando te conectes a un sitio web o una aplicación de la plataforma, nos suministrarán información, incluida la información acerca de las acciones que realizas. En algunos casos, es posible que recibamos una cantidad limitada de información antes de que te conectes a la aplicación o sitio web para poder personalizar el proceso de conexión.

Información procedente de otros sitios web. Podemos establecer programas con socios publicitarios y otros sitios web en los que éstos comparten información con nosotros:

Podemos solicitar a los anunciantes que nos indiquen cómo nuestros usuarios han respondido a los anuncios que les mostramos (y, con fines comparativos, cómo han actuado en su página otros usuarios que no habían visto los anuncios). Esta compartición de datos, denominada comúnmente "seguimiento de conversión" nos ayuda a medir la efectividad de nuestra publicidad y a mejorar la calidad de los anuncios que ves.

Podemos recibir información sobre si has visto o no, o si has interactuado con determinados anuncios de otros sitios, para medir la efectividad de dichos anuncios.

Si en cualquiera de estos casos recibimos datos que todavía no tenemos, les otorgaremos el carácter de "anónimos" en un plazo de 180 días, lo cual significa que no asociaremos la información con ningún usuario en particular. Si establecemos dichos programas, sólo haremos uso de la información según se explica en la sección "Cómo utilizamos tu información" expuesta a continuación.

Información procedente de otros usuarios. Podemos recopilar información acerca de ti a partir de otros usuarios de Facebook (como cuando un amigo te etiqueta en una foto, un vídeo o un lugar, proporciona detalles de vuestra amistad o indica su relación contigo).

3. Compartir información en Facebook

En esta sección se explica cómo funciona la configuración de la privacidad , y cómo se comparte tu información en Facebook. Antes de compartir información en Facebook debes tener en cuenta tu configuración de la privacidad.

Nombre y foto del perfil. Facebook ha sido diseñado para que te resulte sencillo encontrar y conectarte a otros. Por este motivo, tu nombre y la foto de tu perfil carecen de configuración de privacidad. Si no quieres compartir la foto de tu perfil, debes eliminarla (o no añadir ninguna). También puedes controlar quién puede encontrarte al buscar en Facebook o en motores de búsqueda públicos utilizando la configuración de la privacidad de las aplicaciones y los sitios web.

Información de contacto. La configuración de tu información de contacto (disponible en la configuración de la privacidad) controla quién puede ponerse en contacto contigo en Facebook y quién puede ver tu información de contacto (por ejemplo, tu dirección de correo electrónico y número de teléfono). Recuerda que esta información no es obligatoria (excepto la dirección de correo electrónico) y que no tienes por qué compartir tu dirección de correo electrónico con nadie.

Información personal La configuración de tu información personal controla quién puede ver tu información personal (por ejemplo, tus tendencias políticas y creencias religiosas) si decides añadirla. Recomendamos compartir esta información utilizando la opción "amigos de amigos".

Mis publicaciones. Puedes seleccionar una configuración de privacidad para cada publicación que realices usando el editor de nuestro sitio. Tanto si vas a cargar una foto como a publicar una actualización de estado, puedes controlar exactamente quién puede verla en el momento de crearla. Cada vez que compartas algo, busca el icono del candado. Si haces clic en el candado se mostrará un menú que te permite elegir quién podrá ver tu publicación. Si decides no seleccionar tu configuración en el momento de publicar el contenido, dicho contenido se compartirá en consonancia con la configuración de "Mis publicaciones" (disponible en la configuración de la privacidad).

Sexo y fecha de nacimiento. Además del nombre y la dirección de correo electrónico, requerimos que nos facilites tu sexo y fecha de nacimiento durante el proceso de registro. Te pedimos la fecha de nacimiento para comprobar que eres mayor de 13 años y, así, poder limitar mejor el acceso a contenidos y anuncios que no sean adecuados para ciertas edades. Puesto que tu fecha de nacimiento y sexo son obligatorios, no puedes eliminarlos. Sin embargo, puedes editar tu perfil para ocultar todo (o parte) de dichos campos para que no los vean otros usuarios.

Otros. Otras indicaciones que debes recordar:

Parte del contenido que compartes y de las acciones que llevas a cabo se mostrarán en las páginas de inicio de tus amigos y en otras páginas que visiten.

Si otro usuario te etiqueta en una foto, vídeo o lugar, puedes eliminar la etiqueta. También puedes limitar quién puede ver que has sido etiquetado en tu perfil desde la configuración de la privacidad.

Incluso tras haber eliminado la información de tu perfil o tras haber borrado tu cuenta, es posible que alguna copia de dicha información permanezca visible en algún otro lugar si ha sido compartida con otros, ha sido distribuida de algún otro modo según tu configuración de la privacidad o ha sido copiada o almacenada por otros usuarios.

Debes entender que la información puede ser compartida a su vez o copiada por otros usuarios.

Algunos tipos de comunicaciones que envías a otros usuarios no pueden eliminarse, como por ejemplo los mensajes.

Cuando publicas información en el perfil de otro usuario o realizas un comentario en la publicación de otro usuario, dicha información queda sujeta a la configuración de la privacidad del otro usuario.

Si utilizas una fuente externa para publicar información en Facebook (como una aplicación móvil o un sitio web de Connect) debes comprobar la configuración de privacidad de dicha publicación, puesto que la establece la fuente externa.

Información de “Todos”. La información configurada como “todos” está disponible públicamente, como tu nombre, foto de perfil y conexiones. Dicha información permanece accesible y visible para todo aquel que entre en internet (incluidas las personas no registradas en Facebook), queda sujeta a indexación por parte de motores de búsqueda de terceros y puede ser importada, exportada, distribuida y redistribuida por nosotros y otros sin limitaciones de privacidad. Dicha información puede asociarse contigo, incluido tu nombre y fotografía de perfil, incluso fuera de Facebook, por ejemplo, en motores de búsqueda públicos y cuando visites otros sitios de Internet. La configuración de privacidad predeterminada para ciertos tipos de información que publicas en Facebook está establecida en “todos”. Puedes revisar y modificar la configuración predeterminada en tu configuración de la privacidad. Si eliminas el contenido compartido con "todos" previamente publicado en Facebook, lo borraremos de tu perfil de Facebook, pero no podemos controlar su uso fuera de Facebook.

Menores. Nos reservamos el derecho de aplicar métodos de protección especial para menores (como proporcionarles un contenido adecuado a su edad) y aplicar restricciones a la capacidad que tienen los adultos para compartir y conectarse a menores, reconociendo que esto puede suponer para los menores una experiencia más limitada en Facebook.

4. Información que compartes con terceros

Plataforma de Facebook. Como ya hemos mencionado, no operamos los sitios web y aplicaciones que utilizan la plataforma de Facebook ni somos sus propietarios. Esto significa que al utilizar estas aplicaciones y sitios web, tu información de Facebook no está sólo disponible para Facebook. Antes de permitir el acceso a cualquier información sobre ti, les requerimos que acepten una serie de condiciones que limitan su uso de tu información (puedes consultar estas condiciones en la sección 9 de nuestra Declaración de derechos y responsabilidades) y ponemos en práctica medidas técnicas para garantizar que sólo obtienen información autorizada. Para obtener más información sobre la plataforma, visita la página Acerca de la plataforma.

Conexión a una aplicación o sitio web. Cuando te conectas a una aplicación o sitio web, éstos tendrán acceso a Información general sobre ti. El término Información general incluye tu nombre y los nombres de tus amigos, fotografías de perfil, sexo, identificador de usuario, conexiones y cualquier contenido compartido usando la configuración de privacidad “Todos”. Para ayudar a estos sitios web y aplicaciones a poner en práctica medidas de seguridad y controlar la distribución de contenido apropiado a usuarios de diferentes edades, podemos poner a su disposición otra información, como datos técnicos, la localización de tu equipo informático o dispositivo de acceso, así como tu edad. Asimismo, las aplicaciones o sitios web que aceptan créditos pueden acceder a tu saldo de créditos. Si la aplicación o el sitio web desea acceder a otros datos, tendrá que pedirte permiso.

Te proporcionamos herramientas para controlar cómo compartes tu información con aplicaciones y sitios web que utilizan la plataforma. Por ejemplo, puedes bloquear

completamente el acceso a tus datos de todos los sitios web y aplicaciones, o bien bloquear aplicaciones específicas en la configuración de la privacidad de las aplicaciones y los sitios web, o en la página "Acerca de" de la aplicación. También puedes utilizar tu configuración de la privacidad para limitar qué parte de tu información está disponible para “todos”.

Aconsejamos que leas siempre las políticas de los sitios web y las aplicaciones de terceros para cerciorarte de que estás de acuerdo con el modo en el que usan la información que compartes con ellos. Facebook no puede garantizar que estos sitios web o aplicaciones cumplirán nuestras normas. Si encuentras alguna aplicación o sitio web que infringe nuestras normas, infórmanos de este incumplimiento en esta página de ayuda y tomaremos las medidas oportunas.

Cuando tus amigos utilizan la plataforma. Si tu amigo se conecta a una aplicación o sitio web, éstos podrán acceder a tu nombre, fotografía del perfil, sexo, ID de usuario y aquella información que hayas compartido con "todos". También podrán acceder a tus conexiones, pero no podrán acceder a tu lista de amigos. Si ya te has conectado a ese sitio web o aplicación (o dispones de otra cuenta en estos lugares), es posible que éstos también puedan conectarse con tu amigo a través de ese sitio web o aplicación. Si la aplicación o el sitio web desean acceder a cualquier otro contenido o información tuya (incluida tu lista de amigos), tendrá que obtener permiso específico de tu amigo. Si tu amigo concede permiso a la aplicación o al sitio web, sólo podrán acceder a contenido e información sobre ti a la que tu amigo pueda acceder. Además, sólo podrán utilizar dicho contenido y dicha información en conexión con ese amigo. Por ejemplo, si un amigo facilita a una aplicación acceso a una fotografía que sólo compartes con tus amigos, dicha aplicación puede permitir a tu amigo ver o imprimir la fotografía, pero no puede mostrársela a nadie más.

Te proporcionamos una serie de herramientas para controlar cómo se comparte tu información cuando tu amigo se conecta a una aplicación o sitio web. Por ejemplo, puedes utilizar la configuración de privacidad de tus aplicaciones y sitios web para limitar qué información pueden poner tus amigos a disposición de las aplicaciones y los sitios web. Puedes bloquear el acceso a tu información de todas las aplicaciones y sitios web de la plataforma, o de aplicaciones o sitios web concretos. Puedes utilizar tu configuración de la privacidad para limitar los amigos que pueden acceder a tu información o limitar qué parte de tu información está disponible para "todos". También puedes desconectarte de un amigo si no estás de acuerdo con el modo en que utiliza tu información.

