Universitat Autònoma
de Barcelona

Máster de Investigación en Periodismo y Comunicación
Dpto. de Periodismo y de Ciencias de la Comunicación
Facultad de Ciencias de la Comunicación

LA PRIVACIDAD EN EL ESCENARIO DIGITAL.

Análisis de la política de la Unión Europea para la protección de datos de la ciudadanía.

TRABAJO FINAL DE MÁSTER

Lorena CANO ORÓN

Dirigido por
Dra. Carmina CRUSAFON BAQUÉS

Bellaterra, 26 de Junio de 2014

Cuando alguien tomaba una decisión,
estaba zambulléndose en una poderosa corriente
que llevaba a la persona hasta un lugar
que jamás hubiera soñado en el momento de decidirse.

El alquimista. Paulo Coelho

AGRADECIMIENTOS

A mi directora, la Dra. Carmina Crusafon, por ayudarme a crecer.
Al Dr. Xavier Salla por hacer más entendible el derecho.
Al Dr. Chema Alonso, por su atención.
A Laura Rahola, por su tiempo y dedicación.
A mis amigas de derecho, en especial a Marta Pérez, por su paciencia.
A mi padre, por transmitirme sus ganas de saber.
A mi madre, por enseñarme a ver los pequeños detalles.
A mi familia, por su apoyo incondicional.
A mis floras, que a pesar de la distancia siempre han estado ahí.
A Raül Giró, por ser fuente inagotable de consejos.
A Lidia Valera, por ser esa voz de la experiencia que
me pone los pies en la tierra, por sus ánimos y su comprensión.
A mis investigadores clandestinos;
en especial a Marta Portalés y a Isa Villegas por hacerme ver que no estaba sola.
A Elisa Serrano y a Laura Monsalve por compartir algo más que un piso.

ÍNDICE

ÍNDICE DE TABLAS E ILUSTRACIONES

INTRODUCCIÓN

Internet ocupa un gran protagonismo en la sociedad actual tanto en el ámbito laboral como en el personal. La esfera digital se ha convertido en ese lugar de reunión en el que no sólo encontramos toda la información que necesitamos, sino que además realizamos aportaciones personales, precisamente por el carácter interactivo que fomenta la red. Es entonces cuando aparece la preocupación por la imagen digital, y más concretamente, por la huella digital. Ya no se trata sólo de qué datos hay de una persona en el plano virtual, sino de qué tipo de privacidad existe y qué medidas se pueden adoptar tanto para preservarla como para reivindicarla.

La cultura de compartir[1] es propia de la filosofía nativa de la red. Hace referencia a la idea de publicar para todos los públicos cualquier tipo de información que se considere relevante, ya sea de interés general o personal (Castells, 2012, Jarvis, 2012, Clay Shirky, 2012 y Han, 2013). Este modo de actuación resulta positivo en lo que respecta a la liberalización de información en la red y las oportunidades de creación y colaboración en grandes proyectos; pero por otro lado, también supone introducir y producir mucha información sobre uno mismo en la esfera digital. Teniendo en cuenta que en la Sociedad de la Información[2], denominada también sociedad de la exposición (Han, 2013), es cada vez más fácil recoger datos, ya sea por las metodologías de extracción de datos o por la publicación en abierto de contenido, es importante saber cuáles son los límites de la legalidad y los fines para los que son recogidos. Además, el ciudadano debe ser consciente de que no sólo somos portadores de nuestros propios datos, sino que también somos propietarios de todos aquellos que hemos capturado o recogido de nuestros contactos (nombre, imagen, número de teléfono, e-mail, dirección postal, etc.), que quedan almacenados en cualquier dispositivo electrónico, como pueda

[1] No existe un consenso por parte de los autores para denominar la "cultura de compartir". Jarvis (2012), se refiere a este concepto como "publificación", mientras que otros autores describen el fenómeno sin etiquetarlo. En este trabajo, la terminología escogida es "cultura de compartir" (utilizada por Castells, 2012) debido a la descripción del concepto que conlleva el propio nombre. De hecho, esta terminología también puede encontrarse escrita en otros textos pero con un artículo determinado: cultura del compartir.

[2] Hay autores que matizan la diferencia entre Sociedad de la Información y Sociedad del Conocimiento, otros también denominan al mismo concepto como aludiendo a alguna característica o consecuencia de esta sociedad, como son las terminologías Sociedad de la Exposición, Sociedad del Espectáculo, Sociedad de la Transparencia, Sociedad de la Revelación o Sociedad del Control, entre otras. No obstante, en este trabajo, no se harán matizaciones entre los términos y éstos serán utilizados de forma sinónima, aunque son elegidos deliberadamente atendiendo a la connotación de cada vocablo.

ser una agenda electrónica, un Smartphone o una cuenta en una red social (Llácer Matacás, 2011).

Estos datos que poseemos adquieren cierta relevancia puesto que nos permiten identificar al sujeto al que aluden. Los datos personales son la nueva mercancía con la que se comercia en Internet, precisamente por los nuevos avances técnicos que están permitiendo explotar esa información para conseguir distintos objetivos. La existencia de software diseñado específicamente para la recolección de información y elaboración posterior de patrones de conducta así como la nueva tecnología especializada que aumenta su capacidad de captación y gestión de la información "cuestiona la capacidad de la legislación de protección de datos personales para tutelar la libertad informativa" (Llácer Matacás, 2011: 63).

Como consecuencia, aumenta la brecha informativa entre el usuario y el prestador de servicio que capta y procesa los datos. Esto es debido al desconocimiento por parte del sujeto del tratamiento de sus datos y la forma de controlar todo el proceso. De esta manera, sólo el responsable del tratamiento está totalmente informado. "El responsable del tratamiento define los criterios, crea los perfiles, dispone los medios de captación y aplicación en función de sus intereses, poniendo de manifiesto un desequilibrio estructural del sistema" (Llácer Matacás, 2011: 69) Es decir, el silencio y la poca información clara y precisa del tratamiento de los datos personales provoca una situación de desigualdad.

Mientras que las grandes bases de datos y la captación automática de información le quita el poder al usuario, el Derecho y sus recursos jurídicos deberían devolverles el control de su información personal. Se necesita crear nuevos instrumentos jurídicos y técnicos que estén realmente al alcance del usuario, que posibiliten otras formas de tutela del derecho o un reglamento del sistema del tratamiento que garantice "un acceso del usuario sobre su funcionamiento para adecuarlo ad hoc a sus preferencias" (Llácer Matacás, 2011: 64).

Justamente, en contra de todo pronóstico, hace justo un mes, en mayo de 2014, el Tribunal de Justicia de la Unión Europea se ha pronunciado a favor de la Agencia Española de Protección de Datos y del demandante al Derecho al Olvido, obligando a al gran gigante de Internet, Google, a facilitar a sus usuarios una solicitud a partir de la cual dispongan de la facilidad de eliminar el enlace a cierta información indeseada por

los afectados de su lista de resultados. Esto representa, por un lado, la importancia y actualidad de la seguridad, presente en todas las esferas. Y, por otro lado, la situación de vulnerabilidad en la que nos encontramos los usuarios de Internet.

I. Objeto de estudio: La privacidad digital y la protección de datos personales

El contexto tecnológico y digital que caracteriza la Sociedad de la Información ha provocado una serie de cambios de comportamiento y de los valores de la ciudadanía. El objeto de estudio de esta investigación es la privacidad digital, centrada en el marco legislativo del derecho de la protección de datos, que representa una de las consecuencias derivadas de la cultura emergente de la nueva esfera pública digital. La cultura del compartir y de la transparencia sumadas a la estructura de la red hacen posible la pérdida de privacidad e incluso el control de la actividad digital por personas ajenas. Por un lado, adoptando una perspectiva sociológica, se estudian las características del nuevo entorno y en las nuevas formas de actuación en la red, que difieren del código de conducta que se practica en el plano real. De esta forma, el trabajo se centra en las nuevas tendencias que siguen los usuarios de la red, aquellas que ponen en riesgo la privacidad publicando información personal que jamás antes se habría predicado en un espacio público. Por otro lado, se analiza la vertiente legal al respecto. Las instituciones democráticas quieren regular la extracción y utilización de datos por actores externos que realizan tales prácticas ya sea por aumentar sus beneficios económicos o para establecer una vigilancia de los individuos. En concreto, el estudio se enmarca el derecho de la protección de datos dentro de la política de la Unión Europea, examinando la regulación establecida vigente y los cambios que se pretenden realizar en un futuro próximo.

II. Planteamiento del problema de investigación

a. Objetivos

El interés de este estudio es realizar una descripción del espacio público digital y de la situación de la privacidad en Internet desde la perspectiva del usuario. Centrándose en la protección de datos personales, el objetivo principal del proyecto es conocer la legislación referente y su aplicación dentro de la política pública de la Unión Europea.

Los objetivos específicos del trabajo de investigación son:

- Definir el concepto de espacio público en el escenario mediático digital

- Definir el concepto de intimidad y privacidad en Internet
- Describir la adaptación del marco jurídico al nuevo entorno digital
- Analizar el marco legal de protección del espacio público en el seno de la UE
- Explicar la política europea de protección dentro de la estrategia Europa 2020

b. Preguntas de investigación

Las preguntas de investigación que guían la realización de este estudio parten de un interés general, que cuestiona la estructura y las características del nuevo espacio público, y se concretan en la política de la Unión Europea relativa a la protección de datos, como se puede ver a continuación:

1- ¿Cómo definimos el espacio público en Internet?

2- ¿Cómo está afectando la digitalización a la noción de privacidad e intimidad?

3- ¿Cómo se está adaptando el marco jurídico de la protección de datos al nuevo entorno digital?

4- ¿Cómo define e implementa la Unión Europea la protección de datos de la ciudadanía?

5- ¿Dónde está enmarcada dentro de las políticas europeas?

c. Justificación de la investigación

La tecnología digital ha provocado cambios fundamentales en el concepto de privacidad. Los límites entre la intimidad y la esfera pública cada vez son más difusos en Internet, sobre todo si nos fijamos en el protagonismo creciente de las redes sociales. Por una parte, la concepción de espacio público también ha cambiado, la esfera digital toma un rol central en la generación de la opinión pública. Por otra, existen distintas manipulaciones, unas voluntarias y otras involuntarias, que alteran la visión del espacio público digital. Se trata de una personalización de la red a partir de la filtración de datos, una técnica utilizada por buscadores comunes como Google, que identifica e individualiza a las personas ofreciendo aquello que él cree que tienen que ver (Jarvis, 2012; Bozdag, 2013; Thurman y Schifferes, 2012). El conocimiento de este tipo de

técnicas, invisibles para el usuario común, es crucial para la ciudadanía, ya que todos somos afectados del tratamiento de datos que se realiza en la red.

La sociedad digital puede convertirse en la sociedad vigilada. Son muchos los autores que ya advierten del control excesivo que se puede realizar de cada usuario de Internet (Bauman y Lyon, 2013; Solove, 2006 y 2008; Morozov, 2012; Ragneda, 2011). La legislación actual no cubre las nuevas necesidades de la ciudadanía que han surgido a raíz de los avances tecnológicos, concretamente en los avances de la minería y registro de los datos. Es necesario readaptar el marco jurídico a las nuevas demandas y al nuevo espacio público con la finalidad de proteger a la ciudadanía en el plano virtual.

Tras el análisis del marco de acción actual en la red, la investigación se centra en la perspectiva legal relativa a la protección de datos. Ésta se aborda tomando como muestra la política pública de protección de la Unión Europea, debido al peso legislativo del que dispone al determinar la regulación de 28 países y de más de 500 millones de habitantes. Además, la política pública de la Unión Europea relativa a la protección de datos representa un punto de vista singular, ya que difiere en gran medida del resto de políticas adoptadas por otros países, como pueda ser la adoptada en EEUU. Asimismo, se analizan las políticas europeas que remiten a la protección de datos con la intención de definir el estado actual de protección y acción que tiene el ciudadano.

Los derechos que cubren la esfera digital están en constante cambio a pesar de que el ritmo de adaptación del marco jurídico es bastante lento. Teniendo el importante papel que tiene Internet en la actualidad, conocer en qué medida estamos protegidos cuando nos conectamos a la red y qué derechos nos corresponden es vital para garantizar la seguridad digital. A raíz de las nuevas necesidades de protección de los ciudadanos, hace justo un mes, el Tribunal de Justicia Europeo (TJUE) dictaba una sentencia en la que se reconocía por primera vez el derecho al olvido en la red. Este hecho no sólo confirma el avance de los usos y tecnologías de la red, que obligan a crear nuevos derechos que garanticen la seguridad de los ciudadanos; sino que también verifica el grado de importancia que tiene tanto para los usuarios como para la UE asegurar la privacidad en la era digital.

III. Marco teórico

El marco teórico en el que se inscribe este estudio es en el ámbito de las políticas de la comunicación. Este ámbito académico tiene sus orígenes en la década de los años 1970 y desde entonces forman parte de las acciones gubernamentales de los Estados (Crusafon, 2012: 90-94). En esta área de conocimiento se investigan las políticas públicas analizando los actores que realizan la política, es decir, las autoridades públicas y las acciones concretas que un gobierno ejecuta (Kauffer, 2002). Hay que entender como políticas públicas los "procesos de decisión y actuación llevados a cabo principalmente por instituciones públicas, los cuales están orientados a la detección de un problema y a la definición de unos objetivos vinculados a su resolución, para cuya consecución se concretan tanto los recursos a emplear como los mecanismos de intervención a implementar. Todo ello con la pretensión de satisfacer el interés general y beneficiar al conjunto de la sociedad" (Suárez Candel, 2009: 28)

En el caso concreto de las políticas de comunicación como disciplina de estudio, supone un estudio multidisciplinar que relaciona la Ciencia Política, la Estructura de la Información, la Comunicación y el Desarrollo, el Derecho y la Economía Política de la Comunicación. Las políticas de comunicación "deben ser pensadas como respuesta a una compleja y mudada realidad que condiciona ciertas bases de desarrollo y modelos de mediación cultural específicos, en función del contexto histórico-social." (Sierra, 2006: 28)

Siguiendo la evolución de las políticas de comunicación presentada por Van Cuilemburg y McQuail (2003), este trabajo destaca por analizar aspectos relativos a la digitalización del espacio público que suponen nuevos retos para las políticas públicas. Asimismo se enmarca en el análisis de las políticas públicas europeas desarrolladas en el ámbito supraestatal. Sigue los trabajos realizados por distintos académicos europeos como Cullell-March (2010), Crusafon (2012), Pauwels et al. (2009), Sarikakis (2007), Suárez Candel (2009), entre otros, que han analizado con detalle las diferentes políticas europeas relativas a la implantación de la tecnología digital, ya sea en el ámbito audiovisual, televisivo, o del espectro radioeléctrico.

El emplazamiento de esta investigación en el marco teórico de políticas de la comunicación se debe fundamentalmente a que es la perspectiva desde la que se puede plantear un estudio de las políticas de protección del ciudadano, en este caso de la

seguridad digital y salvaguardia de la privacidad, analizando todos los elementos que hacen posible el actual estado de regulación social.

IV. Metodología

Esta investigación es de carácter descriptivo y exploratorio, con ella se pretende conocer el funcionamiento de la esfera pública digital y la política relativa a la protección de datos personales en la red. Debido a los objetivos que se persiguen y el marco de la investigación en el área de conocimiento de políticas de la comunicación, se aplica la metodología propia de esta disciplina.

Se ha realizado una amplia revisión bibliográfica multidisciplinar, concretamente se abarca el campo de conocimiento de la sociología, el periodismo, la ciencia política, el derecho y la ingeniería informática, debido a la interrelación existente entre ellas al trabajar la temática de la protección de datos. Esta revisión documental tenía por objeto identificar también el *material secundario* (Just & Puppis, 2012) que existe al respecto del objeto de estudio, que ofrece interpretación sobre los documentos principales que lo regulan.