Sitios web y aplicaciones de terceros aprobados previamente. Para proporcionarte experiencias sociales útiles fuera de Facebook, en ocasiones necesitamos proporcionar Información general sobre ti a sitios web y aplicaciones de terceros aprobados previamente que utilizan la plataforma cuando los visitas (si aún tienes una sesión iniciada en Facebook). Del mismo modo, cuando uno de tus amigos visita un sitio web o aplicación aprobados previamente, recibirá información general sobre ti para que podáis conectaros también a través de ese sitio web (si también dispones de una cuenta en dicho sitio web). En estos casos, requerimos que estos sitios web y estas aplicaciones se sometan a un proceso de aprobación y participen en diferentes acuerdos con el objetivo de proteger tu privacidad. Por ejemplo, estos acuerdos

incluyen disposiciones relativas al acceso y eliminación de tu Información general, así como la posibilidad de rechazar la participación en la experiencia ofrecida. Puedes inhabilitar la personalización instantánea de todos los sitios web y aplicaciones aprobados previamente mediante la configuración de la privacidadde las aplicaciones y los sitios web. También puedes bloquear un sitio web o una aplicación que han recibido autorización previa haciendo clic en "No, gracias", que verás en la barra de color azul de la aplicación o sitio web concreto. Además, si cierras la sesión de Facebook antes de visitar un sitio web o aplicación aprobados previamente, éstos no podrán acceder a tu información.

Exportación de información. Puedes (al igual que todos aquellos a cuya disposición has puesto tu información) utilizar herramientas como fuentes RSS, aplicaciones de libretas de direcciones del teléfono móvil o funciones de copiar y pegar, para obtener y exportar (y en algunos casos, importar) información de Facebook, incluida tu propia información y todos los datos sobre tu persona. Por ejemplo, si compartes tu número de teléfono con tus amigos, éstos pueden utilizar aplicaciones de terceros para sincronizar dicha información con la libreta de direcciones de sus teléfonos móviles.

Publicidad. En ocasiones, los anunciantes que presentan publicidad en Facebook emplean métodos tecnológicos para medir la efectividad de sus anuncios y personalizar el contenido publicitario. Puedes renunciar a la fijación de cookies de numerosos anunciantes haciendo clic aquí. También puedes usar la configuración de cookies de tu navegador para limitar o evitar la fijación de cookies por parte de redes publicitarias. Facebook no comparte con los anunciantes información que te identifica personalmente salvo si obtenemos tu autorización.

Enlaces. Al hacer clic en algunos enlaces de Facebook, es posible que te lleven fuera de nuestro sitio web. No nos hacemos responsables de las políticas de privacidad de otros sitios web, y te animamos a que leas sus normas de privacidad.

5. Cómo utilizamos tu información

Utilizamos la información que recopilamos para tratar de ofrecerte una experiencia segura, eficaz y personalizada. A continuación, incluimos algunos datos sobre cómo lo hacemos:

Para gestionar el servicio. Utilizamos la información que recopilamos para ofrecerte nuestros servicios y funciones, evaluarlos y mejorarlos y prestarte servicio técnico. Empleamos la información para impedir actividades que podrían ser ilegales y para aplicar nuestra Declaración de derechos y responsabilidades. También utilizamos una serie de sistemas tecnológicos para detectar y ocuparnos de actividades y contenido en pantalla anómalos con el fin de evitar abusos como el correo basura. Estos esfuerzos pueden provocar, en ocasiones, el fin o la suspensión temporal o permanente de algunas funciones para algunos usuarios.

Para ponernos en contacto contigo. Ocasionalmente, podemos ponernos en contacto contigo para informarte de anuncios relativos a servicios. Puedes optar por no recibir ninguna comunicación salvo actualizaciones esenciales en la página de notificaciones de la cuenta. En los mensajes de correo electrónico que te enviemos, podemos incluir contenido que veas en Facebook.

Para ofrecerte anuncios personalizados. No compartimos información tuya con anunciantes sin tu consentimiento. (Un ejemplo de consentimiento sería que nos pidieses que suministrásemos tu dirección de envío a un anunciante para recibir una muestra gratuita.) Permitimos a los anunciantes elegir las características de los usuarios que verán sus anuncios y podemos utilizar cualquiera de los atributos que hayamos recabado que no te identifiquen personalmente (como información que puedas haber decidido no mostrar a otros usuarios, por ejemplo, el año de nacimiento) para seleccionar el público apropiado para dichos anuncios. Por ejemplo, podríamos utilizar tu interés por el fútbol para mostrarte anuncios de equipamiento de fútbol, pero no le decimos a la empresa que vende el equipamiento quién eres. Puedes consultar los criterios que pueden seleccionar los anunciantes visitando nuestra página de publicidad. Aunque no compartimos tu información con anunciantes sin tu consentimiento, cuando hagas clic en un anuncio o interactúes de otro modo con éste, existe la posibilidad de que el anunciante pueda colocar una cookie en tu navegador y tomar nota de que cumple los criterios que ha seleccionado.

Para ofrecer anuncios sociales. En ocasiones, emparejamos los anuncios que ofrecemos con información pertinente que poseemos sobre ti y sobre tus amigos para que los anuncios resulten más interesantes y se adapten mejor a ti y a tus amigos. Por ejemplo, si te conectas a la página de tu grupo de música favorito, podemos mostrar tu nombre y la foto de tu perfil al lado de un anuncio de dicha página que verán tus amigos. Sólo compartimos la información personal visible en el anuncio social con el amigo que puede ver el anuncio. Puedes optar por que tu información no sea utilizada en anuncios sociales en esta página de ayuda.

Para complementar tu perfil. Podemos utilizar información acerca de ti que recabemos de otros usuarios de Facebook para completar tu perfil (por ejemplo, cuando se te etiqueta en una foto o se te menciona en una actualización de estado). En tales casos, generalmente te permitimos eliminar el contenido (por ejemplo, permitiéndote eliminar la etiqueta de una foto tuya) o limitar la visibilidad de tu perfil.

Para hacer sugerencias. Utilizamos tu información, incluidas las direcciones que importas a través de las herramientas de importación de contactos, para hacerte sugerencias a ti y a otros usuarios de Facebook. Por ejemplo, si otro usuario importa la misma dirección de correo electrónico que tú, podemos sugeriros a ambos que añadáis al otro a vuestra lista de amigos. También, si un amigo tuyo carga una foto en la que apareces, podemos sugerirle que te etiquete en ella. Para hacer esto, comparamos las fotos de tu amigo con información recopilada de las fotos en las que se te ha etiquetado. También podemos sugerirte que uses herramientas o funciones concretas, según lo que utilicen tus amigos. Para controlar si podemos sugerir o no a otro usuario que te añada como amigo, ve a la opción "Buscarte en Facebook" de tu configuración de privacidad. También puedes controlar si sugerimos o no a otros

usuarios que te etiqueten en una foto haciendo clic en "Personalizar la configuración" en la página de configuración de la privacidad.

Para ayudar a tus amigos a encontrarte. Permitimos a otros usuarios utilizar información de contacto que tengan sobre ti (como tu dirección de correo electrónico) para encontrarte, incluso a través de herramientas de importación y búsqueda de contactos. Puedes impedir que otros usuarios utilicen tu dirección de correo electrónico para encontrarte en la sección de búsquedas de tu configuración de la privacidad.

Software descargable. Algunas aplicaciones de software descargables y applets que ofrecemos, como las barras de herramientas del navegador y las herramientas para cargar fotos, nos transmiten datos. Podemos no realizar ninguna declaración formal si creemos que la recopilación y uso de información por nuestra parte es el fin obvio de la aplicación, por ejemplo, el hecho de recibir fotografías cuando se utiliza la herramienta para cargar fotos. Si creemos que no resulta obvio que estemos recopilando o utilizando dicha información, te avisaremos la primera vez que nos facilites la información, de tal manera que puedas decidir si deseas utilizar esa función.

Cuentas in memoriam. Si se nos notifica que un usuario ha fallecido, podemos convertir su cuenta en una cuenta conmemorativa. En tales casos, restringimos el acceso al perfil a los amigos confirmados y permitimos a éstos y a los familiares que escriban en el muro del usuario en recuerdo suyo. Podemos cerrar una cuenta si recibimos una solicitud formal de un pariente del usuario u otra solicitud legal pertinente para hacerlo.

6. Cómo compartimos la información

Facebook se basa en compartir información con otros (amigos y personas de tu entorno) al tiempo que se te ofrece una configuración de la privacidadque puedes utilizar para restringir el acceso de otros usuarios a tu información.. Compartimos tu información con terceros cuando creemos que dicha acción está permitida por ti, que es razonablemente necesaria para ofrecer nuestros servicios o cuando se nos exige legalmente que lo hagamos. Por ejemplo:

Cuando realizas un pago. Cuando realices transacciones con otras personas o efectúes pagos en Facebook, sólo compartiremos la información de la transacción con los terceros que sean necesarios para completar la transacción. Requeriremos que los terceros acuerden respetar la privacidad de la información.

Cuando invitas a un amigo a que se una a Facebook. Cuando nos pides que invitemos a un amigo a que se una a Facebook, le enviaremos un mensaje de tu parte, usando tu nombre. La invitación también puede contener información sobre otros usuarios que tu amigo pueda conocer. También le enviamos hasta dos recordatorios en tu nombre. Puedes ver quién ha aceptado tus invitaciones, enviar recordatorios y eliminar las

direcciones de correo electrónico de tus amigos en la página del historial de invitaciones. Si tu amigo no quiere que conservemos su información, la eliminaremos a petición suya en esta página de ayuda.

Cuando eliges compartir tu información con comerciantes. Puedes elegir compartir información con comerciantes o proveedores de comercio electrónico no asociados con Facebook a través de ofertas en el sitio web. Esto será a tu entera discreción y no le suministraremos información tuya a dichos comerciantes sin tu consentimiento.

Para ayudar a tus amigos a encontrarte. De forma predeterminada, incluimos cierta información que has colocado en tu perfil en los resultados de búsqueda de Facebook para ayudar a tus amigos a encontrarte. Sin embargo, puedes controlar quién puede ver alguna de esta información, así como quién puede encontrarte en búsquedas, a través de la configuración de la privacidad. También colaboramos con proveedores de mensajería instantánea y correo electrónico para ayudar a sus usuarios a identificar cuáles de sus contactos son usuarios de Facebook, de forma que podamos promocionar Facebook a dichos usuarios.

Para dar a los motores de búsqueda acceso a información públicamente disponible. En general, restringimos el acceso de los motores de búsqueda a nuestro sitio web. Podemos permitirles acceder a información configurada con la opción "todos" (junto con tu nombre y fotografía de perfil) y a la información de tu perfil que sea visible para todos. Puedes cambiar la visibilidad de parte de la información de tu perfil en la sección de personalización de la configuración de la privacidad. También puedes impedir que los motores de búsqueda sometan a indexado tu perfil en la configuración de la privacidad de las aplicaciones y los sitios web.

Para ayudar a mejorar o promocionar nuestro servicio. A veces compartimos datos agregados o anónimos con terceros para ayudar a mejorar o promocionar nuestro servicio. Sin embargo, sólo lo hacemos de tal manera que no se pueda identificar a ningún usuario en particular ni vincularse a éste con ninguna información o acción específica.

Para prestarte servicios. Podemos ofrecer información a proveedores de servicios que nos ayudan a facilitarte los servicios que ofrecemos. Por ejemplo, podemos utilizar a terceros para alojar nuestro sitio web, enviar actualizaciones por correo electrónico acerca de Facebook, eliminar información repetitiva de nuestras listas de usuarios, procesar pagos u ofrecer enlaces o resultados de búsqueda (lo que incluye enlaces promocionados). Estos proveedores de servicios pueden tener acceso a tu información personal para utilizarla durante un período de tiempo limitado, pero cuando esto ocurre, implantamos sistemas de protección técnicos y contractuales razonables para restringir su uso de dicha información a la ayuda que nos prestan para ofrecer el servicio.

Para publicitar nuestros servicios. Podemos pedir a anunciantes ajenos a Facebook que muestren anuncios para promocionar nuestros servicios. Podemos pedirles que

entreguen dichos anuncios basándose en la presencia de una cookie, pero al hacerlo, no se compartirá ninguna otra información con el anunciante.

Para ofrecer servicios conjuntos. Podemos prestar servicios de forma conjunta con otras empresas, como se el caso del servicio de clasificados del Marketplace de Facebook. Si utilizas estos servicios, podemos compartir tu información para facilitar dicho servicio. Sin embargo, identificaremos al socio y te presentaremos la política de privacidad del proveedor de servicios conjuntos antes de que utilices dicho servicio.

Para responder a requerimientos legales y evitar daños. Podemos revelar información con arreglo a citaciones, órdenes judiciales u otros requerimientos (incluidos asuntos civiles y penales) si creemos de buena fe que la ley exige dicha respuesta. Esto puede incluir respetar requerimientos de jurisdicciones ajenas a los Estados Unidos cuando creamos de buena fe que las leyes locales de tal jurisdicción exigen dicha respuesta, son aplicables a usuarios de dichas jurisdicción y resultan coherentes con estándares internacionales generalmente aceptados. También podemos compartir información si creemos de buena fe que resulta necesario para impedir un fraude u otra actividad ilegal, evitar un daño físico inminente o protegernos tanto a nosotros como al usuario de personas que infrinjan nuestra Declaración de derechos y responsabilidades. Esto puede incluir compartir información con otras empresas, abogados, tribunales u otras entidades gubernamentales.

Transferencia en caso de venta o cambio de control. If the ownership of all or substantially all of our business changes, we may transfer your information to the new owner so that the service can continue to operate. En tal caso, tu información seguiría estando sujeta a las promesas efectuadas en la Política de privacidad preexistente.

7. Cómo puedes cambiar eliminar información

Edición de tu perfil. Puedes cambiar o eliminar la información de tu perfil en cualquier momento yendo a la página de tu perfil y haciendo clic en “Editar mi perfil”. La información se actualizará de inmediato.

Eliminar los contactos cargados. Si utilizas nuestra herramienta para importar contactos con el fin de cargar direcciones, después puedes eliminar la lista en esta página de ayuda. Puedes eliminar las direcciones de correo electrónico de amigos que hayas invitado a unirse a Facebook en tu página del historial de invitaciones.

Desactivación o eliminación de la cuenta. Si quieres dejar de utilizar tu cuenta, puedes desactivarla o eliminarla. Cuando desactivas una cuenta, ningún usuario podrá verla, pero no será eliminada. Guardamos la información de tu perfil (conexiones, fotos, intereses, etc.) por si más tarde decides volver a activarla. Muchos usuarios desactivan sus cuentas por motivos temporales y al hacerlo, nos piden que mantengamos su información hasta que vuelvan a Facebook. Seguirás pudiendo reactivar la cuenta y restaurar tu perfil en su totalidad. Cuando eliminas una cuenta, se

borra de forma permanente. Sólo deberías eliminar tu cuenta si estás seguro de que nunca querrás reactivarla. Puedes desactivar la cuenta en la página de configuración de la cuentao eliminar tu cuenta en esta página de ayuda.

Limitaciones sobre la eliminación. Incluso después de eliminar información de tu perfil o eliminar tu cuenta, pueden permanecer copias de dicha información visibles en otro lugar en la medida en que se haya compartido con otros, se haya distribuido de otro modo conforme a tu configuración de la privacidad, o haya sido copiada o almacenada por otros usuarios. Sin embargo, tu nombre dejará de estar asociado con dicha información en Facebook. (Por ejemplo, si publicas algo en el perfil de otro usuario y después eliminas tu cuenta, dicha publicación podría permanecer, pero atribuirse a un "Usuario de Facebook anónimo.") Asimismo, podemos conservar cierta información para evitar el robo de identidades y otras conductas inadecuadas, incluso si se ha solicitado la eliminación. Si has facilitado a aplicaciones o sitios web de terceros acceso a tu información, éstos pueden conservar tu información hasta el límite permitido por sus condiciones de servicio o políticas de privacidad. Sin embargo, después de desconectarte de ellos, ya no podrán acceder a la información a través de nuestra plataforma.

Copias de seguridad. La información eliminada y borrada puede permanecer en copias de seguridad hasta un máximo de 90 días, pero no estará disponible para los demás.

Información de contacto de no usuarios. Si un usuario nos facilita tu dirección de correo electrónico, pero no eres usuario de Facebook y quieres que la eliminemos, puedes hacerlo en esta página de ayuda. Sin embargo, esa solicitud sólo se aplicará a las direcciones que tengamos en el momento de la solicitud y no a ninguna dirección que los usuarios nos faciliten posteriormente.

8. Cómo protegemos la información

Hacemos todo lo posible para mantener a salvo tu información, pero necesitamos tu ayuda. Para obtener información más pormenorizada sobre cómo mantener la seguridad en Facebook, visita la página Security Page de Facebook.

Medidas que tomamos para mantener a salvo su información. Mantenemos la información de tu cuenta en un servidor protegido con un firewall. Cuando introduces información confidencial (por ejemplo, contraseñas y números de tarjeta de crédito), la ciframos usando tecnología de capa de socket seguro (SSL). También utilizamos medidas sociales y automatizadas para aumentar la seguridad (como el análisis de la actividad de la cuenta por si hubiera algún comportamiento fraudulento o anómalo de otro tipo), podemos limitar el uso de funciones del sitio web en respuesta a posibles signos de abuso, podemos eliminar contenido inadecuado o enlaces a contenido ilegal, y podemos suspender o desactivar cuentas por si hubiera violaciones de nuestra Declaración de derechos y responsabilidades.

Riesgos inherentes a compartir información. Aunque te permitimos definir opciones de privacidad que limiten el acceso a tu información, ten en cuenta que ninguna medida de seguridad es perfecta ni impenetrable. No podemos controlar las acciones de otros usuarios con los que compartas información. No podemos garantizar que sólo vean tu información personas autorizadas. No podemos garantizar que la información que compartas en Facebook no pase a estar disponible públicamente. No somos responsables de que ningún tercero burle cualquier configuración de la privacidad o medidas de seguridad en Facebook. Puedes reducir estos riesgos utilizando hábitos de seguridad de sentido común como elegir una contraseña segura, utilizar contraseñas diferentes para servicios diferentes y emplear software antivirus actualizado.

Informar de incumplimientos. Deberías informarnos de cualquier incumplimiento de la seguridad en esta página de ayuda.

9. Otras condiciones

Cambios. Podemos cambiar esta Política de privacidad conforme a los procedimientos señalados en la Declaración de derechos y responsabilidades. Salvo indicación en contrario, nuestra política de privacidad en vigor se aplica a toda la información que tenemos sobre ti y tu cuenta. Si realizamos cambios en esta Política de privacidad, te lo notificaremos publicándolo aquí y en la página Facebook Site Governance. Si los cambios son sustanciales, mostraremos un aviso prominente si las circunstancias lo requieren. Puedes asegurarte de que recibes notificación directamente haciendo clic en el botón "Me gusta" de la página Facebook Site Governance.

Consentimiento para la recopilación y procesamiento en Estados Unidos. Al utilizar Facebook, das tu consentimiento para que tus datos personales sean transferidos y procesados en Estados Unidos.

Términos definidos. "Nos," "nosotros," "nuestro," "Plataforma" y "Facebook" significan lo mismo que en la Declaración de derechos y responsabilidades. “Información” y “contenido” se utilizan de forma más general e intercambiable aquí que en la Declaración de derechos y responsabilidadessalvo que el contexto lo limite de otro modo.

Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal

43088 Martes 14 diciembre 1999 BOE núm. 298

I. Disposiciones generales

JEFATURA DEL ESTADO

23750 *LEY ORGÁNICA 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.*

JUAN CARLOS I
REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente Ley Orgánica.

TÍTULO I

Disposiciones generales

Artículo 1. *Objeto.*

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

Artículo 2. *Ámbito de aplicación.*

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.
Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:
a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.
c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:
a) A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
b) A los ficheros sometidos a la normativa sobre protección de materias clasificadas.
c) A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a) Los ficheros regulados por la legislación de régimen electoral.
b) Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.
c) Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
d) Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
e) Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

Artículo 3. *Definiciones.*

A los efectos de la presente Ley Orgánica se entenderá por:

a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables.
b) Fichero: todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.
d) Responsable del fichero o tratamiento: persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
e) Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.
f) Procedimiento de disociación: todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable.
g) Encargado del tratamiento: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
h) Consentimiento del interesado: toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen.

i) Cesión o comunicación de datos: toda revelación de datos realizada a una persona distinta del interesado.
j) Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

TÍTULO II

Principios de la protección de datos

Artículo 4. *Calidad de los datos.*

1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.
3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.
4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.
5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.
No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.
6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

Artículo 5. *Derecho de información en la recogida de datos.*

1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.
2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior.
3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.
4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.
5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.
Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten.

Artículo 6. *Consentimiento del afectado.*

1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.
2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado.

Artículo 7. *Datos especialmente protegidos.*

1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.

Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.

2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.

3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.

4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.