Posteriormente, se procedió a realizar un análisis documental multidisciplinar, en el que se analizan las políticas de protección de datos de la Unión Europea. Mediante la revisión e interpretación de documentos primarios y segundarios se describe la política correspondiente. Para poder complementar la información, se recurrió a la realización de entrevistas semi-estructuradas a expertos del objeto de investigación de este trabajo y a personas relevantes que tienen relación directa con las políticas europeas. La intención era la de contrastar y ampliar la información obtenida en la revisión documental a partir de fuentes directas expertas en la materia de protección de datos.

Las estrategias para validar las consultas a expertos han sido, por un lado, la formulación de preguntas –primero realizar preguntas abiertas que le den libertad al experto a encauzar el tema por donde él crea conveniente y después realizar más cuestiones centradas en los problemas que se quieren abordar - y, por otro, la triangulación –buscar otras fuentes de información como informes internos, conferencias, páginas webs u otro tipo de fuentes que corroboren lo que se dice y que ayuden a completar el contexto de la información producida en la entrevista- (Just y Puppis, 2012).

En concreto, los expertos consultados han sido los siguientes:

- Xavier Salla, doctor en Comunicación Audiovisual y Publicidad y abogado especializado en la protección de datos. Actualmente es profesor asociado en el Departamento de Periodismo y Ciencias de la comunicación de la Universidad Autónoma de Barcelona.

- Chema Alonso, doctor en Ingeniería Informática y hacker profesional. Es director del Master de Seguridad de la Universidad Europea de Madrid y profesor de los Masters de Seguridad de la Universidad Oberta de Catalunya y de la Universidad Politécnica de Madrid.

- Laura Rahola, responsable de prensa de la representación de la Comisión Europea en Barcelona.

Las consultas a expertos han permitido verificar y complementar los conocimientos sobre las áreas del derecho, la ingeniería informática y las distintas percepciones en el proceso de tomar decisiones y formular políticas que se escapan de la perspectiva de la comunicación que se adopta en este trabajo. Como resultado de la aplicación de esta metodología se ha elaborado el siguiente estudio.

V. Estructura de trabajo

Esta investigación está dividida en tres capítulos. El primero realiza una descripción de la esfera pública digital. Se enmarca en el contexto de la Sociedad de la Información y expone las características del nuevo espacio público en el que Internet representa un papel principal, abordando no sólo aquellas más técnicas, sino también aquellas que desde una perspectiva más sociológica lo caracteriza, como es el papel de la intimidad o la privacidad en la red.

Se establece una tipología de espacios que atienden a la personalización de la red, haciendo referencia a los mecanismos que individualizan la visión del espacio público digital. En concreto, se hace referencia tanto a los individuos que filtran la información atendiendo a sus intereses como a los motores de búsqueda como Google, que usan los datos que recogen de sus usuarios para configurar un espacio que se adecúe a su perfil. Asimismo, se exponen los peligros que surgen en el nuevo entorno, partiendo de la descripción del concepto de la huella digital como base para explicar las metodologías de extracción de datos, tales como el *data mining*. De este modo se aborda el riesgo que

supone la vigilancia y el control digital para la sociedad red. Este primer capítulo concluye con la descripción de los nuevos valores de la cultura digital, haciendo especial referencia a la cultura de compartir.

En el segundo capítulo se centra en la dimensión jurídica de la protección de datos. Se analiza un conjunto de derechos de la personalidad que están relacionados con el objeto de estudio. En concreto, el derecho a la imagen, a la intimidad personal y familiar y de autodeterminación informativa, ya que son aquellos que protegen la privacidad del individuo y sirven de base para el derecho de protección de datos, que es desarrollado en segundo lugar. Asimismo, se aborda el concepto del derecho al olvido, como un nuevo derecho originado a raíz del uso de Internet como herramienta cotidiana interdisciplinar. Se expone el caso que provoca el reconocimiento de este derecho por el TJUE.

Finalmente, el tercer capítulo se centra en la política de la Unión Europea para la protección de datos. Se explica quiénes son los actores responsables de esa política, cómo se define, con qué instrumentos cuenta y quien la aplica y la controla. Asimismo, se describe de la situación actual, en la que se está debatiendo la reforma que se ha elaborado por la Comisión Europea Barroso II, cuyo interés es ampliar la normativa para salvaguardar la privacidad del ciudadano mediante la inclusión de nuevos derechos y nuevas sanciones. Además, también se explica el programa de acción previsto para un futuro próximo dentro de la estrategia Europa 2020, concretamente aquellas iniciativas y objetivos que están relacionados con la privacidad, la seguridad digital y la protección de datos.

CAPÍTULO 1

EL NUEVO ESPACIO PÚBLICO: INTERNET Y LAS NUEVAS TECNOLOGÍAS

La revolución tecnológica ha supuesto un desarrollo social y ha cambiado radicalmente el paradigma que constituía la sociedad de masas. La actual Sociedad de la Información y/o del Conocimiento se caracteriza por el uso de las nuevas tecnologías y de Internet y por facilitar el acceso a la información (Castells, 2013). La convergencia tecnológica, la digitalización y la democratización del uso de Internet ha transformado nuestra manera de consumir y producir información, e incluso de entender la comunicación (Serrano, 2013). La *World Wide Web* es el espacio público actual de referencia. El debate sobre esta cuestión en el texto será en torno a sus límites respecto a la esfera privada.

En este capítulo presenta una aproximación sociológica y conceptual. En primer lugar, se sitúa el contexto socio-técnico que enmarca este trabajo, concretamente, la Sociedad de la Información. En segundo lugar se presenta Internet como espacio público digital, describiendo sus características y definiendo una tipología propia de espacios personalizados. Seguidamente se identifican los peligros relacionados con la esfera pública digital desde la perspectiva de la privacidad, explicando conceptos como la huella digital, las *cookies* y las metodologías de extracción de datos como puntos clave en este paradigma. Finalmente, se abordan los nuevos valores de la cultura digital, en concreto, la cultura de compartir.

1.1. La Sociedad de la Información

Con la democratización de las nuevas tecnologías, la llegada masiva de Internet y, en general, la incorporación de las innovaciones científicas[3] a la realidad cotidiana, la sociedad ha evolucionado de la Sociedad de Masas o Sociedad Industrial, a la Sociedad de la Información y/o del Conocimiento. Las tecnologías no solo son nuevos mecanismos que nos sirven para comunicarnos, sino que han contribuido a cambiar el mismo concepto de sociedad. "Actualmente, las principales actividades económicas,

[3] Una de las características relevantes de la Sociedad de la Información es la incorporación de las innovaciones científicas, desarrolladas originalmente para otros propósitos como pueda ser la carrera espacial, a la realidad cotidiana. Ejemplos de estos avances puede ser el velcro, los pañales para los bebés, el microondas, etc.

sociales, políticas y culturales de todo el planeta se están estructurando por medio de Internet" (Castells, 2001: 17).

La Sociedad de la Información ha cambiado conceptos básicos como el espacio y el tiempo. Está directamente relacionada con la idea de globalización. Formar parte de esta sociedad supone pertenecer a un mismo sitio, tener un lugar común, teniendo esto como consecuencia una sensación de reducción de distancias. Pero este lugar no sólo es Internet, que en mayor medida lo es, sino también el mundo. La digitalización y la convergencia tecnológica han permitido reducir el espacio que nos separaba de los acontecimientos que ocurren en cualquier lugar del planeta. Estamos ante esa sociedad que preconizaba McLuhan (1995), la aldea global, o Mattelart (1993), con su "ciudad global", en la que todos estamos comunicados mediante herramientas tecnológicas, en la que los ciudadanos dependemos de ellas para poder sentirnos comunicados. Con la reducción del coste y tiempo del transporte y la comunicación instantánea permanente, el mundo ha quedado al alcance de cualquiera. Ahora existe el transporte *low cost*, las posibilidades de intercambio, tanto de estudiantes como de turistas, ha aumentado (intercambio de casas, programas universitarios de intercambio, etc.). Ahora es más fácil mantener una relación a distancia, tener amigos internacionales (básicamente porque cuesta casi lo mismo que mantener una relación con una persona que viva físicamente cerca).

Si nos centramos en la vertiente comunicativa personal, se ha transformado nuestra manera de comunicar y relacionarnos. "Internet permite acercar el contenido deseado y especializado al consumidor de la información, generando nuevos tipos de comunicación interpersonal y redefiniendo la comunicación de masas" (Llorca, 2005: 28). Se ha conseguido la inmediatez en el envío y recepción de información, la creación de lugares virtuales como punto de encuentro (redes sociales), una conexión con todo el mundo, reduciendo las distancias y permitiendo llegar a un público masivo, desde un dispositivo móvil que se puede llevar permanentemente encima. La tecnología hace que las relaciones humanas varíen, las formas de comunicarnos se amplíen y tengamos que aprender nuevos conceptos, actitudes y formas de comportarnos. Las aplicaciones informáticas que permiten estar conectados las 24 horas del día tanto a nuestra vida privada como laboral consiguen que se experimente una especie de *omnipresencia virtual* en la que no existen fronteras. La sociedad de la información ha implantado una *obligación* de interactividad constante.

"La actividad más importante en Internet actualmente pasa por los servicios de redes sociales (SNS), y los SNS se han convertido en plataformas para todo tipo de actividad, no sólo de amistad personal o para charlar, sino para el marketing, el comercio electrónico, la educación, la creatividad cultural, la distribución de los medios de comunicación y entretenimiento, aplicaciones para la salud y , por supuesto, el activismo sociopolítico. Los SNS son espacios vivos que conectan todas las dimensiones de la vida de la gente. Ésta es una importante tendencia para toda la sociedad. Transforma la cultura induciendo una cultura de compartir." (Castells, 2012: 221)

La Sociedad de la Información también ha sido denominada *sociedad red* precisamente por ese espacio virtual de conexiones que establece, que es el resultado de combinar las Tecnologías de la Información y la Comunicación (TIC) con las comunicaciones tradicionales. "El mundo real de nuestra época es un mundo híbrido, no un mundo virtual ni un mundo segregado que se separará online de la interacción offline" (Castells, 2012: 222). La sociedad red es caracterizada también por la creación de comunidades virtuales, redes de comunicación con nuevos patrones de interacción, con una *libertad* sin precedentes, tanto a la hora de emitir como a la de responder. Majó define Internet no como un medio, sino como "un espacio de comunicación como lo fue el ágora (…). Es entrar en un espacio en el que poder encontrar muchas cosas. Es cambiar los hábitos a la hora de informarse, la manera de comunicarse, la manera de establecer las relaciones sociales, la manera de vivir en comunidad." (Majó, 2012: 75)

1.1.1. La nueva esfera pública: el rol central de Internet

El concepto de espacio público designa dos acepciones relacionadas entre sí. El término hace referencia, por un lado, a la noción urbanística de espacios comunes, a los espacios culturales públicos, que sería todo espacio urbano no-privado: calles, plazas, parques, etc.; todo aquel espacio comprendido entre lo privado y lo estatal. Y, por otro lado, el vocablo también alude a un significado político-filosófico, determina la esfera pública como aquel espacio de deliberación democrática en el que cualquier individuo puede participar (Aramburu, 2008).

Ambos significados convergen en una idea subyacente: el espacio público como lugar de debate de las cuestiones de interés público con su consecuente formación de una opinión pública, pero en el más sentido más funcional. Es decir, no de una forma pasiva

y posterior a las decisiones tomadas por los poderes estatales (Almeida, 2002), sino donde "se procede al debate previo de las cuestiones que posteriormente tienen que ser decididas mediante los mecanismos propios de las democracias representativas como las modernas" (Salvat y Serrano, 2011: 76). Ante la ausencia de una definición de espacio público digital, esta investigación propone: la esfera pública digital como todos los portales web de libre acceso que conforman la red y que tienen como objetivo ser un medio para que la ciudadanía pueda comunicarse y debatir sobre las cuestiones de interés actuales. Se trata pues de una trasposición de las ideas tradicionales del espacio público al plano virtual.

Se identifica el origen del concepto de espacio público con la clase burguesa a finales de la Edad Media. Con la introducción del sistema capitalista financiero y mercantil y el incremento de cambio de mercancías e información, la burguesía, cada vez más letrada, comienza a querer ganar poder político, hecho que le lleva a crear espacios públicos de discusión con objetivo de crear una opinión pública que fuera afín a sus intereses. Habermas, filósofo y sociólogo alemán, define estos orígenes del espacio público con el capitalismo y la burguesía, pero reconoce "la existencia histórica de otras versiones, como el espacio público plebeyo, el helénico y el espacio de representación pública feudal." (Almeida, 2002: 2)

Se distinguen tres fases de evolución del espacio público. La primera corresponde a los primeros lugares de debate y reunión y al inicio de la prensa. La segunda se relaciona con la invención de los grandes medios de comunicación en el s. XX (radio, cine y televisión), que a pesar de representar *la opinión pública,* la opinión de *todos,* del *pueblo,* "publican una opinión privada y no pública. Los medios, que deberían ser instituciones ejemplares del espacio público, se comercializan dentro de la lógica de transformar el público ciudadano en consumidor de mercancías" (Almeida, 2002: 4). En esta segunda fase, se puede afirmar que lo que hacen los medios es dar eco del espacio público burgués. La tercera fase, caracterizada por el nuevo espacio público que representa Internet, se presenta como una esfera pública más abierta o más accesible que la anterior, ya que se han multiplicado las voces que pueden acceder al debate. No obstante, algunos académicos afirman que Internet "no es un espacio público, pero es un instrumento inédito que contribuye para el debate público y la organización de la sociedad civil y de espacios públicos activos" (Almeida, 2002: 5).

Siguiendo a Henri Lefebvre, filósofo marxista francés, en su obra escrita en 1968 *El derecho a la ciudad*, el espacio público entendido como derecho a la ciudad, derecho a disponer y crear un lugar común, es un espacio comercializado, producido, estratégico. El espacio público responde a la ideología capitalista exclusivista, es decir, sirve para discriminar a los que no consideramos públicos, a los marginados sociales y a aquellos sujetos que padecen daños colaterales del sistema (Urzúa, 2012). En los primeros espacios públicos burgueses "eran excluidos las mujeres, los empleados y los jóvenes, que eran vistos como personas sin autonomía para decidir" (Almeida, 2002: 3); en los espacios mediáticos son discriminadas las voces de muchas minorías y tanto la información como el discurso que sostienen continúa dependiendo de los intereses de la burguesía, se trata pues de espacios públicos secuestrados. El espacio público, que debería ser un ámbito en el que cualquier diferencia, social, económica o cultural se disolviera posicionando a todas personas como iguales, no ha existido nunca. Esta visión queda relegada como un ideal imposible de cumplir hasta el momento, ya que el espacio público actual continua restringiendo el acceso "a los grupos menos favorecidos de la sociedad y que al mismo tiempo margina otras formas de vida pública diferentes a las dominantes" (Aramburu, 2008: 144)

Internet se acerca más al verdadero concepto de espacio público, porque es un espacio más abierto y más accesible, con más voces y más participación. No obstante, quizás acaba siendo un arma de doble filo para la democracia y la deliberación política. Según Sennett, sociólogo estadounidense, la democracia se consigue con el esfuerzo de los ciudadanos por conocer y cambiar el mundo en el que viven, por lo que si éstos se vuelven cómodos en el sistema consumista, el esfuerzo desaparece y con ello la democracia (Urzúa, 2012). Internet nos hace la vida cómoda y se corre el riesgo que todo lo que se debata o se critique desde la butaca se quede reducido a eso, a meros discursos que se pierden en un universo lleno de información.

A pesar de conformar un espacio público más accesible, la brecha digital existe. Retomando la idea de Lefebvre, Internet vuelve a ser un espacio público en el que se discrimina y se excluye a aquellas personas que no tienen un nivel económico suficiente como para permitirse formar parte de esta sociedad informatizada. No es un espacio con igualdad de condiciones a pesar de que hayan muchas herramientas gratuitas. No todos los portales web tienen la misma oportunidad de audiencia.