5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

Artículo 8. *Datos relativos a la salud.*

Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

Artículo 9. *Seguridad de los datos.*

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Artículo 10. *Deber de secreto.*

El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

Artículo 11. *Comunicación de datos.*

1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

2. El consentimiento exigido en el apartado anterior no será preciso:

a) Cuando la cesión está autorizada en una ley.

b) Cuando se trate de datos recogidos de fuentes accesibles al público.

c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.

3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.
4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.
5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.
6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores.

Artículo 12. *Acceso a los datos por cuenta de terceros.*

1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.
2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.
3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

TÍTULO III

Derechos de las personas

Artículo 13. *Impugnación de valoraciones.*

1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.
3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.
4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado.

Artículo 14. *Derecho de consulta al Registro General de Protección de Datos.*

Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita.

Artículo 15. *Derecho de acceso.*

1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.
2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.
3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes.

Artículo 16. *Derecho de rectificación y cancelación.*

1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.
2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.
3. 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. Cumplido el citado plazo deberá procederse a la supresión.
4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.
5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.

Artículo 17. *Procedimiento de oposición, acceso, rectificación o cancelación.*

1. Los procedimientos para ejercitar el derecho de oposición, acceso, así como los de rectificación y cancelación serán establecidos reglamentariamente.
2. No se exigirá contraprestación alguna por el ejercicio de los derechos de oposición, acceso, rectificación o cancelación.

Artículo 18. *Tutela de los derechos.*

1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los

interesados ante la Agencia de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia de Protección de Datos procederá recurso contencioso-administrativo.

Artículo 19. *Derecho a indemnización.*

1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.

2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.

3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria.

TÍTULO IV

Disposiciones sectoriales

CAPÍTULO I

Ficheros de titularidad pública

Artículo 20. *Creación, modificación o supresión.*

1. La creación, modificación o supresión de los ficheros de las Administraciones públicas sólo podrán hacerse por medio de disposición general publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

2. Las disposiciones de creación o de modificación de ficheros deberán indicar:

a) La finalidad del fichero y los usos previstos para el mismo.

b) Las personas o colectivos sobre los que se pretenda obtener datos de carácter personal o que resulten obligados a suministrarlos.

c) El procedimiento de recogida de los datos de carácter personal.

d) La estructura básica del fichero y la descripción de los tipos de datos de carácter personal incluidos en el mismo.

e) Las cesiones de datos de carácter personal y, en su caso, las transferencias de datos que se prevean a países terceros.

f) Los órganos de las Administraciones responsables del fichero.

g) Los servicios o unidades ante los que pudiesen ejercitarse los derechos de acceso, rectificación, cancelación y oposición.

h) Las medidas de seguridad con indicación del nivel básico, medio o alto exigible.

3. En las disposiciones que se dicten para la supresión de los ficheros, se establecerá el destino de los mismos o, en su caso, las previsiones que se adopten para su destrucción.

Artículo 21. *Comunicación de datos entre Administraciones públicas.*

1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra.

3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa.

4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

Artículo 22. *Ficheros de las Fuerzas y Cuerpos de Seguridad.*

1. Los ficheros creados por las Fuerzas y Cuerpos de Seguridad que contengan datos de carácter personal que, por haberse recogido para fines administrativos, deban ser objeto de registro permanente, estarán sujetos al régimen general de la presente Ley.

2. La recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad.

3. La recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos jurisdiccionales.

4. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento.

A estos efectos, se considerará especialmente la edad del afectado y el carácter de los datos almacenados, la necesidad de mantener los datos hasta la conclusión de una investigación o procedimiento concreto, la resolución judicial firme, en especial la absolutoria, el indulto, la rehabilitación y la prescripción de responsabilidad.

Artículo 23. *Excepciones a los derechos de acceso, rectificación y cancelación.*

1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del

artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

2. Los responsables de los ficheros de la Hacienda Pública podrán, igualmente, denegar el ejercicio de los derechos a que se refiere el apartado anterior cuando el mismo obstaculice las actuaciones administrativas tendentes a asegurar el cumplimiento de las obligaciones tributarias y, en todo caso, cuando el afectado esté siendo objeto de actuaciones inspectoras.

3. El afectado al que se deniegue, total o parcialmente, el ejercicio de los derechos mencionados en los apartados anteriores podrá ponerlo en conocimiento del Director de la Agencia de Protección de Datos o del organismo competente de cada Comunidad Autónoma en el caso de ficheros mantenidos por Cuerpos de Policía propios de éstas, o por las Administraciones tributarias autonómicas, quienes deberán asegurarse de la procedencia o improcedencia de la denegación.

Artículo 24. *Otras excepciones a los derechos de los afectados.*

1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.

2. Lo dispuesto en el artículo 15 y en el apartado 1 del artículo 16 no será de aplicación si, ponderados los intereses en presencia, resultase que los derechos que dichos preceptos conceden al afectado hubieran de ceder ante razones de interés público o ante intereses de terceros más dignos de protección. Si el órgano administrativo responsable del fichero invocase lo dispuesto en este apartado, dictará resolución motivada e instruirá al afectado del derecho que le asiste a poner la negativa en conocimiento del Director de la Agencia de Protección de Datos o, en su caso, del órgano equivalente de las Comunidades Autónomas.

CAPÍTULO II

Ficheros de titularidad privada

Artículo 25. *Creación.*

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías que esta Ley establece para la protección de las personas.

Artículo 26. *Notificación e inscripción registral.*

1. Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia de Protección de Datos.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

3. Deberán comunicarse a la Agencia de Protección de Datos los cambios que se produzcan en la finalidad del fichero automatizado, en su responsable y en la dirección de su ubicación.

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles.

En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Artículo 27. *Comunicación de la cesión de datos.*

1. El responsable del fichero, en el momento en que se efectúe la primera cesión de datos, deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.

2. La obligación establecida en el apartado anterior no existirá en el supuesto previsto en los apartados 2, letras c), d), e) y 6 del artículo 11, ni cuando la cesión venga impuesta por ley.

Artículo 28. *Datos incluidos en las fuentes de acceso público.*

1. Los datos personales que figuren en el censo promocional, o las listas de personas pertenecientes a grupos de profesionales a que se refiere el artículo 3, j) de esta Ley deberán limitarse a los que sean estrictamente necesarios para cumplir la finalidad a que se destina cada listado. La inclusión de datos adicionales por las entidades responsables del mantenimiento de dichas fuentes requerirá el consentimiento del interesado, que podrá ser revocado en cualquier momento.

2. Los interesados tendrán derecho a que la entidad responsable del mantenimiento de los listados de los Colegios profesionales indique gratuitamente que sus datos personales no pueden utilizarse para fines de publicidad o prospección comercial.

Los interesados tendrán derecho a exigir gratuitamente la exclusión de la totalidad de sus datos personales que consten en el censo promocional por las entidades encargadas del mantenimiento de dichas fuentes.

La atención a la solicitud de exclusión de la información innecesaria o de inclusión de la objeción al uso de los datos para fines de publicidad o venta a distancia deberá realizarse en el plazo de diez días respecto de las informaciones que se realicen mediante consulta o comunicación telemática y en la siguiente edición del listado cualquiera que sea el soporte en que se edite.

3. Las fuentes de acceso público que se editen en forma de libro o algún otro soporte físico, perderán el carácter de fuente accesible con la nueva edición que se publique.

En el caso de que se obtenga telemáticamente una copia de la lista en formato electrónico, ésta perderá el carácter de fuente de acceso público en el plazo de un año, contado desde el momento de su obtención.

4. Los datos que figuren en las guías de servicios de telecomunicaciones disponibles al público se regirán por su normativa específica.

Artículo 29. *Prestación de servicios de información sobre solvencia patrimonial y crédito.*

1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos

de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Artículo 30. *Tratamientos con fines de publicidad y de prospección comercial.*

1. Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.

2. Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.

3. En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.

4. Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud.

Artículo 31. *Censo promocional.*

1. Quienes pretendan realizar permanente o esporádicamente la actividad de recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial u otras actividades análogas, podrán solicitar del Instituto Nacional de Estadística o de los órganos equivalentes de las Comunidades Autónomas una copia del censo promocional, formado con los datos de nombre, apellidos y domicilio que constan en el censo electoral.

2. El uso de cada lista de censo promocional tendrá un plazo de vigencia de un año. Transcurrido el plazo citado, la lista perderá su carácter de fuente de acceso público.

3. Los procedimientos mediante los que los interesados podrán solicitar no aparecer en el censo promocional se regularán reglamentariamente. Entre estos procedimientos, que serán gratuitos para los interesados, se incluirá el documento de empadronamiento. Trimestralmente se editará una lista actualizada del censo promocional, excluyendo los nombres y domicilios de los que así lo hayan solicitado.

4. Se podrá exigir una contraprestación por la facilitación de la citada lista en soporte informático.

Artículo 32. *Códigos tipo.*

1. Mediante acuerdos sectoriales, convenios administrativos o decisiones de empresa, los responsables de tratamientos de titularidad pública y privada, así como las organizaciones en que se agrupen, podrán formular códigos tipo que establezcan las condiciones de organización, régimen de funcionamiento, procedimientos aplicables, normas de seguridad del entorno, programas o equipos, obligaciones de los implicados en el tratamiento y uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a los principios y disposiciones de la presente Ley y sus normas de desarrollo.

2. Los citados códigos podrán contener o no reglas operacionales detalladas de cada sistema particular y estándares técnicos de aplicación.

En el supuesto de que tales reglas o estándares no se incorporen directamente al código, las instrucciones u órdenes que los establecieran deberán respetar los principios fijados en aquél.

3. Los códigos tipo tendrán el carácter de códigos deontológicos o de buena práctica profesional, debiendo ser depositados o inscritos en el Registro General de Protección de Datos y, cuando corresponda, en los creados a estos efectos por las Comunidades Autónomas, de acuerdo con el artículo 41. El Registro General de Protección de Datos podrá denegar la inscripción cuando considere que no se ajusta a las disposiciones legales y reglamentarias sobre la materia, debiendo, en este caso, el Director de la Agencia de Protección de Datos requerir a los solicitantes para que efectúen las correcciones oportunas.

TÍTULO V

Movimiento internacional de datos

Artículo 33. *Norma general.*

1. No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas.

2. El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países.

Artículo 34. *Excepciones.*

Lo dispuesto en el artículo anterior no será de aplicación:

a) Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España.
b) Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional.
c) Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios.
d) Cuando se refiera a transferencias dinerarias conforme a su legislación específica.
e) Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista.
f) Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
g) Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
h) Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias.
i) Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
j) Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.
k) Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado.