Es por estos motivos por los que no debemos caer en el error de pensar que el espacio público actual es neutro o que está conformado por todos. En Internet no sólo no se resuelve la desigualdad social sino que incluso cobran más fuerza otros conflictos, como la circulación de rumores, estafas, acoso, delitos cibernéticos, etc. que producen porque el infractor es consciente de cómo utilizar la red en su beneficio. La sociedad red debe concienciarse tanto del funcionamiento de las comunicaciones en Internet y la perspectiva individualizada que éste le ofrece como de quién tiene acceso a dichas publicaciones y a la propia red.

Como consecuencia del uso de esta nueva esfera, los límites entre el espacio público y el espacio privado se están erosionando. El hecho de que se haya trasladado la atención a este plano digital, una esfera nueva sin reglas preestablecidas, hace que la gente se encuentre desubicada y encontremos convergencias de espacios. La privacidad y la intimidad, naturales del ser humano, se trasladan a Internet con cambios significativos (Han, 2013).

El espacio privado determina la zona restringida y controlada por una persona o entidad en la que tienen lugar acciones o conversaciones particulares que son sólo accesibles a las personas autorizadas por el propietario o responsable del ámbito delimitado. Es decir, el espacio privado es aquella área en la que la persona realiza aquellas acciones que no quiere hacer públicas, donde puede transcurrir la intimidad. Mientras que el espacio público es aquello visible y accesible a todos, el espacio privado se define por lo contrario. Cuando se entra en el espacio privado las personas se sienten más cómodas, menos vigiladas, tienen libertad para ser ellas mismas. El espacio privado es aquel donde se permite ser "patético a gusto, pues solamente entre esas acogedoras paredes era posible dejar fluir libremente los propios miedos, angustias y otros patetismos considerados estrictamente íntimos" (Sibilia, 2008: 75).

La delimitación entre el espacio público y el espacio privado se forma en Europa los preludios de la Modernidad, en los siglos XVIII y XIX, debido al desarrollo de las ciudades y la sociedad industrial. El desarrollo del espacio privado fue debido a varios factores, como "la institución de la familia nuclear burguesa, la separación entre el espacio-tiempo de trabajo y el de la vida cotidiana, además de los nuevos ideales de domesticidad, confort e intimidad" (Sibilia, 2008: 73). El espacio privado surgió de la necesidad de un lugar donde sentirse seguro del mundo público y sus exigencias.

Los factores que propiciaron el espacio privado se encuentran actualmente en crisis. La aplicación de las nuevas tecnologías a la vida cotidiana la separación entre espacio-tiempo de la vida laboral y del ocio hacen que sea cada vez es más difuso; el modelo de familia nuclear burguesa comienza a desestructurarse y se fomenta la migración de forma positiva, tanto para seguir formándose como para trabajar, para convertir a las personas en seres globalizados. En lo que respecta a la intimidad, está comenzando a exhibirse, rompiendo así la separación entre el espacio público y el privado. Por esta razón, autores como el ensayista estadounidense Jonathan Franzen, reclaman una defensa del espacio público actual, debido a que "la intimidad parece haberse evadido del espacio privado y pasó a invadir aquel universo que antes se consideraba público" (Sibilia, 2009: 318).

El espacio privado, por su propia definición, estaría situado exclusivamente en un lugar físico donde el control de la situación y el contenido es más fácil de asegurar. Una esfera privada online podemos encontrarla de diversas formas, ya sea esa parte de las plataformas que facilitan la comunicación *exclusiva* entre dos personas (correo electrónico o mensajería *privada* entre usuarios de redes sociales), o foros con participación limitada, en la que los administradores controlan qué usuarios se pueden unir y a qué contenido pueden acceder o webs con contraseñas para áreas privadas, por ejemplo. Aunque, como se verá al final de este capítulo, en la red cualquier movimiento es rastreable y toda información que se comparta en Internet (ya sea con una sola persona o con varias) queda en el limbo informático y no se puede asegurar un control total de la información, ya sea por un descuido del usuario o por un ataque cibernético.

1.1.2. Características del nuevo espacio público

El nuevo modelo de comunicación en red se define por romper las barreras del espacio-tiempo que caracterizan a los medios tradicionales, ofrece instantaneidad, ruptura de la periodicidad, universalidad y capacidad de almacenamiento; se caracteriza por el lenguaje multimedia de la información, por la hipertextualidad y por la interactividad. Este cambio de paradigma ha desarrollado un sistema de transmisión descentralizado y abierto que no atiende a la jerarquía vertical propia de la sociedad de masas (López García, 2005 y 2006). El flujo de la información ahora es horizontal, que resulta la multidireccionalidad comunicativa. Se ha gestado un espacio virtual de intercambio en el que "las esferas públicas periféricas no sólo se han multiplicado en número, sino que han ganado en centralidad y en capacidad para elaborar sus propios mensajes y hacerlos

públicos, interactuando continuamente entre ellas e incluso con el poder, que pierde opacidad" (López García, 2006: 241). Consideramos el nuevo espacio mediático, con nuevas condiciones y nuevas oportunidades, como una esfera pública donde los productores de información no son sólo las grandes empresas mediáticas, sino también los ciudadanos. Internet se ha convertido en el espacio público de referencia, en el que no sólo se consultan las noticias, se comentan y se aporta información. Se han establecido comunidades virtuales en las que se suman las aportaciones de sus miembros, llegando a formar "multitudes inteligentes" (Rheingold, 2004).

Una de las características de este nuevo espacio público es la facilidad de acceso a la información que permite Internet. Esto es, "el ámbito doméstico se ha convertido en el centro desde donde se tienden puentes con el mundo" (Wincour, 2001: 76). Esta concepción de Internet como esfera pública se debe a la adopción de distintas ideologías por parte de los creadores y usuarios de la red: la utopía comunicativa –la información fluye libremente-, la utopía política –ideología libertaría que apela a la no interferencia de los gobiernos-, la ideología activista –Internet para transformar la sociedad-, la utopía del conocimiento –ideología de software libre- y la autoorganizativa -que supone una síntesis de todas-. A pesar de sus ventajas, Internet también incorpora nuevos desafíos y peligros, como el riesgo que se corre al concebir Internet como espacio público, destacando la falsa concepción de que en Internet está todo el mundo –existencia de la brecha digital-, y la ignorancia por parte de los usuarios que creen que su actividad y su correspondencia privada permanece invisible y no se archiva en miles de ordenadores (Casacuberta, 2008).

Internet se caracteriza como un espacio donde todo tiene cabida, de hecho, es catalogado como exuberante, es decir, que se presenta como un conjunto de información inabarcable por una persona. Esta cantidad abrumadora de información heterogénea tiene como inconvenientes el sentimiento de desorientación que produce, ya que sin una educación específica, es difícil distinguir entre qué información es fiable y cual es susceptible de ser errónea. Además, el ritmo vertiginoso con el que se crean y se difunden los contenidos por la red fomenta esa necesidad de conexión permanente para poder estar actualizado.

El nuevo espacio público o esfera digital supone en primer lugar un proceso de individualización física, un aislamiento del medio que le rodea para contextualizarse en

aquello que está ocurriendo o quiere comunicar en la red. Pero, a la vez, supone un proceso de socialización constante que se efectúa mediante los dispositivos móviles o incluso desde los ordenadores a través de plataformas diseñadas para comunicarse, estableciendo una comunicación instantánea en distintos formatos (escrita, oral y/o audiovisual). Las relaciones sociales durante siglos se han basado en el contacto personal. Pero ahora ya no es así, muchas relaciones humanas se establecen solo a través de la tecnología.

Desde una perspectiva sociológica, los límites entre la privacidad y el espacio público digital se están diluyendo. El concepto de intimidad se replantea en un nuevo entorno digital adaptándose a la cultura de compartir que caracteriza Internet. Los límites entre la vida privada y la vida pública están siendo distorsionados. Un gran ejemplo de ello lo tienen los usuarios de la red al ver la actividad de sus contactos en cualquier red social. *Si no está publicado, no ha ocurrido*, podríamos decir que ese es el lema que se sigue en la red. Los contactos tienden a hacer público los datos propios de la vida íntima que les identifican, precisamente para poder ampliar su imagen digital y crear un perfil que se ajuste a su *yo real*. La filosofía es clara: cuanta más visibilidad mejor, cuantos más "me gusta" o más comentarios mejor. Jeff Jarvis (2012), profesor de periodismo en la City University de Nueva York, autor posicionado a favor de la *publificación*[4], afirma que esta tendencia aporta enormes beneficios, tales como el fomento de las relaciones, la facilidad para compartir, relacionarse y organizarse o el aumento del conocimiento de las personas. Asimismo defiende la naturaleza de este modo de actuar frente a la tecnología, insistiendo en que el grado que deseamos de intimidad está en nuestra mano.

Pero si analizamos el concepto de intimidad, podemos comprobar cómo los valores están cambiando y que no tiene sentido que se hable de grados de intimidad sino de privacidad. El concepto intimidad proviene del la palabra latina "intimus", que significa "zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia" (RAE, 2001), así como el derecho a estar solo, el derecho a la soledad. El concepto de intimidad hace referencia a pensamientos, actos y todos aquellos aspectos de nosotros mismos que no queremos compartir públicamente. "La intimidad se sitúa en el terreno oculto de cada persona, donde se forjan las decisiones más propias e intransferibles." (García Fernández, 2010: 271).

[4] Término acuñado por él que describe como compartir información, pensamientos o acciones a través de Internet (Jarvis, 2012)

Se puede dividir la intimidad en dos aspectos: la intimidad de la persona consigo misma y la intimidad de la persona con los otros. El primero abarca las reflexiones internas y la conciencia de uno mismo; mientras que el segundo acota los espacios y las personas con las que compartimos nuestra intimidad, construyendo así momentos y encuentros íntimos. Este tipo de intimidad se suele dar en tres áreas de la vida, la familiar, la de los amigos y la amorosa, pero con distintos matices (García Fernández, 2010).

En Internet, "la intimidad pierde fatalmente su valor al dejar de definirse por oposición a aquel otro espacio donde debería regir su contrario: lo no íntimo, el lugar donde ocurren los intercambios con los otros y la acción pública" (Sibilia, 2008: 88). Esto es debido principalmente a la nueva tendencia de publicar y compartir contenidos e información personal, que podríamos catalogar como íntima, en la red. Se muestra un comportamiento despreocupado y confesado, interesado por rellenar y definir su imagen digital a costa de hacer visible en la esfera virtual lo que quizás en la realidad offline no les habría sido de agrado difundir. "Las nuevas prácticas expresan un deseo de desbordar la propia intimidad, ganas de exhibirse y hablar de sí mismo para que todo el mundo vea y sepa 'quién soy yo'" (Sibilia, 2009: 318). La publicación de la intimidad en plataformas de Internet supone, por consiguiente, una mediatización de aquello íntimo y privado de la persona, tornando así esos contenidos en éxtimos, públicos y accesibles.

Por definición, aquellos contenidos que intentamos controlar en Internet no es intimidad sino privacidad. Intimidad mediada con una máquina no es intimidad. En cambio la privacidad como concepto define esa información, espacio o acto a los que pretendemos controlar su acceso; es decir, ese ámbito propio restringido que queremos proteger de aquellas personas a las que no permitimos su intromisión. Se trata pues de "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, 2010: 71).

La privacidad, que constituye un derecho inherente de la persona, supone "el derecho de mantener ciertos aspectos de la vida privada fuera del alcance de otros y, por lo tanto, el derecho a construir diferentes 'personalidades situacionales'" (Abril y Pizarro, 2014:8-9). En España, en particular, la palabra privacidad, que proviene de del término inglés

privacy, ha comenzado a utilizarse sobre todo para referirse al escenario digital, de hecho no fue incluida en la RAE hasta el 2001 (Salgado, 2010).

En la esfera digital podemos observar dos tipos de comportamientos en lo que respecta a la privacidad. "Por un lado, sigue vigente la celosa preservación de ciertos datos personales bajo señas y candados, contra posibles invasiones de la privacidad; sobre todo las informaciones bancarias y comerciales de los individuos. Por otro lado, se promueve una verdadera evasión de la privacidad en campos que otrora concernían a la púdica intimidad personal" (Sibilia, 2009: 317).

Aquello concebido como privacidad varía según la cultura, debido a que la calificación de espacios, hechos o pensamientos íntimos atiende a una variable sociocultural. La cultura propia de Internet está basada en compartir información, es por ello que autores como Jeff Jarvis (2012) defienden que los nativos digitales tienen otro concepto de intimidad y privacidad. Este autor pone ejemplo para ilustrar dicho condicionante: mientras que en EEUU las finanzas personales y la información sobre el estado de salud son datos privados, en Suiza lo son los ingresos y los impuestos. También realiza una comparación con las fotografías que se reparten de los delincuentes buscados, que en Alemania les cubren los ojos en las fotos y en otros estados se publican sin modificar nada. "El concepto refleja las relaciones entre los miembros de la sociedad y entre los gobiernos y los individuos" (Abril y Pizarro, 2014:7).

Los usuarios de redes sociales, a diferencia de las páginas web o los blogs, sí que pueden configurar y establecer las condiciones que prefieran de privacidad online. "La información es considerada por los participantes en las redes sociales como "privada" en tanto la misma no sea divulgada fuera de la red en la cual inicialmente fue difundida, si la misma fue originada entre ellos; o si la información no afecta la personalidad del internauta, si la misma fue originada por otros" (Abril y Pizarro, 2014:10).

Desde una perspectiva jurídica también podemos observar esa distinción. Para la Unión Europea, la privacidad es entendida como dignidad, "como un derecho humano a la vida privada, un derecho y valor sustantivos de primer orden" (Abril y Pizarro, 2014:7). Sin embargo, para los Estados Unidos, la privacidad es entendida como control sobre la información personal y como libertad, "la autonomía de decidir con quién compartirla (…) y escoger libremente quién tiene acceso a dicha información" (Abril y Pizarro, 2014:7).

La privacidad se ha ido erosionando conforme los usuarios se han adecuado al nuevo espacio público. El término "extimidad", concepto definido ya en 1958 por psicoanalista francés Jaques Lacan, se ha convertido en un perfecto descriptor de la realidad actual digital (Tello, 2013 y García Fernández, 2010). El término alude a la conducta que adoptan los usuarios de Internet al publicar contenidos que se podrían catalogar de íntimos o privados. Se trata de un fenómeno que se ha generalizado tanto en los blogs, las redes sociales, como programas de televisión (reality shows); en los que se muestra la intimidad a todos los públicos, tanto personas públicas como anónimas (García Fernández, 2010). Este fenómeno surgió antes del apogeo de las redes sociales, concretamente con el auge de los blogs, blogs de fotografías (fotologs) y blogs de vídeos (vlogs), en los que el tipo de contenido íntimo que se publicaba insertaba a los usuarios y lectores "en un modelo comunicativo que produce y reproduce continuamente la individualidad de acuerdo a los modos que va adquiriendo la exposición de la intimidad" (Dipaola, 2008: 3)

En las redes sociales se ofrece una gran cantidad de información a cambio de crear un perfil completo o una identidad digital que nos represente. En internet se publican los estados de ánimo, los pensamientos, los lugares en los que uno se encuentra –incluso se suben fotos para verificar la información-, la música que se escucha, los libros que se han leído, las noticias que nos llaman la atención y sus respectivas recomendaciones. También se publican los gustos, la biografía, el lugar de trabajo y residencia, e incluso el número de teléfono de contacto. La extimidad acaba siendo "una serie de intercambios de intimidades" (García Fernández, 2010: 281) sin tener el control absoluto de quién puede acceder a esa información. Se hace público esa parte íntima de cada de cada uno que permite describir y enriquecer la imagen digital que se configura en Internet.

Este tipo de discurso centrado en el "yo", en la parte íntima de cada uno, es "una novedosa forma de imponer lo íntimo como público, haciendo traslucir en eso un nuevo modo de experiencia social en donde lo visible asume el grado primordial de vinculación entre los múltiples participantes de una tal interacción comunitaria y comunicativa" (Dipaola, 2008: 1) Esta cultura de lo visible, de lo público, que está directamente relacionada con el ego de las personas, provoca que convirtamos nuestra vida en hechos noticiables. Comienza a estar bien valorado que la gente se publicite en la red, que muestre qué es lo que hace y qué es lo que le gusta (Tello, 2013), estamos

encaminados hacia la sociedad de la transparencia (Han, 2013). Esto supone la invasión del espacio público digital y la puntual convergencia de la esfera pública y privada, disolviéndose así la clara separación entre ambos espacios.

Es importante relacionar este fenómeno con el sistema capitalista en el que está inscrita la sociedad. Desde esta perspectiva, la extimidad también se debe a un "fetichismo mercantil basado en la circulación indefinida de la inmaterialidad, y que implica que absolutamente todo es expuesto y todo adquiere, aunque sea en su forma simbólica, la cualidad de "mercancía", incluso la propia intimidad" (Dipaola, 2008: 21). Es decir, se comercializa con lo que tenemos y que nos hace únicos, nuestra intimidad, nuestras características y detalles personales. Esto no ocurre de forma original y voluntaria, si no que se puede llegar a entender como una *obligación* social, una *necesidad creada* que induce a las personas a compartir, a ser transparentes.

El filósofo coreano Byung-Chul Han (2013) habla de la sociedad de la exposición, en la que la si no estás expuesto, no existes. Esta exhibición elimina el valor de culto de las cosas, reduciéndolas a mercancía. Reduce la existencia a algo insignificante. No se suele preguntar más allá de lo expuesto, pero sí que se sospecha de aquello que no se muestra. El mundo se ha convertido en "un mercado en el que se exponen, venden y consumen intimidades" (Han, 2013: 68). La transparencia conlleva la exposición de la intimidad, la confesión, el desnudamiento y la falta de distanciamiento. La intimidad vuelta éxtima supone una contradicción, pero es debido a que "la transparencia va unida a un vacío de sentido" (Han, 2013: 32).

No obstante, el hecho de que se pueda mantener el anonimato en este espacio público fomenta no sólo la autoexpresión, es decir, hablar de sí mismo sin ningún tipo de tabú o pudor. Si no que también fomenta la impunidad de cualquier acto que quizás no se realizaría si fuera en el plano real con una identidad inevitable. Este anonimato puede ser positivo en lo que respecta a reforzar la identidad del sujeto, ya que sin la necesidad de identificarse con un nombre real puede tomar esa libertad para poder experimentar su personalidad y sus gustos y eso no supone que esta persona no se implique personalmente en lo que esté haciendo. Pero a su vez tiene efectos negativos como pueda ser aprovechar el anonimato para insultar, fomentar comportamientos desinhibidos y antinormativos o incluso realizar ataques a la seguridad de los demás mediante virus o programas espía. Aunque también es cierto que el anonimato puro no

existe en este medio porque cualquier acción es rastreable y es difícil no dejar huellas, ya que desde que nos conectamos estamos produciendo y dejando datos por todas partes (Moral, 2001).

El perfil personal que se crea en la web no sólo está compuesto por los datos que se introducen y las publicaciones y acciones que se realizan mediante esa cuenta, sino también por los contactos agregados y la información que éstos revelan sobre los usuarios. Esta cultura de lo visible, de lo público, que está directamente relacionada con el ego de las personas, provoca que convirtamos nuestra vida en hechos noticiables. Está bien valorado que la gente se publicite en la red, que muestre qué es lo que hace y qué es lo que le gusta. El problema de todo esto es cuando una persona ajena, o simplemente alguien con acceso autorizado a los contenidos que se han publicado, utiliza esos datos sin tu consentimiento; es decir, cuando se pierde el control de los datos. Sin embargo, en las redes sociales, los beneficios que pueda aportar la publicación de la información tiene más peso que los riesgos que pueda conllevar su revelación (Tello, 2013).

Jarvis (2012) afirma que los jóvenes son conocedores de este tipo de amenazas a su intimidad, y que a pesar de ello comparten información y crean su propio entorno en el espacio público. Aunque también expone que muchos de ellos sí que reflexionan qué desean compartir y dónde, sostiene que "a los jóvenes no les importa la desaparición de la intimidad porque ya han renunciado a la suya" (2012: 136), que las nuevas generaciones ya no adoptan el sentido de privacidad tradicional.

No obstante, Tello (2013: 206) alega que "la generalidad de los usuarios desconoce que sus datos personales, las elecciones que realiza en los distintos buscadores, los productos que compra o los enlaces que visita son almacenados y empleados para fines de variada naturaleza sin su consentimiento ni conocimiento". La autora hace hincapié en la idea de que los datos que utilizan no son solo los visibles e introducidos por el usuario, sino también los generados a partir de su actividad en la red. De hecho, Jarvis (2012) cita en su libro unas declaraciones de Eric Schmidt, presidente ejecutivo de Google, en las que éste afirmaba que "los internautas violan su propia intimidad a un ritmo desenfrenado. La causa principal de los futuros problemas para la intimidad será la publicación de información por parte de los interesados" (Jarvis, 2012: 151).

La suma de nuestros datos provoca una pérdida de intimidad (Tello, 2013), debido a los avances tecnológicos de rastreo de información se han multiplicado las posibilidades de intrusión en la vida privada y de vigilancia, por este motivo se necesita un refuerzo de la protección (Tremblay, 2006). Rheingold (2004) alerta sobre la capacidad de espionaje que están adquiriendo todo tipo de aparato electrónico que nos rodea y que los efectos secundarios de esa omnipresencia computacional están empezando a producirse. Frente a esto, Jarvis (2012) mantiene una postura contraria; propone restringir el uso de la información, que no el acceso. Expone que si la información de la red no puede ser utilizada para discriminar a las personas, la tendencia a publicar seguiría en auge y se reduciría el miedo a la vigilancia. "La tecnología nos está obligando a poner en cuestión supuestos vigentes desde hace siglos asociados al papel del individuo y la sociedad: nuestros derechos, privilegios, capacidades, responsabilidades, preocupaciones y posibilidades" (Jarvis, 2012: 23).

1.2. Tipología de espacios: La personalización de la esfera pública

En Internet cabe todo, es decir, el conjunto de información y contenidos que presenta es heterogéneo. Podemos encontrar todo tipo de ideas, opiniones, valores, actitudes, etc. tanto negativos como positivos. Sin embargo, el espacio y la cantidad de información que existe en la red no es toda a la que podemos acceder. En general, atendiendo a la variable de acceso a la red, podemos encontrar tres tipos de Internet (Fornas, 2003).

- **Internet global** es la red de información libre y gratuita a la que se accede de forma común, a través de buscadores o protocolos de internet (ftp, http, p2p, etc.). Propios de este sector son motores de búsqueda como Google, las redes sociales como Facebook, Twitter, YouTube, etc., blogs y páginas de contenido libre indexadas.

- **Internet invisible** o **Internet profunda**[5][6], es la red de información que no es indexada por los buscadores de forma natural, aunque podemos acceder desde cualquier ordenador a estas páginas sin problemas. Esta información está

[5] El tamaño de la web invisible, en 2006, era de 91.850Tb mientras que la web global era de sólo 167Tb, teniendo un 50% más de tráfico la web invisible que la global (Brocos y Salinas, 2006). En 2001, la web profunda era entre 400 y 550 veces más grande que la web global (Bergman, 2001)

[6] Para consultar más sobre esta parte de Internet explórese la web http://www.brightplanet.com y véase la referencia Bergman, M. K. (2001) White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing*. [en línea] Disponible en: http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104

disponible pero no mediante las herramientas habituales de navegación, a no ser que sepamos la URL exacta de acceso (Fornas, 2003). Los recursos disponibles en este sector son bases de datos, archivos y depósitos de documentos, directorios, etc. (Brocos y Salinas, 2006). Aquí se alojan webs como Wikileaks y la base de datos de la Biblioteca del Congreso de EEUU, pero también páginas que albergan actividades ilegales y el mercado negro (*El País*, 2014d).

El término internet profunda (***deep web***) fue acuñado por Michael K. Bergman en 2001 y es difícil asegurar su tamaño, pero la mayoría de expertos hablan del 96% de la red. Aunque la red TOR (The Onion Router) se diseñó para poder mantener el anonimato dentro de Internet y mantener la privacidad de los envíos de información (que no sepan ni la identidad, ni la localización, ni ningún tipo de información que se puede obtener mediante softwares araña o de extracción de datos). Esta red se ha utilizado para poder entrar a la web invisible y ocultar contenidos, aunque ni TOR consigue abarcar toda la profundidad de esta parte de la red. Las transacciones económicas que suceden en esta zona de Internet no son mediante divisas reconocidas en el plano "real", sino que es mediante su propia unidad digital: Bitcoin[7], una moneda anónima, no depende de intermediarios ni de ninguna entidad que controle las transacciones, cómo lo puedan ser los sobres de dinero negro. Esa fue la primera en utilizarse y que sigue en activo, pero han surgido otras también para competir con ella (Alonso, 2013).

- **Internet oscuro** es el conjunto de redes restringidas a las que es imposible acceder desde cualquier ordenador, ya que son servidores y redes privadas (hosts) cuya utilización es sólo por el personal autorizado. Este tipo de redes suelen ser por fines de seguridad nacional y militar, o por errores de configuración de routers o servidores destinados a un uso ilegal (Fornas, 2003).

Cuando se busca información a partir de cualquier motor de búsqueda, como pueda ser Google, ya se está prescindiendo de una gran cantidad de información que contiene la red, ya limitamos nuestra capacidad de búsqueda. Dentro de estos límites, en los que

[7] Se puede ver la cotización mundial de esta moneda en el siguiente enlace: http://bitcoincharts.com/markets/

encontramos, a su vez, una reducción de este sector de Internet debido a su personalización, a su individualización.

Se entiende personalización como una forma de interactividad que tiene el usuario con el sistema al utilizar las herramientas que dispone para poder adaptar el contenido que alberga a las preferencias e intereses que el usuario ha demandado de forma explícita o implícita (Thurman y Schifferes, 2012). La personalización es una forma de filtraje de información (Bozdag, 2013), un ajuste o modificación de los aspectos de la web que están expuestos al usuario para adecuarse a sus gustos y necesidades (Wu *et al*., 2003).

La visión de espacio público que nos da Internet está personalizada dependiendo del tratamiento de los datos que conforman el tejido virtual. Esta visión puede ser involuntaria, que hace referencia a la personalización de forma implícita, es decir, la técnica que utilizan las empresas de Internet, aprovechando su estructura de metadatos, para perfeccionar tanto su producto como la oferta individualizada; o voluntaria, es decir, personalización explícita, que hace referencia a la configuración que realizan los usuarios de las páginas web de noticias.

1.2.1. Personalización involuntaria: Perspectiva prefabricada

La digitalización de la información ha permitido que todo se reduzca a datos y que éstos puedan almacenarse, transmitirse y procesarse fácilmente. El sesgo de información de forma involuntaria se realiza a partir de los datos que obtienen de nosotros; es decir, se trata de una personalización prefabricada[8] del espacio público, llevada a cabo por los buscadores de Internet -y algunas redes sociales como Facebook-, que tienen en cuenta distintas variables que se ha ido generando a partir del uso de la plataforma por el usuario. Este tipo de personalización no tiene por qué estar relacionada con un perfil que se haya creado, sino que tiene en cuenta otras variables como la localización desde donde se está consultando. La idea de que Internet nos conecta con todo el mundo por igual, sin filtros y que ofrece una información plural, creando un espacio democrático, no es real. La esfera pública se adapta al usuario, es decir, pierde su característica de pública para pasar a ser personal.

[8] Eli Pariser se centra en este tema en su libro *The Filter Bubble: What the Internet is Hiding from You*, 2011.

Podría denominarse también personalización implícita o pasiva, puesto que recrean una perspectiva del espacio público adecuada al usuario sin que éste lo solicite de forma activa. Ejemplos de este tipo de personalización son también las recomendaciones basadas en el historial del usuario o en su comportamiento en una red social, la adecuación de los contenidos basados en su posición geográfica o la ordenación jerárquica de los contenidos atendiendo al número de visitas o "me gusta", que en este caso se trataría de un filtro basado en la popularidad (Thurman y Schifferes, 2012).

Por ejemplo, en el caso de Google, cada usuario recibe una jerarquización de resultados diferente de la misma búsqueda a partir de palabras clave. Esto es debido a que "Google usa varias 'señales' para personalizar búsquedas incluyendo la localización, palabras clave de búsquedas previas y contactos recientes en un usuario de red social" (Bozdag, 2013: 211). De esta manera Google puede predecir qué es relevante para el usuario, utilizando filtros que sesgan la información para ofrecerle los resultados que (según Google) más le interesan al usuario (Bozdag, 2013).

En el caso de Facebook, por ejemplo, si no se interactua con un contacto (darle a "me gusta", compartir algo suyo, comentar una fotografía, escribir en su muro o incluso mirar su perfil), el sistema lo reconoce como productor de información de interés para el usuario, por lo que cualquier cosa que publique dicho contacto aparecerá en el timeline del usuario. Mientas que si no se mantiene ningún tipo de interacción con un contacto, su información permanecerá oculta del timeline del usuario de manera automática e involuntaria (Bozdag, 2013).

Oficialmente las webs de noticias no se personalizan de forma involuntaria, sino voluntaria (como veremos en el siguiente apartado), pero ¿qué sucedería si dichas webs acabasen adoptando este tipo de personalización involutaria, atendiendo al historial de búsqueda, a los likes de Facebook o de noticias similares, etc.? ¿no se nos estaría negando una parte de realidad? ¿no se nos niega ya?

Desde la perspectiva de la privacidad esto no es menos alarmante, ya que en estos casos no se trata de un descuido, de una confesión a voces o de un contenido que se ha escapado de las manos, sino de una intercepción de los datos, de una creación del perfil del usuario, de un análisis de ellos y una explotación económica de los resultados.

1.2.2. Personalización voluntaria: construcción propia del espacio público

La personalización voluntaria de la red se trata de la construcción propia del espacio público, es decir, la configuración deliberada de las fuentes de información online que usamos. "El proceso de personalización al que puede llegar el usuario en Internet es máximo, puesto que parte de la máxima selección posible (…) y, además, cuenta con casi total libertad para ir moviéndose de un espacio a otro en busca de la información que más le interese" (López García, 2005: 49).

Ejemplos de esta tipología de personalización, que también podríamos denominarla como personalización activa debido a la decisión libre y decidida del usuario de ejercer este tipo de caracterización de su espacio, son los newsletters que los usuarios solicitan marcando las áreas de interés de las que le interesa recibir información de forma periódica. También es personalización activa o explícita cuando el usuario decide personalizar la página principal de las webs de noticias con las secciones y periodistas de las que prefiere informarse o las aplicaciones móviles o widgets que permiten personalizar la recepción de noticias atendiendo a las preferencias que el usuario le ha añadido, como pueda ser la localización, los temas de interés, etc. (Thurman y Schifferes, 2012).

Según Cass Sustein (2003), profesor de derecho en la Escuela de Harvard y en la Universidad de Chicago, la posibilidad de poder personalizar el espacio público de acuerdo a los gustos e intereses de los usuarios puede suponer un peligro para la concepción de esfera pública que se forma al no estar expuesto al conjunto de la sociedad. El hecho de que sea posible estar en contacto con solo aquello que se quiere ver, leer y escuchar, dejando a un lado aquellas opiniones y temas que no interesan pueden suponer un gran problema para una sociedad democrática. De hecho, Sunstein (2003) afirma que este tipo de acciones provoca la polarización del espacio público y la radicalización de las ideologías de las personas. Cuando el individuo no está expuesto a la variedad tanto social como informacional, cualquier tipo de debate será siempre con ideas afines que reforzarán sus creencias, su visión social se acaba reduciendo a una postura extrema debido a la falta de contacto con la diversidad. Esta tendencia informativa pone al civismo democrático en peligro en la nueva sociedad red, ya que "la revolución cognitiva atribuida a Internet puede devenir en auténtica involución cognitiva si finalmente las únicas fuentes de información del mundo son las que extraemos del ciberespacio o del espacio audiovisual tras haber seleccionado

estrictamente el tipo de información que previamente deseábamos recibir" (Gozálvez, 2011: 1).