TÍTULO VI

Agencia de Protección de Datos

Artículo 35. *Naturaleza y régimen jurídico.*

1. La Agencia de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones públicas en el ejercicio de sus funciones. Se regirá por lo dispuesto en la presente Ley y en un Estatuto propio, que será aprobado por el Gobierno.
2. En el ejercicio de sus funciones públicas, y en defecto de lo que disponga la presente Ley y sus disposiciones de desarrollo, la Agencia de Protección de Datos actuará de conformidad con la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. En sus adquisiciones patrimoniales y contratación estará sujeta al derecho privado.
3. Los puestos de trabajo de los órganos y servicios que integren la Agencia de Protección de Datos serán desempeñados por funcionarios de las Administraciones públicas y por personal contratado al efecto, según la naturaleza de las funciones asignadas a cada puesto de trabajo. Este personal está obligado a guardar secreto de los datos de carácter personal de que conozca en el desarrollo de su función.
4. La Agencia de Protección de Datos contará, para el cumplimiento de sus fines, con los siguientes bienes y medios económicos:

a) Las asignaciones que se establezcan anualmente con cargo a los Presupuestos Generales del Estado.
b) Los bienes y valores que constituyan su patrimonio, así como los productos y rentas del mismo.
c) Cualesquiera otros que legalmente puedan serle atribuidos.

5. La Agencia de Protección de Datos elaborará y aprobará con carácter anual el correspondiente anteproyecto de presupuesto y lo remitirá al Gobierno para que sea integrado, con la debida independencia, en los Presupuestos Generales del Estado.

Artículo 36. *El Director.*

1. El Director de la Agencia de Protección de Datos dirige la Agencia y ostenta su representación. Será nombrado, de entre quienes componen el Consejo Consultivo, mediante Real Decreto, por un período de cuatro años.
2. Ejercerá sus funciones con plena independencia y objetividad y no estará sujeto a instrucción alguna en el desempeño de aquéllas.
En todo caso, el Director deberá oír al Consejo Consultivo en aquellas propuestas que éste le realice en el ejercicio de sus funciones.
3. El Director de la Agencia de Protección de Datos sólo cesará antes de la expiración del período a que se refiere el apartado 1, a petición propia o por separación acordada por el Gobierno, previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso.
4. El Director de la Agencia de Protección de Datos tendrá la consideración de alto cargo y quedará en la situación de servicios especiales si con anterioridad estuviera desempeñando una función pública. En el supuesto de que sea nombrado para el cargo algún miembro de la carrera judicial o fiscal, pasará asimismo a la situación administrativa de servicios especiales.

Artículo 37. *Funciones.*

Son funciones de la Agencia de Protección de Datos:

a) Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de información, acceso, rectificación, oposición y cancelación de datos.
b) Emitir las autorizaciones previstas en la Ley o en sus disposiciones reglamentarias.
c) Dictar, en su caso, y sin perjuicio de las competencias de otros órganos, las instrucciones precisas para adecuar los tratamientos a los principios de la presente Ley.
d) Atender las peticiones y reclamaciones formuladas por las personas afectadas.
e) Proporcionar información a las personas acerca de sus derechos en materia de tratamiento de los datos de carácter personal.
f) Requerir a los responsables y los encargados de los tratamientos, previa audiencia de éstos, la adopción de las medidas necesarias para la adecuación del tratamiento de datos a las disposiciones de esta Ley y, en su caso, ordenar la cesación de los tratamientos y la cancelación de los ficheros, cuando no se ajuste a sus disposiciones.
g) Ejercer la potestad sancionadora en los términos previstos por el Título VII de la presente Ley.

h) Informar, con carácter preceptivo, los proyectos de disposiciones generales que desarrollen esta Ley.
i) Recabar de los responsables de los ficheros cuanta ayuda e información estime necesaria para el desempeño de sus funciones.
j) Velar por la publicidad de la existencia de los ficheros de datos con carácter personal, a cuyo efecto publicará periódicamente una relación de dichos ficheros con la información adicional que el Director de la Agencia determine.
k) Redactar una memoria anual y remitirla al Ministerio de Justicia.
l) Ejercer el control y adoptar las autorizaciones que procedan en relación con los movimientos internacionales de datos, así como desempeñar las funciones de cooperación internacional en materia de protección de datos personales.
m) Velar por el cumplimiento de las disposiciones que la Ley de la Función Estadística Pública establece respecto a la recogida de datos estadísticos y al secreto estadístico, así como dictar las instrucciones precisas, dictaminar sobre las condiciones de seguridad de los ficheros constituidos con fines exclusivamente estadísticos y ejercer la potestad a la que se refiere el artículo 46.
n) Cuantas otras le sean atribuidas por normas legales o reglamentarias.

Artículo 38. *Consejo Consultivo.*

El Director de la Agencia de Protección de Datos estará asesorado por un Consejo Consultivo compuesto por los siguientes miembros:

Un Diputado, propuesto por el Congreso de los Diputados.
Un Senador, propuesto por el Senado.
Un representante de la Administración Central, designado por el Gobierno.
Un representante de la Administración Local, propuesto por la Federación Española de Municipios y Provincias.
Un miembro de la Real Academia de la Historia, propuesto por la misma.
Un experto en la materia, propuesto por el Consejo Superior de Universidades.
Un representante de los usuarios y consumidores, seleccionado del modo que se prevea reglamentariamente.
Un representante de cada Comunidad Autónoma que haya creado una agencia de protección de datos en su ámbito territorial, propuesto de acuerdo con el procedimiento que establezca la respectiva Comunidad Autónoma.
Un representante del sector de ficheros privados, para cuya propuesta se seguirá el procedimiento que se regule reglamentariamente.

El funcionamiento del Consejo Consultivo se regirá por las normas reglamentarias que al efecto se establezcan.

Artículo 39. *El Registro General de Protección de Datos.*

1. El Registro General de Protección de Datos es un órgano integrado en la Agencia de Protección de Datos.
2. Serán objeto de inscripción en el Registro General de Protección de Datos:

a) Los ficheros de que sean titulares las Administraciones públicas.
b) Los ficheros de titularidad privada.
c) Las autorizaciones a que se refiere la presente Ley.
d) Los códigos tipo a que se refiere el artículo 32 de la presente Ley.
e) Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

3. Por vía reglamentaria se regulará el procedimiento de inscripción de los ficheros, tanto de titularidad pública como de titularidad privada, en el Registro General de Protección de Datos, el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes y demás extremos pertinentes.

Artículo 40. *Potestad de inspección.*

1. Las autoridades de control podrán inspeccionar los ficheros a que hace referencia la presente Ley, recabando cuantas informaciones precisen para el cumplimiento de sus cometidos.
A tal efecto, podrán solicitar la exhibición o el envío de documentos y datos y examinarlos en el lugar en que se encuentren depositados, así como inspeccionar los equipos físicos y lógicos utilizados para el tratamiento de los datos, accediendo a los locales donde se hallen instalados.
2. Los funcionarios que ejerzan la inspección a que se refiere el apartado anterior tendrán la consideración de autoridad pública en el desempeño de sus cometidos.
Estarán obligados a guardar secreto sobre las informaciones que conozcan en el ejercicio de las mencionadas funciones, incluso después de haber cesado en las mismas.

Artículo 41. *Órganos correspondientes de las Comunidades Autónomas.*

1. Las funciones de la Agencia de Protección de Datos reguladas en el artículo 37, a excepción de las mencionadas en los apartados j), k) y l), y en los apartados f) y g) en lo que se refiere a las transferencias internacionales de datos, así como en los artículos 46 y 49, en relación con sus específicas competencias serán ejercidas, cuando afecten a ficheros de datos de carácter personal creados o gestionados por las Comunidades Autónomas y por la Administración Local de su ámbito territorial, por los órganos correspondientes de cada Comunidad, que tendrán la consideración de autoridades de control, a los que garantizarán plena independencia y objetividad en el ejercicio de su cometido.
2. Las Comunidades Autónomas podrán crear y mantener sus propios registros de ficheros para el ejercicio de las competencias que se les reconoce sobre los mismos.
3. El Director de la Agencia de Protección de Datos podrá convocar regularmente a los órganos correspondientes de las Comunidades Autónomas a efectos de cooperación institucional y coordinación de criterios o procedimientos de actuación. El Director de la Agencia de Protección de Datos y los órganos correspondientes de las Comunidades Autónomas podrán solicitarse mutuamente la información necesaria para el cumplimiento de sus funciones.

Artículo 42. *Ficheros de las Comunidades Autónomas en materia de su exclusiva competencia.*

1. Cuando el Director de la Agencia de Protección de Datos constate que el mantenimiento o uso de un determinado fichero de las Comunidades Autónomas contraviene algún precepto de esta Ley en materia de su exclusiva competencia podrá requerir a la Administración correspondiente que se adopten las medidas

correctoras que determine en el plazo que expresamente se fije en el requerimiento.

2. Si la Administración pública correspondiente no cumpliera el requerimiento formulado, el Director de la Agencia de Protección de Datos podrá impugnar la resolución adoptada por aquella Administración.

TÍTULO VII

Infracciones y sanciones

Artículo 43. *Responsables.*

1. Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la presente Ley.

2. Cuando se trate de ficheros de los que sean responsables las Administraciones públicas se estará, en cuanto al procedimiento y a las sanciones, a lo dispuesto en el artículo 46, apartado 2.

Artículo 44. *Tipos de infracciones.*

1. Las infracciones se calificarán como leves, graves o muy graves.

2. Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.

c) No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

3. Son infracciones graves:

a) Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general, publicada en el «Boletín Oficial del Estado» o Diario oficial correspondiente.

b) Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades distintas de las que constituyen el objeto legítimo de la empresa o entidad.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la presente Ley ampara.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.

h) 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.

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.

j) La obstrucción al ejercicio de la función inspectora.

k) No inscribir el fichero de datos de carácter personal en el Registro General de Protección Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

4. Son infracciones muy graves:

a) La recogida de datos en forma engañosa y fraudulenta.

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del artículo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.

d) No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.

e) La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.

f) Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.

g) La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Artículo 45. *Tipo de sanciones.*

1. Las infracciones leves serán sancionadas con multa de 100.000 a 10.000.000 de pesetas.

2. Las infracciones graves serán sancionadas con multa de 10.000.000 a 50.000.000 de pesetas.

3. Las infracciones muy graves serán sancionadas con multa de 50.000.000 a 100.000.000 de pesetas.

4. La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceras personas, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuridicidad y de culpabilidad presentes en la concreta actuación infractora.

5. Si, en razón de las circunstancias concurrentes, se apreciara una cualificada disminución de la culpabilidad del imputado o de la antijuridicidad del hecho, el órgano sancionador establecerá la cuantía de la sanción aplicando la escala relativa a la clase de infracciones que preceda inmediatamente en gravedad a aquella en que se integra la considerada en el caso de que se trate.

6. En ningún caso podrá imponerse una sanción más grave que la fijada en la Ley para la clase de infracción en la que se integre la que se pretenda sancionar.

7. El Gobierno actualizará periódicamente la cuantía de las sanciones de acuerdo con las variaciones que experimenten los índices de precios.

Artículo 46. *Infracciones de las Administraciones públicas.*

1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de los que sean responsables las Administraciones públicas, el Director de la Agencia de Protección de Datos dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.

2. El Director de la Agencia podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.

3. Se deberán comunicar a la Agencia las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

4. El Director de la Agencia comunicará al Defensor del Pueblo las actuaciones que efectúe y las resoluciones que dicte al amparo de los apartados anteriores.

Artículo 47. *Prescripción.*

1. Las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves al año.

2. El plazo de prescripción comenzará a contarse desde el día en que la infracción se hubiera cometido.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reanudándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

4. Las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año.

5. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que adquiera firmeza la resolución por la que se impone la sanción.

6. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor.

Artículo 48. *Procedimiento sancionador.*

1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

2. Las resoluciones de la Agencia de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

Artículo 49. *Potestad de inmovilización de ficheros.*

En los supuestos, constitutivos de infracción muy grave, de utilización o cesión ilícita de los datos de carácter personal en que se impida gravemente o se atente de igual modo contra el ejercicio de los derechos de los ciudadanos y el libre desarrollo de la personalidad que la Constitución y las leyes garantizan, el Director de la Agencia de Protección de Datos podrá, además de ejercer la potestad sancionadora, requerir a los responsables de ficheros de datos de carácter personal, tanto de titularidad pública como privada, la cesación en la utilización o cesión ilícita de los datos. Si el requerimiento fuera desatendido, la Agencia de Protección de Datos podrá, mediante resolución motivada, inmovilizar tales ficheros a los solos efectos de restaurar los derechos de las personas afectadas.

Disposición adicional primera. *Ficheros preexistentes.*

Los ficheros y tratamientos automatizados inscritos o no en el Registro General de Protección de Datos deberán adecuarse a la presente Ley Orgánica dentro del plazo de tres años, a contar desde su entrada en vigor. En dicho plazo, los ficheros de titularidad privada deberán ser comunicados a la Agencia de Protección de Datos y las Administraciones públicas, responsables de ficheros de titularidad pública, deberán aprobar la pertinente disposición de regulación del fichero o adaptar la existente.

En el supuesto de ficheros y tratamientos no automatizados, su adecuación a la presente Ley Orgánica, y la obligación prevista en el párrafo anterior deberán cumplimentarse en el plazo de doce años a contar desde el 24 de octubre de 1995, sin perjuicio del ejercicio de los derechos de acceso, rectificación y cancelación por parte de los afectados.

Disposición adicional segunda. *Ficheros y Registro de Población de las Administraciones públicas.*

1. La Administración General del Estado y las Administraciones de las Comunidades Autónomas podrán solicitar al Instituto Nacional de Estadística, sin consentimiento del interesado, una copia actualizada del fichero formado con los datos del nombre, apellidos, domicilio, sexo y fecha de nacimiento que constan en los padrones municipales de habitantes y en el censo electoral correspondientes a los territorios donde ejerzan sus competencias, para la creación de ficheros o registros de población.

2. Los ficheros o registros de población tendrán como finalidad la comunicación de los distintos órganos de cada Administración pública con los interesados residentes en los respectivos territorios, respecto a las relaciones jurídico administrativas derivadas de las competencias respectivas de las Administraciones públicas.

Disposición adicional tercera. *Tratamiento de los expedientes de las derogadas Leyes de Vagos y Maleantes y de Peligrosidad y Rehabilitación Social.*

Los expedientes específicamente instruidos al amparo de las derogadas Leyes de Vagos y Maleantes, y de Peligrosidad y Rehabilitación Social, que contengan datos de cualquier índole susceptibles de afectar a la seguridad, al honor, a la intimidad o a la imagen de las personas, no podrán ser consultados sin que medie consentimiento expreso de los afectados, o hayan transcurrido cincuenta años desde la fecha de aquéllos.

En este último supuesto, la Administración General del Estado, salvo que haya constancia expresa del fallecimiento de los afectados, pondrá a disposición del solicitante la documentación, suprimiendo de la misma los datos aludidos en el párrafo anterior, mediante la utilización de los procedimientos técnicos pertinentes en cada caso.

Disposición adicional cuarta. *Modificación del artículo 112.4 de la Ley General Tributaria.*

El apartado cuarto del artículo 112 de la Ley General Tributaria pasa a tener la siguiente redacción:

«4. La cesión de aquellos datos de carácter personal, objeto de tratamiento, que se debe efectuar a la Administración tributaria conforme a lo dispuesto en el artículo 111, en los apartados anteriores de este artículo o en otra norma de rango legal, no requerirá el consentimiento del afectado. En este ámbito tampoco será de aplicación lo que respecto a las Administraciones públicas establece el apartado 1 del artículo 21 de la Ley Orgánica de Protección de Datos de carácter personal.»

Disposición adicional quinta. *Competencias del Defensor del Pueblo y órganos autonómicos semejantes.*

Lo dispuesto en la presente Ley Orgánica se entiende sin perjuicio de las competencias del Defensor del Pueblo y de los órganos análogos de las Comunidades Autónomas.

Disposición adicional sexta. *Modificación del artículo 24.3 de la Ley de Ordenación y Supervisión de los Seguros Privados.*

Se modifica el artículo 24.3, párrafo 2.º de la Ley 30/1995, de 8 de noviembre, de Ordenación y Supervisión de los Seguros Privados, con la siguiente redacción:

«Las entidades aseguradoras podrán establecer ficheros comunes que contengan datos de carácter personal para la liquidación de siniestros y la colaboración estadístico actuarial con la finalidad de permitir la tarificación y selección de riesgos y la elaboración de estudios de técnica aseguradora. La cesión de datos a los citados ficheros no requerirá el consentimiento previo del afectado, pero sí la comunicación al mismo de la posible cesión de sus datos personales a ficheros comunes para los fines señalados con expresa indicación del responsable para que se puedan ejercitar los derechos de acceso, rectificación y cancelación previstos en la ley.

También podrán establecerse ficheros comunes cuya finalidad sea prevenir el fraude en el seguro sin que sea necesario el consentimiento del afectado. No obstante, será necesaria en estos casos la comunicación al afectado, en la primera introducción de sus datos, de quién sea el responsable del fichero y de las formas de ejercicio de los derechos de acceso, rectificación y cancelación.

En todo caso, los datos relativos a la salud sólo podrán ser objeto de tratamiento con el consentimiento expreso del afectado.»

Disposición transitoria primera. *Tratamientos creados por Convenios internacionales.*

La Agencia de Protección de Datos será el organismo competente para la protección de las personas físicas en lo que respecta al tratamiento de datos de carácter personal respecto de los tratamientos establecidos en cualquier Convenio Internacional del que sea parte España que atribuya a una autoridad nacional de control esta competencia, mientras no se cree una autoridad diferente para este cometido en desarrollo del Convenio.

Disposición transitoria segunda. *Utilización del censo promocional.*

Reglamentariamente se desarrollarán los procedimientos de formación del censo promocional, de oposición a aparecer en el mismo, de puesta a disposición de sus solicitantes, y de control de las listas difundidas. El Reglamento establecerá los plazos para la puesta en operación del censo promocional.

Disposición transitoria tercera. *Subsistencia de normas preexistentes.*

Hasta tanto se lleven a efectos las previsiones de la disposición final primera de esta Ley, continuarán en vigor, con su propio rango, las normas reglamentarias existentes y, en especial, los Reales Decretos 428/1993, de 26 de marzo; 1332/1994, de 20 de junio, y 994/1999, de 11 de junio, en cuanto no se opongan a la presente Ley.

Disposición derogatoria única. *Derogación normativa.*

Queda derogada la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del tratamiento automatizado de los datos de carácter personal.

Disposición final primera. *Habilitación para el desarrollo reglamentario.*

El Gobierno aprobará, o modificará, las disposiciones reglamentarias necesarias para la aplicación y desarrollo de la presente Ley.

Disposición final segunda. *Preceptos con carácter de Ley ordinaria.*

Los Títulos IV, VI excepto el último inciso del párrafo 4 del artículo 36 y VII de la presente Ley, la disposición adicional cuarta, la disposición transitoria primera y la final primera tienen el carácter de Ley ordinaria.

Disposición final tercera. *Entrada en vigor.*

La presente Ley entrará en vigor en el plazo de un mes, contado desde su publicación en el «Boletín Oficial del Estado».

Por tanto,
Mando a todos los españoles, particulares y autoridades, que guarden y hagan guardar esta Ley Orgánica.

Madrid, 13 de diciembre de 1999.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSÉ MARÍA AZNAR LÓPEZ

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

BOE núm. 251 Viernes 19 octubre 2007 42517

I. Disposiciones generales

JEFATURA DEL ESTADO

18243 *LEY 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.*

JUAN CARLOS I

REY DE ESPAÑA

A todos los que la presente vieren y entendieren.
Sabed: Que las Cortes Generales han aprobado y Yo vengo en sancionar la siguiente ley.

PREÁMBULO

I

La aplicación de las nuevas tecnologías desarrolladas en el marco de la sociedad de la información ha supuesto la superación de las formas tradicionales de comunicación, mediante una expansión de los contenidos transmitidos, que abarcan no sólo la voz, sino también datos en soportes y formatos diversos. A su vez, esta extraordinaria expansión en cantidad y calidad ha venido acompañada de un descenso en los costes, haciendo que este tipo de comunicaciones se encuentre al alcance de cualquier persona y en cualquier rincón del mundo.

La naturaleza neutra de los avances tecnológicos en telefonía y comunicaciones electrónicas no impide que su uso pueda derivarse hacia la consecución de fines indeseados, cuando no delictivos.

Precisamente en el marco de este último objetivo se encuadra la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y por la que se modifica la Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio, cuya transposición a nuestro ordenamiento jurídico es el objetivo principal de esta Ley.

El objeto de esta Directiva es establecer la obligación de los operadores de telecomunicaciones de retener determinados datos generados o tratados por los mismos, con el fin de posibilitar que dispongan de ellos los agentes facultados. Se entienden por agentes facultados los miembros de los Cuerpos Policiales autorizados para ello en el marco de una investigación criminal por la comisión de un delito, el personal del Centro Nacional de Inteligencia para llevar a cabo una investigación de seguridad amparada en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. Se trata, pues, de que todos éstos puedan obtener los datos relativos a las comunicaciones que, relacionadas con una investigación, se hayan podido efectuar por medio de la telefonía fija o móvil, así como por Internet. El establecimiento de esas obligaciones, justificado en aras de proteger la seguridad pública, se ha efectuado buscando el imprescindible equilibrio con el respeto de los derechos individuales que puedan verse afectados, como son los relativos a la privacidad y la intimidad de las comunicaciones.