1.3.Peligros del nuevo entorno

El nuevo espacio digital presenta, a parte de sus múltiples beneficios, varios peligros, sobre todo desde la perspectiva de la privacidad. Esta esfera, que otorga más visibilidad y protagonismo al usuario, tiene facilidades de ser rastreada y vigilar a los individuos de forma silenciosa. Mediante el rastro o huella digital que dejan los usuarios de Internet, las *cookies* y otros programas araña y las distintas metodologías de extracción de datos, la vigilancia líquida de la que hablan Bauman y Lyon (2013) se hace plausible. Por otra parte, desde una perspectiva más cognitiva, hay que tener en cuenta las consecuencias que tiene la personalización voluntaria del espacio público digital, ya que una visión sesgada del mundo puede traer peligros que no son precisamente nuevos.

1.3.1. Vigilancia y control digital

Una de las características de este universo virtual es su composición de datos, y todos ellos, públicos o privados, forman parte de la red. ¿Hay más riesgo de ser vigilado a través de Internet que en la realidad *offline*? Por supuesto. No se puede asegurar completamente la privacidad en el plano virtual, ya que realmente, todo se reduce a código y un experto en la materia puede conseguir romper las barreras de seguridad en la red. No obstante, esto no quiere decir que todo aquel que esté en la red esté siendo vigilado ahora mismo, pero sí que es susceptible de serlo.

La vigilancia digital o vigilancia líquida según Bauman y Lyon (2013) se caracteriza, en primer lugar, por ser ejercida a través de las técnicas digitales y la técnica estadística. En segundo lugar, destaca por ser aquella en la que los propios vigilados contribuyen a facilitar su investigación mediante la publicitación de sus datos. "A menudo es el ciudadano-consumidor el que, de forma voluntaria, confía a la torre las informaciones que ésta necesita para construir un perfil de sus hábitos de consumo: perfil que más tarde será vendido a otras empresas convirtiéndose así en una fuente de ingresos adicional" (Ragneda, 2011: 46)

Esto es debido, en mayor medida, al uso de las redes sociales. Bauman y Lyon (2013) detectan que las redes sociales es un espacio de vigilancia, en el que el usuario sabe que todo lo que publica será observado por todos sus contactos y hasta puede que incluso por más personas. "La existencia de las redes sociales depende de su capacidad para

observar el comportamiento de los usuarios y vender esos datos a otros" (Bauman y Lyon, 2013: 15). Los autores argumentan este hecho basándose en que actualmente el miedo a ser vigilado ha sido superado el miedo a ser olvidado o excluido. "La vigilancia no se realiza como ataque a la libertad. Más bien cada uno se entrega voluntariamente a la mirada panóptica. A sabiendas, contribuimos al panóptico digital, en la medida en que nos desnudamos y exponemos. El morador del panóptico digital es víctima y actor a la vez." (Han, 2013: 95)

Y en último lugar, la vigilancia digital se define también por su invisibilidad, es decir, por el carácter silencioso con la que se establece, haciéndola indetectable. Tiene como consecuencia directa la clasificación social, la categorización de los sujetos en perfiles y el análisis de su comportamiento en la red. Desde un punto de vista ético, Bauman y Lyon (2013) sostienen que el principal problema que plantea la vigilancia digital es la *adiaforización*. Es decir, que este tipo de vigilancia, al ser automática y alejada del verdadero sujeto, también separa con ello a los vigilantes y registradores de información de las consecuencias de sus acciones. Distanciando cualquier implicación moral del análisis o seguimiento informático de un sujeto.

Aquellos que conocen las posibilidades de control o vigilancia que pueden sufrir, los instrumentos que se pueden utilizar para ello y la aparente facilidad con la que se puede dar acaban modificando su conducta (Solove, 2006). La vigilancia consigue el autocontrol por parte de los sujetos, de hecho ha sido definida por varios autores como mecanismo de autodisciplina, como detectaron Bentham o Foucault en su momento, caracterizando este mecanismo como forma de poder. Al presentarse éste de forma visible e inverificable, es decir, saber que puede pasar siempre y que nunca se sepa a ciencia cierta cuando está pasando, el poder cobra mayor fuerza (Ragneda, 2011).

El miedo a la vigilancia que se está creando a partir del conocimiento de la existencia de técnicas de extracción de información de la red no es infundado, y el hecho de que todo este procedimiento se haga de forma silenciosa hace que aumente la preocupación sobre la privacidad de los usuarios. Evgeny Morozov (2012), al igual que César Rendueles (2013), Bauman y Lyon (2013), Ragneda (2011) y Solove (2006) relacionan el funcionamiento de internet con el prototipo de prisión perfecta –el panóptico- descrita en el s.XIX por Jeremy Bentham, que consiste en tener capacidad de controlar siempre el comportamiento de los presos sin que éstos sepan con precisión cuándo están siendo

observados. El panóptico era el diseño de un edificio circular en cuyo centro se erige una torre de control que permite que unos pocos vigilen a muchos. En esa prisión los presos están aislados, pero, al contrario que en la cárcel de Bentham, "los que habitan en el panóptico digital se creen que están en libertad" (Han, 2013: 89). No obstante, en la esfera digital no se puede afirmar que el único modelo de control que se esté ejerciendo sea el panóptico; también sucede un modelo sinóptico, en el que muchos pueden vigilar a unos pocos. Estos dos modelos se complementan en la red (Ragneda, 2011).

Morozov (2012) cita ejemplos de vigilancia online gubernamental de Irán y Vietnam, como contraargumento a la idea de que Internet es la herramienta maravillosa que traerá la democracia o que es el espacio ideal en el que se puede compartir todo tipo de información y de ese modo evitar la censura tradicional. El autor afirma todo lo contrario, "cuando nadie sabe con certeza hasta qué punto se extiende la vigilancia del gobierno, cada nueva detección de un bloguero, tanto si se debe a verdaderas prácticas de vigilancia, chivatazos, intuición o inspección de un listín telefónico, contribuirá a combatir la acción subversiva, sobre todo entre aquellos que no son disidentes al cien por cien" (Morozov, 2012: 196). El autor también advierte sobre el uso despreocupado de redes sociales, en concreto habla de Facebook, que ha incorporado recientemente herramientas de reconocimiento facial. Esta empresa se jactó de haber reconocido 52 millones de individuos y haber escaneado unas 9.000 millones de fotos en 2010. El autor señala cómo este tipo de tecnología permitiría identificar a todos los asistentes de cualquier manifestación sin mucha dificultad. De hecho, ya existe una aplicación –Recognizr- que con solo fotografiar a una persona en la calle ya te dice todo lo que hay asociado a la imagen de esa persona en la red (Morozov, 2012).

La información colgada de forma abierta en las redes sociales, como la lista de amigos y "me gusta", otorga la posibilidad de relacionar a la persona con cierto tipo de actividades, "antes de la llegada de las redes sociales, a los gobiernos represivos les costaba mucho esfuerzo averiguar con qué personas se relacionaban los disidentes" (Morozov, 2012: 208). Lo que antes se conseguía torturando a la gente, ahora se consigue en silencio a través de aplicaciones en Internet. "La mayoría de nosotros sabemos lo fácil que es comprobar si nuestros amigos se han apuntado ya a una red social concreta, tan solo concediendo a Facebook, Twitter o LinkedIn acceso temporal a

nuestra libreta de direcciones de correo electrónico" (Morozov, 2012: 211). La información personal es mucho más accesible de lo que creemos.

¿Este tipo de control del espacio público digital dónde nos lleva? ¿Estamos ante el fin de la privacidad? El propio Mark Zuckerberg anunció hace años que la privacidad tal y como la conocíamos había muerto, que habíamos sacrificado nuestro espacio íntimo por un espacio donde compartir información (El País, 2014a). Franganillo (2009) se cuestiona si la seguridad se ha convertido en un pretexto para poder imponer la vigilancia y recortar las libertades. En el caso de EEUU, después de los atentados del 11 de Septiembre de 2001, se aprobó la denominada *Ley Patriota* (Patriot Act) "legitima las intrusiones en la esfera privada, entre otras a través de la vigilancia de las comunicaciones interpersonales telefónicas o electrónicas, invocando para ello motivos de seguridad pública" (Tremblay, 2006: 233). Respondiendo a Franganillo, podríamos decir que, efectivamente, se utiliza el miedo para aumentar la vigilancia. El caso de Edward Snowden (El País, 2013), ha desvelado que este tipo de control de la información no sólo lo usan los piratas informáticos o gobiernos dictatoriales, sino que también es ejercido. Tal y como vaticina Franganillo (2009: 323), "se necesitará entonces una profunda regulación para proteger los derechos y la identidad de las personas, y evitar entrar en una sociedad de la vigilancia que, a pesar del control, sea incapaz de mantenernos seguros."

La vigilancia se puede ejercer de muchas formas, pero principalmente su inicio es por la huella digital. A partir de la ella, se puede reconstruir el perfil de una persona y sus acciones, permitiendo a su vez predecir su comportamiento. Mediante el uso de las cookies y las metodologías de extracción de datos, se puede reconstruir todos los movimientos que una persona haya realizado en la web, pudiendo elaborar así un informe completo con todo el tipo de información que crea y consume una persona.

1.3.1.1. Huella digital

La huella digital define al conjunto de información que uno crea voluntaria e involuntariamente en Internet. Es decir, todo tipo de información que se puede encontrar en Internet de una persona o entidad, que ayuda a crear una imagen del individuo o empresa, ya sea por una página web personal, perfiles en redes sociales, comentarios en blogs o foros, imágenes, entre otros. Pero también por los procesos que realiza el sistema informático de forma interna como puede ser la exploración de una

web, recibir un mail, la geo-posición desde la que realizas la conexión en Internet, etc. Estos datos se quedan todos registrados en Internet aunque no todos están a la vista de cualquier usuario, sino que se requiere de un profesional y de programas especializados para poder extraer toda la información que hay en la web (Madden et al., 2007).

El concepto de huella digital proviene de la expresión inglesa *digital footprint*, tratada como tal por primera vez por Nicholas Negroponte, científico y cofundador del laboratorio de medios del MIT, en el libro *Being Digital* (1995). No obstante la traducción en castellano no ha sido aceptada de forma ecuánime. Debido a que en inglés se distingue entre *digital finguerprint* y *digital footprint*, y que su traducción al la lengua hispana en ambos sería *huella digital*, en español se ha traducido el concepto como *sombra digital*, *rastro digital* o *huella digital*. Por esta razón, a veces se encuentran textos que se refieren a la huella digital como un sistema de seguridad de los derechos de autor, este significado proviene de la traducción en inglés de *digital fingerprint* (Sánchez Muñoz, 2012). En este trabajo optamos por el término *huella digital* porque es el que mejor se adapta con una forma descriptiva a lo que representa.

Podemos diferenciar dos tipos de huella digital, aquella que se realiza de forma pasiva involuntaria y la que se forma de una forma activa voluntaria. La huella digital pasiva se genera sin que el individuo sea consciente de que la información que está proporcionando va a ser almacenada, como cuando el usuario navega por páginas web. El registro de la actividad que realizan las personas por Internet genera una información que permite tener información sobre ellas, cuáles son sus intereses, qué horarios lleva, entre otras cosas. De forma pasiva también se genera información en las redes sociales cuando la información de la persona es añadida por una tercera persona, por ejemplo, cuando un amigo sube una fotografía en la que la persona aparece, y los múltiples y diversos comentarios que se pueden publicar que los contactos de la persona que ha compartido la información y de la persona afectada.

Es decir, la huella digital pasiva es aquel registro invisible a simple vista que deriva de nuestro uso de la web y toda información que alude directamente a nosotros proporcionada por un tercero. Mientras que la huella digital activa es formada de forma consciente por el individuo al proporcionar la información sobre su persona de forma totalmente voluntaria, como puede ser la información personal del perfil de la red social (edad, lugar de nacimiento, residencia actual, estudios, trabajo...), fotos, música, enlaces

que se comparten en la red, etc. (Madden et al., 2007).

Actualmente la huella digital se ha convertido en una mercancía. El uso que se le da a este tipo de información es variado, tanto para realizar campañas de marketing dirigidas a un público específico como para estudios académicos de sociología o psicología que ayuden a entender el comportamiento de los usuarios en la red. Cada vez hay más portales que utilizan la huella digital pasiva para ofrecer publicidad dirigida al usuario o una visión de la plataforma especializada. Aunque, lamentablemente, también existe una utilización ilegal y delincuente de la huella digital, como puede ser la vigilancia de una persona o el robo de identidad, entre otros.

La huella digital constituye un peligro para la privacidad por su carácter visible, es decir, el hecho de que cada usuario (a no ser que sea experto en informática y sepa navegar de forma anónima) se vaya desprendiendo de datos conforme utiliza Internet, dejando una serie de elementos imborrables que desvelan datos sobre la vida privada, como puedan ser los gustos o los hábitos. Pero el problema no son esos datos por separados, sino cuando son recopilados de forma deliberada para reconstruir el perfil del usuario y con eso su identidad digital, de forma actualizada para más énfasis. "Ahora se sabe qué periódicos leemos, qué ropa compramos, qué viajes hacemos; se sabe qué ideas políticas tenemos, qué gustos sexuales, qué religión profesamos" (Ragneda, 2011: 45).

1.3.1.2. Cookies

Las *cookies* son "dispositivos de almacenamiento y recuperación de datos que se descargan en el equipo terminal de un usuario con la finalidad de almacenar datos que podrán ser actualizados y recuperados por la entidad responsable de su instalación" (García-Ull, 2013: 236). Según el tipo de *cookie* que sea, se puede consultar hasta la actividad previa del usuario en la red. Esta información permite a los receptores de datos "llevar el control de usuarios pero también conseguir información sobre sus hábitos de navegación" (Touriño, 2014: 139)

En relación con el tipo de recolección de datos que afecta directamente privacidad, cabe destacar una de las clasificaciones de *cookies* que realiza la Agencia Española de Protección de Datos (2013) atendiendo a la finalidad de dicha *cookie*.

- *Cookies* técnicas: son necesarias para la navegación en Internet, aquellas que agilizan la carga de todos los elementos de una web y su correcto funcionamiento.
- *Cookies* de personalización: adecúan, de forma general, los contenidos de la página web atendiendo a variables predefinidas basadas en los datos del usuario, como pueda ser el idioma o la configuración regional desde donde accede al servicio.
- *Cookies* de análisis: permiten al receptor de la información procesar los datos y trazar un patrón de comportamiento del usuario. Es utilizada para la medición de índices de visita o actividad en una web, para ver qué tipo de público es la que la consulta.
- *Cookies* publicitarias: permiten la gestión de los espacios publicitarios en una página web, pero la publicidad que se muestra no varía en función al comportamiento del usuario. Los criterios que sigue esta cookie se basan en el contenido que está editado o el tiempo que se muestran los anuncios.
- *Cookies* de publicidad comportamental: habilitan la gestión de los espacios publicitarios de las páginas web. Permite personalizarlos atendiendo a la información que ha obtenido del usuario para que la publicidad que éste vea, dentro de las opciones publicitarias que tenga la web, se adecúe a sus necesidades dependiendo de su comportamiento en la red.

Las *cookies* pueden ser buenas para el usuario en tanto que ayuda técnica, pero aquellas cuyo único fin es almacenar la información en paquetes para que posteriormente esos datos brutos sean enviados a una empresa para que sean tratados, es una invasión a la privacidad. Con el marco jurídico actual las *cookies* son legales y están reguladas. Para utilizarlas los responsables del tratamiento deben obtener un consentimiento informado del usuario, pero, por desgracia, se permite que la confirmación del uso de este tipo de dispositivo con el usuario sea mediante la simple navegación por la web, sin necesidad de presionar ningún botón. Con el simple banner que anuncie el uso de *cookies* por la página web es suficiente para activarlas y ponerlas en funcionamiento.