En este sentido, la Ley es respetuosa con los pronunciamientos que, en relación con el derecho al secreto de las comunicaciones, ha venido emitiendo el Tribunal Constitucional, respeto que, especialmente, se articula a través de dos garantías: en primer lugar, que los datos sobre los que se establece la obligación de conservación son datos exclusivamente vinculados a la comunicación, ya sea telefónica o efectuada a través de Internet, pero en ningún caso reveladores del contenido de ésta; y, en segundo lugar, que la cesión de tales datos que afecten a una comunicación o comunicaciones concretas, exigirá, siempre, la autorización judicial previa.

En relación con esta última precisión, cabe señalar que la Directiva se refiere, expresamente, a que los datos conservados deberán estar disponibles a los fines de detección o investigación por delitos graves, definidos éstos de acuerdo con la legislación interna de cada Estado miembro.

II

La Ley cuenta con diez artículos que se agrupan en tres capítulos.

El Capítulo I («Disposiciones Generales») se inicia describiendo su objeto, que básicamente se circunscribe a la determinación de la obligación de conservar los datos enumerados en el artículo 3, que se hayan generado o tratado en el marco de una comunicación de telefonía fija o móvil, o realizada a través de una comunicación electrónica de acceso público o mediante una red pública de comunicaciones. Igualmente, se precisan los fines que, exclusivamente, justifican la obligación de conservación, y que se limitan a la detección, investigación y enjuiciamiento de un delito contemplado en el Código Penal o las leyes penales especiales, con los requisitos y cautelas que la propia Ley establece.

En este capítulo también se precisan las limitaciones sobre el tipo de datos a retener, que son los necesarios para identificar el origen y destino de la comunicación, así como la identidad de los usuarios o abonados de ambos, pero nunca datos que revelen el contenido de la comunicación. Igualmente, la Ley impone la obligación de conservación de datos que permitan determinar el momento y duración de una determinada comunicación, su tipo, así

como datos necesarios para identificar el equipo de comunicación empleado y, en el caso de utilización de un equipo móvil, los datos necesarios para su localización.

En relación con los sujetos que quedan obligados a conservar los datos, éstos serán los operadores que presten servicios de comunicaciones electrónicas disponibles al público, o que exploten una red pública de comunicaciones electrónicas en España.

La Ley enumera en su artículo 3, de manera precisa y detallada, el listado de datos que quedan sujetos a la obligación de conservación en el marco de las comunicaciones por telefonía fija, móvil o Internet. Estos datos, que, se repite, en ningún caso revelarán el contenido de la comunicación, son los necesarios para identificar el origen y destino de la comunicación, su hora, fecha y duración, el tipo de servicio utilizado y el equipo de comunicación de los usuarios utilizado. En aplicación de las previsiones contenidas en la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo, quedan incluidas también en el ámbito de aplicación de la Ley las denominadas llamadas telefónicas infructuosas. Igualmente se incluye la obligación de conservar los elementos que sean suficientes para identificar el momento de activación de los teléfonos que funcionen bajo la modalidad de prepago.

En el Capítulo II («Conservación y cesión de datos») se establecen los límites para efectuar la cesión de datos, el plazo de conservación de los mismos, que será, con carácter general, de doce meses desde que la comunicación se hubiera establecido (si bien reglamentariamente se podrá reducir a seis meses o ampliar a dos años, como permite la Directiva 2006/24/CE), y los instrumentos para garantizar el uso legítimo de los datos conservados, cuya cesión y entrega exclusivamente se podrá efectuar al agente facultado y para los fines establecidos en la Ley, estando cualquier uso indebido sometido a los mecanismos de control de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y su normativa de desarrollo. Además, se establecen previsiones específicas respecto al régimen general regulador de los derechos de acceso, rectificación y cancelación de datos contenido en la referida Ley Orgánica 15/1999.

El Capítulo III, al referirse al régimen sancionador, remite, en cuanto a los incumplimientos de las obligaciones de conservación y protección y seguridad de los datos de carácter personal, a la regulación contenida en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. Por otro lado, los incumplimientos de la obligación de puesta a disposición de los agentes facultados, en la medida en que las solicitudes estarán siempre amparadas por orden judicial, constituirían la correspondiente infracción penal.

En las disposiciones contenidas en la parte final se incluyen contenidos diversos. Por un lado, y a los efectos de poder establecer instrumentos para controlar el empleo para fines delictivos de los equipos de telefonía móvil adquiridos mediante la modalidad de prepago, se establece, como obligación de los operadores que comercialicen dicho servicio, la llevanza de un registro con la identidad de los compradores.

Por último, la Ley incorpora en las disposiciones finales una modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, para adaptarla al contenido de esta Ley, una referencia a su amparo competencial, una habilitación general al Gobierno para su desarrollo y un periodo de seis meses para que las operadoras puedan adaptarse a su contenido.

CAPÍTULO I

Disposiciones generales

Artículo 1. *Objeto de la Ley.*

1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales.

2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado.

3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas.

Artículo 2. *Sujetos obligados.*

Son destinatarios de las obligaciones relativas a la conservación de datos impuestas en esta Ley los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones, en los términos establecidos en la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.

Artículo 3. *Datos objeto de conservación.*

1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes:

a) Datos necesarios para rastrear e identificar el origen de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:

i) Número de teléfono de llamada.
ii) Nombre y dirección del abonado o usuario registrado.

2.º Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) La identificación de usuario asignada.
ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía.
iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono.

b) Datos necesarios para identificar el destino de una comunicación:

1.º Con respecto a la telefonía de red fija y a la telefonía móvil:

i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas.
ii) Los nombres y las direcciones de los abonados o usuarios registrados.

2.° Con respecto al correo electrónico por Internet y la telefonía por Internet:

i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por Internet.
ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación.

c) Datos necesarios para determinar la fecha, hora y duración de una comunicación:

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia.
2.° Con respecto al acceso a Internet, al correo electrónico por Internet y a la telefonía por Internet:

i) La fecha y hora de la conexión y desconexión del servicio de acceso a Internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a Internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado.
ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por Internet o del servicio de telefonía por Internet, basadas en un determinado huso horario.

d) Datos necesarios para identificar el tipo de comunicación.

1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia).
2.° Con respecto al correo electrónico por Internet y a la telefonía por Internet: el servicio de Internet utilizado.

e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación:

1.° Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino.
2.° Con respecto a la telefonía móvil:

i) Los números de teléfono de origen y destino.
ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada.
iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada.
iv) La IMSI de la parte que recibe la llamada.
v) La IMEI de la parte que recibe la llamada.
vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio.

3.° Con respecto al acceso a Internet, correo electrónico por Internet y telefonía por Internet:

i) El número de teléfono de origen en caso de acceso mediante marcado de números.
ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación.

f) Datos necesarios para identificar la localización del equipo de comunicación móvil:

1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación.
2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones.

2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley.

CAPÍTULO II

Conservación y cesión de datos

Artículo 4. *Obligación de conservar datos.*

1. Los sujetos obligados adoptarán las medidas necesarias para garantizar que los datos especificados en el artículo 3 de esta Ley se conserven de conformidad con lo dispuesto en ella, en la medida en que sean generados o tratados por aquéllos en el marco de la prestación de los servicios de comunicaciones de que se trate.
En ningún caso, los sujetos obligados podrán aprovechar o utilizar los registros generados, fuera de los supuestos de autorización fijados en el artículo 38 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.
2. La citada obligación de conservación se extiende a los datos relativos a las llamadas infructuosas, en la medida que los datos son generados o tratados y conservados o registrados por los sujetos obligados. Se entenderá por llamada infructuosa aquella comunicación en el transcurso de la cual se ha realizado con éxito una llamada telefónica pero sin contestación, o en la que ha habido una intervención por parte del operador u operadores involucrados en la llamada.
3. Los datos relativos a las llamadas no conectadas están excluidos de las obligaciones de conservación contenidas en esta Ley. Se entenderá por llamada no conectada aquella comunicación en el transcurso de la cual se ha realizado sin éxito una llamada telefónica, sin que haya habido intervención del operador u operadores involucrados.

Artículo 5. *Período de conservación de los datos.*

1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación. Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores.
2. Lo dispuesto en el apartado anterior se entiende sin perjuicio de lo previsto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, sobre la obligación de conservar datos bloqueados en los supuestos legales de cancelación.

Artículo 6. *Normas generales sobre cesión de datos.*

1. Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial.
2. La cesión de la información se efectuará únicamente a los agentes facultados.

A estos efectos, tendrán la consideración de agentes facultados:

a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal.

c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia.

Artículo 7. *Procedimiento de cesión de datos.*

1. Los operadores estarán obligados a ceder al agente facultado los datos conservados a los que se refiere el artículo 3 de esta Ley concernientes a comunicaciones que identifiquen a personas, sin perjuicio de la resolución judicial prevista en el apartado siguiente.

2. La resolución judicial determinará, conforme a lo previsto en la Ley de Enjuiciamiento Criminal y de acuerdo con los principios de necesidad y proporcionalidad, los datos conservados que han de ser cedidos a los agentes facultados.

3. El plazo de ejecución de la orden de cesión será el fijado por la resolución judicial, atendiendo a la urgencia de la cesión y a los efectos de la investigación de que se trate, así como a la naturaleza y complejidad técnica de la operación.

Si no se establece otro plazo distinto, la cesión deberá efectuarse dentro de las setenta y dos horas contadas a partir de las 8:00 horas del día laborable siguiente a aquél en que el sujeto obligado reciba la orden.

Artículo 8. *Protección y seguridad de los datos.*

1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

2. Las obligaciones relativas a las medidas para garantizar la calidad de los datos y la confidencialidad y seguridad en el tratamiento de los mismos serán las establecidas en la Ley Orgánica 15/1999, de 13 de diciembre, y su normativa de desarrollo.

3. El nivel de protección de los datos almacenados se determinará de conformidad con lo previsto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo.

4. La Agencia Española de Protección de Datos es la autoridad pública responsable de velar por el cumplimiento de las previsiones de la Ley Orgánica 15/1999, de 13 de diciembre, y de la normativa de desarrollo aplicables a los datos contemplados en la presente Ley.

Artículo 9. *Excepciones a los derechos de acceso y cancelación.*

1. El responsable del tratamiento de los datos no comunicará la cesión de datos efectuada de conformidad con esta Ley.

2. El responsable del tratamiento de los datos denegará el ejercicio del derecho de cancelación en los términos y condiciones previstos en la Ley Orgánica 15/1999, de 13 de diciembre.

CAPÍTULO III

Infracciones y sanciones

Artículo 10. *Régimen aplicable al incumplimiento de obligaciones contempladas en esta Ley.*

El incumplimiento de las obligaciones previstas en esta Ley se sancionará de acuerdo con lo dispuesto en la Ley 32/2003, de 3 de noviembre, sin perjuicio de las responsabilidades penales que pudieran derivar del incumplimiento de la obligación de cesión de datos a los agentes facultados.

Disposición adicional única. *Servicios de telefonía mediante tarjetas de prepago.*

1. Los operadores de servicios de telefonía móvil que comercialicen servicios con sistema de activación mediante la modalidad de tarjetas de prepago, deberán llevar un libro-registro en el que conste la identidad de los clientes que adquieran una tarjeta inteligente con dicha modalidad de pago.

Los operadores informarán a los clientes, con carácter previo a la venta, de la existencia y contenido del registro, de su disponibilidad en los términos expresados en el número siguiente y de los derechos recogidos en el artículo 38.6 de la Ley 32/2003.

La identificación se efectuará mediante documento acreditativo de la personalidad, haciéndose constar en el libro-registro el nombre, apellidos y nacionalidad del comprador, así como el número correspondiente al documento identificativo utilizado y la naturaleza o denominación de dicho documento. En el supuesto de personas jurídicas, la identificación se realizará aportando la tarjeta de identificación fiscal, y se hará constar en el libro-registro la denominación social y el código de identificación fiscal.

2. Desde la activación de la tarjeta de prepago y hasta que cese la obligación de conservación a que se refiere el artículo 5 de esta Ley, los operadores cederán los datos identificativos previstos en el apartado anterior, cuando para el cumplimiento de sus fines les sean requeridos por los agentes facultados, los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, el personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, así como los funcionarios de la Dirección Adjunta de Vigilancia Aduanera.

3. Los datos identificativos estarán sometidos a las disposiciones de esta Ley, respecto a los sistemas que garanticen su conservación, no manipulación o acceso ilícito, destrucción, cancelación e identificación de la persona autorizada.

4. Los operadores deberán ceder los datos identificativos previstos en el apartado 1 de esta disposición a los agentes facultados, a los miembros de las Fuerzas y Cuerpos de Seguridad del Estado y de los Cuerpos Policiales de las Comunidades Autónomas con competencia para la protección de las personas y bienes y para el mantenimiento de la seguridad pública, o al personal del Centro Nacional de Inteligencia, así como a los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, cuando les sean requeridos por éstos con fines de investigación, detección y enjuiciamiento de un delito contemplado en el Código Penal o en las leyes penales especiales.

5. Sin perjuicio del régimen sancionador establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, constituyen infracciones a lo previsto en la presente disposición las siguientes:

a) Son infracciones muy graves tanto el incumplimiento de la llevanza del libro-registro referido, como la negativa a la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición.

b) Son infracciones graves la llevanza incompleta de dicho libro-registro, así como la demora injustificada, en más de setenta y dos horas, en la cesión y entrega de los datos a las personas y en los casos previstos en esta disposición.

6. A las infracciones previstas en el apartado anterior les será de aplicación el régimen sancionador establecido en la Ley 32/2003, de 3 de noviembre, correspondiendo la competencia sancionadora al Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información.

El procedimiento para sancionar las citadas infracciones se iniciará por acuerdo del Secretario de Estado de Telecomunicaciones y para la Sociedad de la Información, pudiendo el Ministerio del Interior instar dicho inicio.

En todo caso, se deberá recabar del Ministerio del Interior informe preceptivo y determinante para la resolución del procedimiento sancionador.

7. La obligación de inscripción en el libro-registro de los datos identificativos de los compradores que adquieran tarjetas inteligentes, así como el resto de obligaciones contenidas en la presente disposición adicional, comenzarán a ser exigibles a partir de la entrada en vigor de esta Ley.

8. No obstante, por lo que se refiere a las tarjetas adquiridas con anterioridad a la entrada en vigor de esta Ley, los operadores de telefonía móvil que comercialicen estos servicios dispondrán de un plazo de dos años, a contar desde dicha entrada en vigor, para cumplir con las obligaciones de inscripción a que se refiere el apartado 1 de la presente disposición adicional.

Transcurrido el aludido plazo de dos años, los operadores vendrán obligados a anular o a desactivar aquellas tarjetas de prepago respecto de las que no se haya podido cumplir con las obligaciones de inscripción del referido apartado 1 de esta disposición adicional, sin perjuicio de la compensación que, en su caso, corresponda al titular de las mismas por el saldo pendiente de consumo.

Disposición transitoria única. *Vigencia del régimen de interceptación de telecomunicaciones.*

Las normas dictadas en desarrollo del Capítulo III del Título III de la Ley 32/2003, de 3 de noviembre, continuarán en vigor en tanto no se opongan a lo dispuesto en esta Ley.

Disposición derogatoria única. *Derogación normativa.*

1. Quedan derogados los artículos 12, 38.2 c) y d) y 38.3 a) de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

2. Asimismo, quedan derogadas cuantas disposiciones de igual o inferior rango se opongan a lo dispuesto en esta Ley.

Disposición final primera. *Modificación de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones.*

La Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, se modifica en los siguientes términos:

Uno. El artículo 33 queda redactado de la siguiente forma:

«Artículo 33. *Secreto de las comunicaciones.*

1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias.

2. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes.

3. La interceptación a que se refiere el apartado anterior deberá facilitarse para cualquier comunicación que tenga como origen o destino el punto de terminación de red o el terminal específico que se determine a partir de la orden de interceptación legal, incluso aunque esté destinada a dispositivo de almacenamiento o procesamiento de la información; asimismo, la interceptación podrá realizarse sobre un terminal conocido y con unos datos de ubicación temporal para comunicaciones desde locales públicos. Cuando no exista una vinculación fija entre el sujeto de la interceptación y el terminal utilizado, este podrá ser determinado dinámicamente cuando el sujeto de la interceptación lo active para la comunicación mediante un código de identificación personal.

4. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímiles.

El acceso facilitado servirá tanto para la supervisión como para la transmisión a los centros de recepción de las interceptaciones de la comunicación electrónica interceptada y la información relativa a la interceptación, y permitirá obtener la señal con la que se realiza la comunicación.

5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación:

a) Identidad o identidades del sujeto objeto de la medida de la interceptación.

Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso.

b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica.
c) Servicios básicos utilizados.
d) Servicios suplementarios utilizados.
e) Dirección de la comunicación.
f) Indicación de respuesta.
g) Causa de finalización.
h) Marcas temporales.
i) Información de localización.
j) Información intercambiada a través del canal de control o señalización.

6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos:

a) Identificación de la persona física o jurídica.
b) Domicilio en el que el proveedor realiza las notificaciones.

Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes:

c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado).
d) Número de identificación del terminal.
e) Número de cuenta asignada por el proveedor de servicios Internet.
f) Dirección de correo electrónico.

7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada.

8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas.

9. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio.

10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles.

Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación.»

Dos. El último párrafo del apartado 5 del artículo 38 pasa a tener la siguiente redacción:

«Lo establecido en las letras a) y d) del apartado 3 de este artículo se entiende sin perjuicio de las obligaciones establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

Tres. En el artículo 53, se modifican los párrafos o) y z), que quedan redactados de la siguiente forma:

«o) El incumplimiento deliberado, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de esta Ley y el incumplimiento deliberado de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones.»

«z) La vulneración grave o reiterada de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, y el incumplimiento grave o reiterado de las obligaciones de protección y seguridad de los datos almacenados establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.»

Cuatro. En el artículo 54 se modifican los párrafos ñ) y r), que quedan redactados de la siguiente forma:

«ñ) El incumplimiento, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de la presente Ley y el incumplimiento de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, salvo que deban considerarse como infracción muy grave, conforme a lo dispuesto en el artículo anterior.»

«r) La vulneración de los derechos previstos en el artículo 38.3, salvo el previsto por el párrafo h), cuya infracción se regirá por el régimen sancionador previsto en la Ley 34/2002, de 11 de julio, y el incumplimiento de las obligaciones de protección y seguridad de los datos establecidas en el artículo 8 de la Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, salvo que deban considerarse como infracción muy grave.»

Disposición final segunda. *Competencia estatal.*

Esta Ley se dicta al amparo de lo dispuesto en el artículo 149.1.29.ª de la Constitución, que atribuye al Estado la competencia exclusiva en materia de seguridad pública, y del artículo 149.1.21.ª, que confiere al Estado competencia exclusiva en materia de telecomunicaciones.

Disposición final tercera. *Desarrollo reglamentario.*

Se habilita al Gobierno a dictar cuantas disposiciones sean necesarias para el desarrollo y ejecución de lo previsto en esta Ley.

Disposición final cuarta. *Formato de entrega de los datos.*

1. La cesión a los agentes facultados de los datos cuya conservación sea obligatoria, se efectuará en formato electrónico, en la forma que se determine por Orden conjunta de los Ministros de Interior, de Defensa y de Economía y Hacienda, que se aprobará en el plazo de tres meses desde la entrada en vigor de esta Ley.

2. Los sujetos obligados a los que se refiere el artículo 2 de esta Ley, tendrán un plazo de seis meses desde la entrada en vigor de la misma para configurar, a su costa, sus equipos y estar técnicamente en disposición de cumplir con las obligaciones de conservación y cesión de datos.

Disposición final quinta. *Entrada en vigor.*

Esta Ley entrará en vigor a los veinte días de su publicación en el «Boletín Oficial del Estado».

Por tanto,
Mando a todos los españoles, particulares y autoridades que guarden y hagan guardar esta ley.

Madrid, 18 de octubre de 2007.

JUAN CARLOS R.

El Presidente del Gobierno,
JOSÉ LUIS RODRÍGUEZ ZAPATERO

MINISTERIO DE DEFENSA

18245 *ORDEN DEF/3033/2007, de 11 de octubre, por la que se modifica el despliegue de la Unidad Militar de Emergencias, que figura en el anexo IV del Real Decreto 416/2006, de 11 de abril, por el que se establece la organización y el despliegue de la Fuerza del Ejército de Tierra, de la Armada y del Ejército del Aire, así como de la Unidad Militar de Emergencias.*

El Real Decreto 416/2006, de 11 de abril, por el que se establece la organización y el despliegue de la Fuerza del Ejército de Tierra, de la Armada y del Ejército del Aire, así como de la Unidad Militar de Emergencias (UME), atribuye al Ministro de Defensa la competencia para establecer los planes de transición a las nuevas estructuras de la Fuerza de los Ejércitos, y le autoriza a modificar la estructura orgánica y el despliegue que figuran en sus anexos. En virtud