Las *cookies*, también conocidas como *chivatos*, suponen una vulneración de nuestra privacidad. A pesar de que estos datos sean utilizados, aparentemente, para fines publicitarios y para mejorar el acceso a la información mediante la personalización de la web, no deja de ser un espionaje a pequeña escala. Supone una identificación

involuntaria del usuario y una manipulación de su entorno de forma invisible con fines económicos en última instancia.

1.3.1.3. Metodologías de extracción de datos

Los datos que se suben y se crean en la red son inabarcables por un ser humano. Es por ello que se necesitan herramientas y sistemas de procesamiento de datos que permitan su uso y análisis. Se utiliza el término *Big Data* o *macrodatos* para referirse a un conjunto de datos imposible de procesar por ningún método o programa convencional. Las bases de datos actuales suelen ser de tal magnitud que requieren tecnologías informáticas que automaticen el procesamiento de toda la información (Riquelme, Ruiz y Gilbert, 2006). Se denomina *Big Data* a "grandes Volúmenes de información que se mueven o analizan a alta Velocidad y que pueden presentar una compleja Variabilidad en cuanto a la estructura de su composición" (Tascón, 2013:48). Es por ello que diversos autores coinciden en que los macrodatos se definen por las 3V's: volumen, variabilidad y velocidad (Tascón, 2013 y Sabater, 2013).

Se identifican por el volumen debido a que el conjunto de datos puede ocupar más de un Petabyte (PB), es decir más de 1 000 000 000 000 000 bytes, que equivale a 10^6 Gigabytes (GB). Un ejemplo de esta gran masa de datos lo tenemos en Facebook, según los datos que publicaron en 2013, cada día se comparten más de 4750 millones de contenidos en Facebook, concretamente, se suben más de 350 millones de imágenes al día, sumando un total aproximado de 250 billones de fotos disponibles en la red social. Para soportar estos datos, la empresa cuenta con una infraestructura de más de 250 PB (Internet.org, 2013). La velocidad distingue a los macrodatos precisamente por la rapidez con la que se generan y la que tardan en analizarse, porque una vez están establecidos los patrones de análisis y se tiene bajo control la base de datos, el procesamiento de la nueva información que entra es también agilizado (Sabater, 2013). Esto permite poder captar los cambios en los datos y tomar decisiones rápidas en función de los resultados (Vega, 2013). La variedad caracteriza al Big Data por la heterogeneidad de los datos, ya que no sólo provienen de distintas fuentes sino que también de formato (números, caracteres, imágenes, vídeo, audio, enlaces, localizaciones, etc.), almacenados de forma desestructurada (Sabater, 2013).

A parte de las 3V's, hay autores que han seguido sumando características definitorias de los macrodatos, tales como: Variabilidad, Veracidad, Visualización y Valor. La

variabilidad designa estos conjuntos de datos porque se pueden interpretar de diversas formas, dependiendo de la pregunta formulada se obtiene una respuesta distinta de la misma base de datos (Sabater, 2013). La veracidad distingue al big data por obtener información verídica, ya que la información que recoge se basa en acciones reales de usuarios (Sabater, 2013 y Vega, 2013). La visualización también define estos volúmenes de datos por sus resultados finales, ya que éstos se presentan como nuevas formas de visualizar la información (Tascón, 2013). El valor que aportan los resultados que se obtienen de los macrodatos es muy beneficioso para la empresa (Sabater, 2013).

El Big Data supone un compendio de herramientas, almacenaje y procesamiento de grandes volúmenes de información que está aumentando su uso de forma exponencial. Esto es debido a los grandes beneficios que obtienen las empresas y entidades al poder analizar la ingente cantidad de datos que les interesa con el tiempo necesario para poder tomar una decisión sobre el futuro.

Se obtiene un doble beneficio del contenido que podemos extraer de estas bases de datos que se generan de un entorno web concreto (Riquelme, Ruiz y Gilbert, 2006). Por un lado, se extrae información de gran valor para las empresas o propietarios de esa infraestructura virtual, como pueda ser el número de visitantes, el tiempo medio que han pasado en la web, desde qué explorador, si es hombre o mujer, el país desde dónde se efectúa la visita, etc.; elementos que ayudan a conocer al público que utiliza un espacio web y las preferencias que éste tiene. Por otro lado, la explotación de la información obtenida permite comprender el fenómeno que se está analizando. Este segundo beneficio proviene del *data mining* o minería de datos, que es "un intento de buscarle sentido a la explosión de información que actualmente puede ser almacenada" (Riquelme, Ruiz y Gilbert, 2006: 11).

La minería de datos o data mining es el análisis de la información de grandes bases de datos con objeto de encontrar relaciones entre los datos que sean de interés o aporten valor para los propietarios de los macrodatos. Este procesamiento de la información se realiza mediante tecnologías de inteligencia artificial y técnicas estadísticas. Los problemas que resuelve la minería de datos son aquellos cuya resolución consiste en tratar datos históricos almacenados.

Los usos más comunes son para buscar relaciones inesperadas mediante de la descripción de la realidad a partir de múltiples variables; buscar asociaciones entre los

sucesos almacenados; crear y definir tipologías (de consumidores, de comportamientos, de opiniones, de sucesos, etc.); detectar ciclos temporales; y hacer predicciones (Aluja, 2001). "*Data mining* implica la creación de perfiles a través de la recolecta y combinación de datos de carácter personal, y analizándolos crea patrones particulares de comportamiento que se estiman sospechosos" (Solove, 2008: 343).

La minería de datos forma parte de las metodologías de análisis inteligente de datos, cuya misión es encontrar la información útil de los datos y revelar las relaciones que existen entre ellos. Concretamente, el *data mining* es un paso del proceso denominado Descubrimiento de conocimiento en bases de datos (*Knowledge Discovery in Databases* - KDD). Este término, acuñado en 1989, tiene como objetivo final convertir las grandes e ininteligibles bases de datos en un volumen de información más útil y manejable (Riquelme, Ruiz y Gilbert, 2006). Mientras que el KDD es el proceso completo de la extracción del conocimiento implícito de las bases de datos, la minería de datos es la etapa de descubrimiento de los patrones y relaciones de la información a través de distintas técnicas –aplicación de diversos algoritmos- escogidas según los intereses del investigador. "El data mining trabaja en el nivel superior buscando patrones, comportamientos, agrupaciones, secuencias, tendencias o asociaciones que puedan generar algún modelo que nos permita comprender mejor el dominio para ayudar en una posible toma de decisión" (Molina, 2002: 2). El espacio público digital está siendo constantemente rastreado y analizado por todos aquellos agentes que quieren sacar información de él, de hecho, actualmente se aplica este proceso de minería de datos en diversas áreas de forma rutinaria[9].

El *data mining* aplicado a la huella digital que dejamos en Internet -*web mining* (Molina, 2002)-, que básicamente se basa en la clasificación y agrupación de personas según distintas variables. Empezamos a producir estereotipos a aplicar cierto grado de discriminación e incluso manipulación, debido a que "la minería de datos revela cómo

[9] Este tipo de actividad no se produce sólo en Internet; Molina (2002) ofrece ejemplos ilustrativos de la utilización habitual de esta técnica en el plano real: en el gobierno estadounidense, por ejemplo, el FBI analiza las bases de datos comerciales para detectar terroristas; a nivel empresarial, se ha utilizado para detectar fraudes con tarjetas de crédito, para descubrir la pérdida de clientes o para predecir audiencias en medios de comunicación. También se aplica a la medicina, a la meteorología y a la astronomía, permitiendo en este caso avanzar en la ciencia. Este tipo de uso podemos considerarlo útil y necesario, no obstante, también se utiliza para la discriminación negativa de las personas; como por ejemplo, cuando los comercios realizan ofertas especiales a los clientes que menos compran en el establecimiento para fidelizarlos. Franganillo (2009) señala la necesidad de un código ético para la minería de datos precisamente por este tipo de discriminación, que se hace más a menudo de lo que nos creemos.

se puede influir sobre las personas y cómo se las puede manipular para obtener un beneficio que no suele ser mutuo, sino exclusivo de quien posee y explota esos datos" (Franganillo, 2009: 321). A pesar de que legalmente los usuarios son los propietarios de sus datos, si no pueden controlarlos, quienes realmente se convierten en dueños de nuestra información son aquellos que recopilan y explotan esos datos (Franganillo, 2009). Es por estas razones que algunos autores como Franganillo (2009) reclaman un código ético para la utilización de la minería de datos.

1.4. Nuevos valores de la cultura digital: la cultura de compartir

La intención con la que se creó Internet fue la de conectar distintos ordenadores del mundo para poder compartir información independientemente de la distancia que les separase. Castells (2012) afirma que la cultura de la red es la cultura de la libertad desde sus inicios, "fue diseñada por científicos y hackers deliberadamente como una red de comunicación de ordenadores descentralizada capaz de resistir el control desde cualquier centro de mando. Surgió de la cultura de la libertad predominante en los campus universitarios de los años setenta" (Castells, 2012: 221)

La filosofía que predomina en la Internet es la de compartir; ejemplos de este modo de comportamiento pueden desde el movimiento de software libre hasta las redes P2P (*peer to peer*), que consisten en conectar de forma directa los ordenadores de aquellas personas que disponen o desean un contenido en concreto, facilitando una descarga directa y con ello la compartición de estos archivos (estas suelen ser las redes que se utilizan también para la piratería). Es decir, desde el punto de vista de la estructura de la web, podemos afirmar que está diseñada para compartir y fomentar la unión y colaboración de los usuarios.

Pero esta filosofía no se ha quedado en elementos estructurales sólo, se ha trasladado al terreno personal, al terreno de la privacidad. Ya no sólo se comparten archivos o información, como por ejemplo el proyecto de Wikipedia, que se ha elaborado entre muchos colaboradores voluntarios, sino que también se comparten experiencias de vida. "Esto transforma la cultura, porque la gente comparte experiencias con un bajo coste emocional, ahorrando energía y esfuerzos. Trascienden el tiempo y el espacio mientras siguen generando contenidos, creando enlaces y conectándose." (Castells, 2013:18) Como dice el autor, esto supone un cambio de valores respecto a la sociedad del s. XX.

Clay Shirky (2012), define esta capacidad de compartir y colaborar como "excedente cognitivo", basada en la predisposición de las personas a consumir, crear y compartir. "Nuestras nuevas redes de comunicación fomentan la afiliación y el intercambio, y ambas son cosas buenas tanto por sí mismas como por lo que generan, y también proporcionan apoyo para la autonomía y la competencia" (Shirky, 2012: 93) Las redes sociales fomentan la socialización digital y la interconectividad de las personas, teniendo esto como efecto directo la necesidad de publicar o ser visible en la red.

Jeff Jarvis (2012), también observa esta conducta desde una perspectiva positiva. Para el autor, la publicificación (compartir información, pensamientos o acciones en la red) supone muchas ventajas, entre las que destaca el fomento de las relaciones. "Internet ha cambiado la infraestructura de las relaciones. Del mismo modo que ahora suponemos que sólo nos separa una búsqueda de cualquier tipo de información que necesitemos, damos por hecho que sólo nos separa un contacto de la gente que queremos conocer" (Jarvis, 2012: 67). El autor profundiza diciendo que gracias a la publificación podemos conocer a gente con nuestros mismos gustos o con nuestros mismos problemas, creando así nuevos contactos y nuevos grupos, enfatizando en la idea en que si las personas no se abren y publican es imposible encontrarse los unos a los otros.

Jarvis (2012) también destaca como valor positivo la anulación de los desconocidos. "¿Quién es hoy en día un desconocido cuando en cualquier minuto, ya sea en Facebook o en Twitter, alguien que estaba en la sombra puede salir a la luz?" (Jarvis, 2012: 68). Partiendo de esta premisa, el autor explica que los desconocidos han dejado atrás esa "demonización" que los caracterizaba antaño, que ahora somos más abiertos a conocer gente por Internet y a establecer vínculos con aquellas personas con las que tenemos algo en común.

La publificación también facilita la colaboración y aumenta los conocimientos (y la generosidad) de las personas. Según Jarvis (2012), también desmonta el mito de la perfección, es decir, al contrario que en la esfera material en la que los productos ya están acabados (son perfectos) para la venta, en la esfera digital los productos salen en versiones de prueba e incluso ofrecen la posibilidad a los usuarios de colaborar para mejorar el producto, demostrando con esto que la perfección no existe y que entre todos se consiguen mejores resultados. Por otra parte, el autor también sostiene que la publificación acaba con los estigmas, en el sentido de que al encontrar a gente con los

mismos gustos en la red y grupos en los que se puede conversar de aquello que quizás en la realidad más inmediata de una persona no se atreve, gracias a Internet, deja de ser un tabú. “El hecho de llevar una vida pública no solamente demuestra lo poco que tenemos que ocultar, sino lo poco que tenemos que temer” (Jarvis, 2012:81). El académico finaliza esta idea sugiriendo que en un mundo sin intimidad no existiría la vergüenza.

Durante toda su obra, Jarvis (2012) elogia todos los aspectos positivos que encuentra de compartir información (sobre todo privada) en Internet. Sin embargo, desde una perspectiva más crítica, Byung-Chul Han (2013) realiza un análisis a la sociedad actual, a la sociedad de la transparencia. El filósofo coreano, al contrario que Jarvis, defiende la intimidad de las personas, afirmando que la transparencia no es natural en el ser humano, solo la máquina es transparente. La esfera privada es natural en las personas, no podemos ser completamente transparentes, ni siquiera para nosotros mismos, tenemos un inconsciente que ni la propia gestiona es capaz de gestionar.

Han (2013) detecta que ha habido un cambio de paradigma y que en la sociedad actual se exige transparencia, pero no sólo referida a la política y la economía, o a la corrupción y libertad de expresión, sino a todos los sucesos del sistema social. Explica que estamos ante la sociedad de la exposición que se reduce a “un mercado en el que se exponen, venden y consumen intimidades” (Han, 2013: 68).

El principal problema que encuentra Han (2013) es que el exceso de transparencia y de visibilidad provoca un efecto anestésico a las personas, evitando la reflexión sobre los sucesos. Afirma que no se suele preguntar más allá de lo expuesto, pero sí que se sospecha de aquello que no se expone. De hecho, el filósofo profundiza y sostiene que “la transparencia va unida a un vacío de sentido” (Han, 2013: 32), ya que no se valora aquello que se está viendo, se normaliza y con ello se anestesia.

Han (2013) muestra su preocupación por el espacio público anunciando que éste se encuentra en peligro. Alega que es un espacio necesario para la reflexión conjunta y que se está reduciendo a un lugar de exposición y consumismo. “La pérdida de la esfera pública deja un vacío en el que se derraman intimidades y cosas privadas. En lugar de lo público se introduce la publicación de la persona. La esfera pública se convierte con ello en un lugar de exposición” (Han, 2013: 69) El autor expone que la sensación de cercanía que provocan las redes sociales es la que provoca la crisis del espacio público.

> "Los *social media* y los motores de búsqueda personalizados erigen en la red un absoluto *espacio cercano*, en el que está eliminando el *afuera*. Allí nos encontramos solamente a nosotros mismos y a nuestros semejantes. […] Esta cercanía digital presenta al participante tan solo aquellas secciones del mundo que *le gustan*. Así desintegra la esfera pública, la conciencia pública, *crítica*, y privatiza el mundo. La red se transforma en una esfera íntima, o en una zona de bienestar." (Han, 2013: 68-69)

La dura crítica que sostiene el filósofo coreano, a la tendencia social actual de compartir intimidades y experiencias que se está viviendo, resalta muy bien las consecuencias. El exceso de publicación de intimidades en la red supone el fin del espacio público, convirtiéndose en una realidad ligada a nuestra zona de confort cotidiana, siendo una extensión más de nuestra vida social. No obstante la tendencia de exposición de intimidades en la red configura un gran riesgo para la privacidad, convirtiéndose en uno de los problemas principales de la actual sociedad red.

CAPÍTULO 2

EL IMPACTO DE LA TRANSFORMACIÓN TECNOLÓGICA EN LOS DERECHOS DE LOS CIUDADANOS RELACIONADOS CON LA PRIVACIDAD

La aceptación y adaptación por parte de la sociedad de los avances tecnológicos ha supuesto un incremento exponencial tanto del número de adquisiciones de dispositivos electrónicos (ordenadores, tablets, smartphones, etc.) como del número de servicios ofertados en la red (correo electrónico, redes sociales, webs, foros, wikis, aplicaciones, etc.), pero también ha aumentado la capacidad de recolección, procesamiento, análisis y almacenamiento de datos personales así como los emisores de información. Se han multiplicado los emisores, con mayor o menor protagonismo, pero todos ellos deben respetar la ley por igual. Esto significa que al igual que un periodista, profesional de la información, sería juzgado si no respeta el derecho a la información y los derechos de la personalidad de los individuos sobre los que informa, "las leyes y la jurisprudencia no pueden resultar diferentes porque el sujeto emisor no sea un profesional, sino que deben ser las mismas y, por lo tanto, deben estar sometidas a los mismos criterios de responsabilidad jurídica." (Carrillo, 2007: 68)

Internet y la evolución tecnológica han conseguido eliminar las barreras del espacio-tiempo (la distancia, ubicación, temporalidad y sincronía, entre otras). Esto supone beneficios para el usuario común, pero es un gran inconveniente para la aplicación legislativa, porque los derechos y sus reglamentos se aplican sólo en aquella zona geográfica donde tiene jurisdicción. Ahí es donde aparece el verdadero problema a la hora de ejercer o reclamar nuestros derechos en la red, donde los sistemas legales que regulan la privacidad y el intercambio de datos personales pueden quedarse sin potestad de actuar. Por ejemplo, si la empresa o plataforma tiene sede en EEUU, aunque el usuario lo utilice desde España, la legislación que debe cumplir esa plataforma es la estadounidense y, a menos que tenga una sede en Europa, el Tribunal Europeo no podrá intervenir. Por eso muchas páginas de descargas (ilegales en Europa) están alojadas en países cuya legislación no prohíbe el intercambio de esos contenidos.

Esta situación pone en riesgo los tradicionales derechos de la personalidad de los ciudadanos, tanto por el desconocimiento del individuo, que se pone en peligro sin ser

consciente, como por la estructura de la red. "El individuo tiende a acceder a una nueva plataforma de Internet, a una nueva aplicación o red social, sin advertir los riesgos en la exposición de datos personales, privados e íntimos, de manera que, sin apenas percibirlo, se coloca a sí mismo en una situación de vulnerabilidad." (Touriño, 2014: 21-22)

No existe una ley que regule Internet específicamente; la forma que ha adoptado la legislación tanto europea como española de abordar la digitalización ha sido mediante la ampliación de la cobertura de los derechos existentes. Es decir, las leyes que habían antes de Internet se han ampliado y modificado para que en la esfera virtual sigan protegiendo a los ciudadanos. Los textos legales de un sitio web, que pueden recibir nombres como términos y condiciones de uso, constituyen un contrato entre usuario y prestador del servicio. Este documento supone una declaración de intenciones en el que se dice no sólo la legislación a la que se acoge sino también qué es lo que hará la empresa de la plataforma con los datos que se faciliten o generen en ella. El desconocimiento por parte del usuario de la regulación que atañe a los distintos aspectos de la red y de la autoridad a la que debe acudir para pedir justicia, crea una falsa sensación de aparente impunidad a la persona que ha infringido el derecho (Touriño, 2014). El derecho no está del todo preparado para hacer frente a las nuevas modalidades de infracciones como *grooming*[10], *cyberbulling*[11], *sexting*[12], suplantación de identidad, etc. y "uno de los problemas jurídicos de especial relevancia que presenta el ejercicio del derecho a la información en internet es la determinación de la autoría y fijación de responsabilidades" (Carrillo, 2007: 70). Los comentarios que exceden la libertad de expresión, la publicación de información que revela datos de la vida privada, o la publicación de fotos por terceras personas en las que aparece el usuario sin su consentimiento, son ejemplos de cómo se pone en entredicho la protección de derechos de la personalidad en Internet (Touriño, 2014).

[10] Grooming: "modalidad de ciberacoso en la que el acoso lo ejerce un adulto frente a un menor, pretendiendo además aquel obtener del menor algún tipo de favor sexual, amparándose en su especial vulnerabilidad y desprotección" (Touriño, 2014: 140-141)

[11] Cyberbulling: "forma de acoso entre iguales a través de la tecnología, la cual incluye actuaciones de chantaje, vejaciones o insultos, teniendo como rasgo definitorio que acosador y acosado son compañeros de colegio o instituto en la vida física." (Touriño, 2014: 139)

[12] Sexting: "anglicismo que, mediante la combinación de los términos *sex* y *texting*, define la práctica consistente en el envío, especialmente a través de dispositivos móviles, de fotografías o vídeos con contenido sexual, captados normalmente por el protagonista de los mismos" (Touriño, 2014:141)

Los riesgos más destacados en cuanto al control y protección de datos y la consecuente privacidad del individuo en el uso de redes sociales son, por ejemplo, la dificultad o imposibilidad de eliminar todos los datos personales de un perfil (aunque uno elimine la cuenta la compañía la bloquea o la cancela a la espera de que cuando el usuario quiera volver sus datos sigan disponibles; o si se elimina, se realizará sólo de los datos proporcionados por el usuario, no todos los que le afecten a él); la facilidad de la suplantación de identidad, creación de perfiles falsos, extorsión y consecuente daño a la imagen de un individuo; la indexación de información personal por motores de búsqueda, como la imagen de perfil y el nombre; la venta de los datos personales por parte de estas plataformas para revertir en publicidad específica no deseada para el usuario. Las plataformas tienen configurado por defecto el acceso libre a toda la información que se publica, incluyendo todo tipo de datos personales que se proporcionan para abrir la cuenta, sin restricciones; es decir, la responsabilidad de la privacidad recae directamente en el ciudadano (Herrán Ortiz, 2010). Las redes sociales han tomado conciencia de que si no ponen herramientas a disposición del usuario y no son rápidas a la hora de actuar frente a estas denuncias, los ciudadanos perderán la confianza y la fiabilidad en estas plataformas. Debido a esta razón, las herramientas de reporte de abuso en las redes sociales más populares son rápidas y efectivas (Touriño, 2014).

En este capítulo se aborda, en primer lugar, la definición de los derechos de la personalidad que protegen la esfera privada del ciudadano. En concreto, el derecho a la imagen, a la intimidad personal y familiar y de autodeterminación informativa. Estos derechos se desarrollan siempre en dos partes: primero, se realiza una definición conceptual del derecho, lo que podríamos entender como su variante tradicional, y después se aborda ese derecho dentro del escenario digital. Para poder ilustrar estos conceptos se hace referencia a la legislación europea y a la española con la finalidad de hacer más comprensible su explicación. En segundo lugar, se aborda el derecho de protección de datos, ya que este derecho no sólo se encarga de preservar los anteriores, sino que en temas de privacidad y seguridad en Internet es el derecho de referencia. Este derecho se presenta también en dos partes: una primera se centra en su definición y en los derechos que crea; y una segunda en su evolución histórica, dibujando su marco jurídico tanto en el ámbito europeo como en el territorio estatal español. Finalmente, se aborda el derecho al olvido, el concepto, su historia y sus posibilidades de actuación,

teniendo en cuenta que está recientemente reconocido por el Tribunal de Justicia de la Unión Europea (TJUE).

2.1. Derechos de la personalidad

Los derechos de la personalidad, derechos personalísimos o derechos de la persona, hacen referencia a una serie de derechos personales, absolutos, inalienables e intransferibles que el individuo tiene desde el nacimiento y no puede ni ceder ni renunciar a ellos. Son aquellos que se dirigen a proteger la integridad personal del ser humano desde una vertiente física (el derecho a la vida, por ejemplo) y espiritual (el derecho al honor, por ejemplo). Estos derechos están recogidos en la Declaración Universal de los Derechos Humanos de 1948, en concreto en la Unión Europea los encontramos en el Convenio Europeo de los Derechos Humanos (CEDH), en los primeros capítulos de la Carta de Derechos Fundamentales de Unión Europea y en el Pacto Internacional de Derechos Civiles y Políticos de 1966, adoptado por la asamblea general de la ONU. Los derechos de la personalidad son declarados y desarrollados en la constitución de cada Estado miembro; en España, los derechos de la personalidad[13] se encuentran en la Constitución de 1978 (del artículo 15 al artículo 18).

Ejercer este conjunto de derechos en Internet y subsanar la falta cometida tiene más complicaciones en el plano digital debido a sus inabarcables dimensiones y a la multiplicidad de tipos de plataforma y usuarios. Es decir, por la parte de la legislación sí que reconoce estos derechos en la red, pero eso no garantiza que su marco de actuación sea muy efectivo; es por ello que se deben redefinir y contemplarlos también desde la perspectiva digital.

[13] Los derechos de la personalidad en la legislación española, que podemos encontrar en la Constitución de 1978, están clasificados en tres grupos: vida e integridad física (derecho a la vida y a la integridad física y moral); libertades (desarrolladas a lo largo del articulado de la Constitución: Libertad religiosa y de culto; libertad personal; libertad de fijación de residencia y de circulación; libertad ideológica y de expresión; libertad de producción y creación literaria, artística, científica y técnica; libertad de cátedra; libertad informativa; libertades públicas -derecho de reunión y manifestación y de asociación-; libertad de enseñanza y de creación de centros docentes; libertad de sindicación y de huelga.); integridad moral y esfera reservada de la persona (derecho al honor, a la intimidad personal y familiar y a la propia imagen) y derecho al nombre.

Hay que tener en cuenta que los derechos de la personalidad están en formación porque van creciendo sus especificidades, como por ejemplo aquellos relacionados con la esfera digital, que se ven obligados a evolucionar debido a los nuevos retos que le plantea esta tecnología.

Los derechos de la personalidad que se desarrollan en este trabajo son aquellos que están vinculados directamente con el objeto de estudio de esta investigación.

Tabla nº1: Derechos de la personalidad que protegen la esfera privada del ciudadano

Derechos de la personalidad que protegen la esfera privada del ciudadano	**-Derecho a la imagen** **-Derecho a la intimidad personal y familiar** **-Derecho al honor** **-Derecho de autodeterminación informativa**

Fuente: Elaboración propia

Los usuarios se ven *obligados* a publicitar su personalidad y sus actividades, a renunciar a estos derechos que protegen la personalidad y la privacidad de la persona, siempre de forma *voluntaria* al usar las redes sociales. Esto es debido, en primer lugar, a que deben aceptar estas condiciones para poder utilizarlas y que su funcionalidad así como su filosofía es conectar y compartir información. Y en segundo lugar, a la cultura de compartir propia de la red, que "normaliza" la publicación y el libre acceso a todo tipo de información.

2.1.1. Derecho a la imagen

El derecho de imagen supone el derecho a la captación, reproducción o publicación de la imagen y a su vez, del nombre, voz o imagen de una persona. Antes, al haber menos medios y ser más corto el circuito de difusión se podía controlar con más facilidad la vulneración del derecho a la imagen y calcular su daño. Ahora con la dimensión global de Internet, su viralidad y la cantidad de imágenes que se suben al día, da como resultado un descontrol de las imágenes que se difunden en la red y de las posibles violaciones de este derecho.

Desmitificando lo que muchos usuarios piensan, las imágenes de Internet tienen derechos, todas ellas. Cualquier foto consta de dos tipos de derecho: el derecho a la propia imagen de las personas que aparecen y el derecho de autor de propiedad intelectual. Si alguno de estos derechos se vulneran, las plataformas de Internet habilitan recursos para retirar fotos, con el objetivo de garantizar la seguridad y fiabilidad del usuario. No obstante, cuando un usuario sube una foto a Internet, está cediendo parte de sus derechos a los propietarios de la plataforma y a los usuarios, esta

información debería ser leída siempre antes de aceptar los términos y condiciones de uso, donde viene reflejado el uso que harán con los datos y los elementos que se publiquen en la red, la cesión o renuncia de derechos, etc. La publicación en Internet no hace perder el derecho legítimo, pero si se han cedido los derechos por subirlo a una plataforma, se ha perdido el control absoluto de la circulación de esa imagen. Oficialmente, con el cierre de la cuenta en una plataforma, se acaba con ello el contrato y el *poder* que ésta tenía sobre tus datos, sin embargo, redes sociales como Facebook, establecen en sus cláusulas que con el fin de una cuenta se acaba la licencia que tienen sobre tus datos a no ser que hayan sido compartidos por terceros, lo que supone una pérdida absoluta del control (Touriño, 2014).

2.1.2. Derecho a la intimidad

El desarrollo tecnológico ha provocado un avance de técnicas que permiten una intromisión casi invisible en un sector que es de soberanía individual y que afecta al derecho a la intimidad. Estos innumerables avances han permitido la acumulación de inmensas cantidades de información, concretamente datos personales, que hace poco más de una década era imposible de imaginar. Por ello la legislación de una potencia como Europa ha tenido que adaptarse a estas exigencias.

El derecho a la intimidad, recogido en la Declaración Universal de Derechos del Hombre en 1948, estipula que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (Art. 12). Es decir, supone el "derecho concedido a la persona sobre el conjunto de actividades que forman su círculo íntimo, personal y familiar, y que le permite excluir a los extraños de entrometerse en él y darle una publicidad que no desee el interesado" (Touriño, 2014: 140). La intimidad se presenta pues como

> "una esfera de protección que rodea la vida más privada del individuo frente a injerencias ajenas o conocimiento de terceros, salvo excepciones muy concretas contenidas en la Ley. Dicha esfera protege tanto elementos físicos e instrumentales (como la propia vivienda, la correspondencia o las comunicaciones privadas), como elementos sustanciales que suponen determinados datos sensibles sobre el individuo (su ideología, religión, creencias, vida sexual o salud)" (Salgado, 2010: 71).

Se considera que hay una intromisión a este derecho cuando se produce una "divulgación no consentida de hechos ciertos relativos a la vida privada de una persona o familia" (Touriño, 2014: 52) y que no haya sido publicada antes por el autor.

En el plano virtual cada vez es más difícil proteger la intimidad. Los usuarios de plataformas sociales, que no son sus clientes sino sus productos, ya que la información que subimos y generamos automáticamente es procesada y vendida a las distintas empresas publicitarias interesadas en dirigir sus campañas a un público específico, ponen en riesgo su intimidad constantemente. Este tipo de prácticas que realizan con los datos las empresas propietarias de las redes de comunicación son totalmente legales, ya que tienen el consentimiento (de forma consciente o inconsciente) del usuario al aceptar las condiciones de la plataforma al registrarse. Las *cookies* conforman otra opción de extracción y recopilación de datos legal en la red que consiguen otorgar también un control tanto de la información de los usuarios como de aquella que generan con sus hábitos de consumo. Las razones por la que aceptamos los términos y condiciones de uso prácticamente sin preocuparse demasiado son principalmente dos. Porque es la única forma de poder utilizar la aplicación y formar parte de esa red y porque el hecho de que esta situación se repita constantemente en la mayoría de las plataformas en las que nos registramos hace que nos acostumbremos y no le demos importancia al contrato que estamos firmando (Touriño, 2014).

Relacionado con el derecho a la intimidad, el derecho a la privacidad, en cambio, no pertenece a los derechos de la personalidad (Salgado, 2010); precisamente por esto es necesaria su distinción respecto al derecho a la intimidad. El derecho a la privacidad –right to privacy- en EEUU, corresponde con el derecho a la intimidad europeo, pero en la Unión Europea, sí que se distinguen dos esferas de protección distintas. Por derecho a la privacidad se entiende la protección de datos de carácter personal, convirtiéndose así la privacidad en una esfera de protección más amplia que la intimidad, ya que protege "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, 2010: 72).

2.1.3. Derecho al honor

La libertad de manifestar una opinión libre tiene su límite (entre otros) en el derecho al honor de los sujetos afectados. Este derecho personalísimo consiste en "derecho a no ser

escarnecido o humillado, a que nadie se refiera a una persona de forma insultante o injuriosa, o atentando injustificadamente contra su reputación, haciéndola desmerecer ante la opinión ajena" (Touriño, 2014: 140). El honor comprendería pues tanto el respeto a la intimidad, la reputación, el respeto al individuo y la buena imagen, así como lo que los demás piensan sobre nosotros. Sin embargo este tipo de derechos es del tipo indemnizatorio, debido a que éste se reclama cuando ha sido vulnerado y se subsana con una compensación, normalmente monetaria, hacia la persona (Gozaíni, 2011).

¿Hasta qué punto se respeta esto en la red? Oficialmente, debería ser así, ya que la ley que se aplica es la misma que en plano offline, es decir, que si alguien considera que ha sido insultado, se han divulgado hechos falsos sobre su persona o han lanzado opiniones injuriosas o juicios de valor sobre ella, que son las tres infracciones reconocidas, tiene el derecho de denunciar estos actos para subsanar el daño y ser indemnizado. Por desgracia, transgredir los límites de la libertad de expresión cada vez es más frecuente en redes sociales. Un ejemplo común es el caso de los *trols*[14] en todas sus variantes, desde la suplantación de identidad hasta el envío de comentarios nocivos por parte de usuarios anónimos (Touriño, 2014).

2.1.4. Derecho de Autodeterminación informativa

El derecho de autodeterminación informativa o *habeas data,* protegido por el derecho de protección de datos personales, hace referencia al derecho legítimo del individuo a "la libre disposición de los datos personales" (Gozaíni, 2011:67). Esto significa tener poder para decidir sobre el tratamiento que se va a realizar a los datos personales propios que han sido almacenados en distintos lugares; es decir, el ejercicio de la libertad informativa de uno mismo es la capacidad de controlar la información que le concierne. En concreto hay dos vías de controlar esta información, por un lado, consintiendo (de forma inequívoca, libre e informada) la captación y el tratamiento de los datos por terceros y, por otro lado, mediante la autorización expresa de la legislación (por ejemplo, los datos que recoge y analiza Hacienda, que no depende de la voluntad de la persona sino que consiste en un acto establecido por la ley). No obstante, ni el consentimiento ni la habilitación legal suponen la pérdida del poder sobre los datos, ya

[14] Trol: "vocablo de Internet que describe a una persona que solo busca provocar intencionadamente a los usuarios o lectores, creando controversia y reacciones predecibles, con fines diversos, desde el simple divertimento hasta interrumpir o desviar los temas de las discusiones, o bien enfadar a sus participantes y enfrentarlos entre sí." (Touriño, 2014: 142)

que existen una serie de derechos que complementan a la autodeterminación informativa (Murillo, 2007), que se pueden consultar en la siguiente tabla.

Tabla nº2: Derechos que complementan a la autodeterminación informativa

-Derecho a revocar la autorización del tratamiento de los datos personales.
-Derecho a ser informado de la recogida de datos personales.
-Derecho a conocer los ficheros y tratamientos en los que se almacenarán y analizarán los datos personales.
-Derecho de acceso a los datos personales recogidos para comprobar su exactitud y fidelidad a la realidad, así como para saber qué tipo de información se almacena sobre la persona.
-Derecho de rectificación de los datos que no sean exactos.
-Derecho de cancelación del tratamiento de los datos personales.
-Derecho de oposición a un tipo de tratamiento determinado de los datos personales que se considere innecesario o que no sea requerido por el consentimiento inicial.
-Derecho a no sufrir prejuicios derivados de la clasificación y análisis de los datos personales.
-Derecho a ser protegido por las instituciones que se han creado para asegurar la protección de datos y el derecho de autodeterminación informativa.

Fuente: Elaboración propia a partir de Murillo (2007)

El derecho de autodeterminación informativa es el derecho al control personal de la información que circula sobre el propio individuo. Quizás es el más vulnerable en la esfera digital, principalmente porque al ser ésta una magnitud inabarcable por una persona, nunca se llega a controlar con gran certeza qué información hay sobre un individuo en la red. Además, cuando sí que se encuentra un dato concreto y se quiere retirar o rectificar, no sólo depende de la plataforma web a la que se ha subido dicha información y del usuario en cuestión que la ha proporcionado (que puede ser hasta el mismo afectado), sino de en qué país está alojada la empresa que proporciona el servicio. Dependiendo del Estado en el que se encuentre, se podrá ejercitar el *habeas data* o no, ya que la jurisdicción tiene como límite la zona geográfica que legisla.

El derecho al olvido, que se desarrolla al final de este capítulo, supondría para el derecho de autodeterminación informativa su culminación. Hacer factible la retirada de

la información sobre la persona que no interesa que circule por la red significaría una ampliación del margen de actuación que dispone el usuario de Internet a la hora de gestionar su información.

2.2. Derecho a la protección de datos personales

El derecho a la protección de datos personales implica la protección de los derechos de la personalidad que hemos tratado anteriormente, ya que tiene por finalidad proteger la información personal del afectado cuyo almacenamiento o tratamiento suponga un agravio hacia la persona, a parte de crear nuevos derechos con la finalidad de dicha protección.

2.2.1. Definición y derechos que crea

El derecho de protección de datos personales es entendido en la Carta Europea de Derechos Fundamentales (art. 8) como aquel que posee toda persona a proteger los datos que le conciernen, los cuales serán tratados de forma leal y con la finalidad que haya sido establecida en el consentimiento por parte de la persona afectada. Además, este derecho implica la capacidad de acceso a los datos que le conciernen y a su rectificación si es pertinente. Por su parte, Pérez Luño, catedrático de Filosofía del Derecho de la Universidad de Sevilla, define la protección de datos como "el conjunto de bienes o intereses que pueden ser afectados por la elaboración de informaciones referentes a personas que pueden ser identificadas o identificables" (Sánchez Bravo, 1998: 53).

Se ha de entender dato personal como aquella información relativa a la persona que, o bien lo identifica de forma directa, como pueda ser el nombre, el DNI, el ADN, el email, etc; o bien de forma indirecta, como el color del pelo, la edad, el género, la localización geográfica, etc. También es un dato personal aquel que hace identificable a la persona, es decir, aquel que aunque no la identifica de forma directa hacer que sí que lo sea para ciertas personas, por ejemplo *la chica que vino ayer preguntando por ti* es un dato que hace identificable a una persona pero por un conjunto reducido de individuos (Gutiérrez Zarza, 2012 y Heckh y Cárdenas, 2012). Los datos sensibles, considerados como una subcategoría de los datos personales, hacen referencia a "el origen racial o étnico, opiniones políticas, religiosas u otro tipo de creencias, salud, vida sexual, afiliación sindical o actividades criminales" (Gutiérrez Zarza, 2012: 52).

En lo que respecta al tratamiento o procesamiento de estos datos, que son las actividades que realizan con los datos personales (posesión, almacenaje, análisis, etc.), dependen del responsable del tratamiento, que es aquel que ejecuta el procesamiento de los datos, ya sea una persona física o jurídica, y el que se somete a la correcta aplicación de la ley en esta materia (Gutiérrez Zarza, 2012). El tratamiento de los datos no puede ser realizado sin el previo consentimiento por parte del afectado, que consiste en la "manifestación de voluntad libre, inequívoca, específica e informada, mediante la que el interesado consiente el tratamiento de sus datos de carácter personal" (Heckh y Cárdenas, 2012: 11).

La protección de datos implica el cumplimiento de una serie de normas por los responsables del tratamiento, concretamente los datos deben ser: "procesados de manera lícita y leal; almacenados con una finalidad específica y legítima, y no procesados de manera incompatible con tal finalidad; adecuados, relevantes y no excesivos; exactos y, cuando sea necesario, actualizados; mantenidos no más allá del tiempo necesario para el cumplimiento de la finalidad para la cual fueron recogidos." (Gutiérrez Zarza, 2012: 54)

Es de suma importancia el ámbito en el que se haga este procesamiento de datos, ya que la legislación que garantiza el derecho de protección de datos personales, ya sean en formato de texto, imagen o sonido, sólo actúa en el territorio legislado y sobre las empresas que tengan una sede ahí (en nuestro caso sería Europa). Dentro de ese ámbito la regulación se aplica a cualquier tramitación, automática o no, de los datos personales (Gutiérrez Zarza, 2012).

Para entender mejor los derechos que crea la regulación del derecho de protección de datos personales, vamos a analizar el caso español, regulado por la Ley Orgánica de Protección de Datos 15/1999 (LOPD). En concreto aquellos que reconoce la ley de forma específica a las personas físicas son el derecho de acceso, de cancelación, de rectificación, de oposición, de indemnización, de información, de impugnación de valores de la persona y de consulta al Registro de la Agencia Española de Protección de Datos (AEPD) (Acedo, 2012).

El derecho de acceso a los datos reconoce la capacidad de toda persona a consultar la información personal que haya sido recogida y almacenada, así como su origen y las comunicaciones realizadas o que se prevean realizar. Además, este acceso será de forma gratuita, y si la entidad no contesta a esta petición en un rango inferior a 30 días, la

persona tiene derecho a presentar una denuncia. El derecho de cancelación o derecho de bloqueo hace referencia a la potestad de la persona a pedir la inutilización de sus datos, y en todo caso, su eliminación, pero ésta sólo procede cuando no hay una razón jurídica para conservarlos. El derecho de rectificación supone poder reclamar la modificación de los datos cuando estos resulten inexactos o incompletos. El derecho de oposición consiste en la potestad del individuo de negarse a un tratamiento concreto de sus datos personales. El plazo máximo de espera para la contestación de la entidad ante la reclamación de estos últimos tres derechos comentados es de 10 días, sino la persona afectada puede presentar una denuncia. El derecho de indemnización hace referencia a la potestad que tiene el individuo de reclamar un resarcimiento por un daño o una lesión en sus bienes o intereses a partir del tratamiento de los datos. El derecho de impugnación de valores personales reconoce la facultad de la persona interponer un recurso contra una resolución judicial fundada en el tratamiento de los datos personales que evalúen su personalidad, también otorga la potestad de ser informada de los criterios que le fueron aplicados a este tratamiento. El derecho de consulta del Registro de la AEPD garantiza el derecho del individuo a conocer la información, los tratamientos que reciben, su finalidad y la identidad de los responsables del tratamiento de forma gratuita (Acedo, 2012).

Podemos concluir que el objetivo final del derecho de protección de datos es evitar la captación y procesamiento ilegal de los datos, "de este modo se elimina -al menos parcialmente- el llamado 'rumor informático' y se instala una valla a las empresas que hacen las bases de datos su fuente de comercialización" (Alfredo Gozaíni, 2011: 118).

2.2.2. Marco jurídico

El marco jurídico del derecho de protección de datos se presenta en dos ámbitos, primero el comunitario (UE) y después el territorio estatal español. En el esquema que hay a continuación se puede observar una panorámica de ambos ámbitos. Los distintos componentes están ordenados cronológicamente y atendiendo al valor jurídico de cada instrumento.

Tabla nº3: Marco jurídico del derecho de protección de datos

	Ámbito europeo	Ámbito estatal español
Tratados	▪ Tratado de Funcionamiento de la Unión Europea (TFUE) ▪ Carta de los Derechos Fundamentales de la Unión Europea	▪ Constitución Española de 1978 ▪ Ley de Protección de Datos de Carácter Personal (LOPD) ▪ Reglamento de Protección de Datos de Carácter Personal ▪ Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico ▪ Ley de conservación de Datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones ▪ Ley General de Telecomunicaciones ▪ Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de usuarios ▪ Estatuto de la Agencia Española de Protección de Datos ▪ Normativa autonómica relevante
CdE	▪ Convenio 108 del Consejo de Europa ▪ Convenio Europeo de Derechos Humanos (CEDH)	
Instrumentos de referencia	▪ Directiva 95/46/CE del Parlamento Europeo y del Consejo ▪ Directiva 2002/58/CE del Parlamento Europeo y del Consejo ▪ Directiva 2006/24/CE del Parlamento Europeo y del Consejo ▪ Reglamento CE/45/2001 del Parlamento Europeo y del Consejo ▪ Propuesta de Reglamento comunitario ▪ Decisión Marco 2008/977/JAI ▪ Recomendaciones	

Fuente: Elaboración propia

La normativa europea se caracteriza por su proteccionismo hacia el ciudadano, como también se puede comprobar en el caso de la protección de datos, pudiendo establecer así un símil a la evolución que han sufrido los derechos humanos (Sánchez Bravo, 1998); ya que, como tal, un derecho fundamental debe ser siempre respetado. Los antecedentes al marco jurídico actual se encuentran el artículo 12 de la Declaración Universal de los Derechos Humanos de 1948, que garantizaba el derecho a la protección frente ataques a la vida privada; y en el Convenio Europeo para la Protección de Derechos Humanos y Libertades Fundamentales del Consejo de Europa de 1950, en el

que se reconoce el derecho a protección de la vida privada y familiar, del domicilio y de la correspondencia (Heckh y Cárdenas, 2012).

Si nos centramos en el marco jurídico vigente actual, como punto de partida y como uno de los dos fundamentos jurídicos de la protección de datos, encontramos el Tratado de Funcionamiento de la Unión Europea (TFUE), que es uno de los cuatro pilares que configuran la Constitución de la Unión Europea[15], en su artículo 16 se encuentra la protección de datos:

> "16(1). Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
>
> 16(2). El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes."

Tabla nº4: Marco legislativo vigente de la UE en relación con su valor jurídico

Tratados	-Tratado de Funcionamiento de la Unión Europea (TFUE) -Carta de los Derechos Fundamentales de la Unión Europea
Convenios	-Convenio 108 del Consejo de Europa -El Convenio Europeo de Derechos Humanos (CEDH)
Directivas	-Directiva 95/46/CE del Parlamento Europeo y del Consejo -Directiva 2002/58/CE del Parlamento Europeo y del Consejo
Reglamentos	-Reglamento CE/45/2001 del Parlamento Europeo y del Consejo
Decisiones	-Decisión Marco 2008/977/JAI

Fuente: Elaboración propia

La Carta de los Derechos Fundamentales de la Unión Europea, proclamada en el año 2000, es un Tratado de la UE, concretamente es el segundo fundamento jurídico relativo a la protección de datos y el principal instrumento legislativo. Lo referente a la protección de datos se encuentra en el capítulo II, relativo a las Libertades, el artículo 7 reconoce el derecho al respeto de la vida privada y familiar; y el artículo 8, reconoce el

[15] Los cuatro documentos que componen la Constitución Europea son: el Tratado de Funcionamiento de la Unión Europea (TFUE), el Tratado de la Unión Europea (TUE), el Tratado constitutivo de la Comunidad Europea de la Energía Atómica (Tratado Euratom) y la Carta de Derechos Fundamentales de la Unión Europea (CDF).

derecho a la protección de datos de carácter personal. La Carta no adquiriría carácter jurídico vinculante hasta 2009, ya que está integrada en el Tratado de Lisboa. Los redactores justifican la inclusión del derecho en la Carta por "la necesidad de actualizar los catálogos de derechos existentes a la luz del progreso tecnológico" (González Fuster, 2012: 51). Es así como el derecho a la protección de datos ha pasado a ser un derecho fundamental de todo ciudadano europeo, ya que se trata de un documento jurídicamente vinculante para todas las instituciones y órganos de la UE así como para sus Estados miembros.

Enmarcado en el Consejo de Europa (CdE), destacan dos convenios. Primero, el Convenio nº108, aprobado en 1981 y en vigor desde 1985, para la protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal, supone el inicio del desarrollo del resto de normas reguladoras. Este convenio obliga a los Estados miembros a tomar medidas que se encargasen de asegurar el cumplimiento de la protección de datos (Bru Cuadrada, 2007; Heckh y Cárdenas, 2012). Segundo, el Convenio Europeo de Derechos Humanos (CEDH) de 1950, anteriormente mencionado como antecedente a la normativa que reconoce el derecho al respecto de la vida privada y familiar.

Como instrumento legislativo de la UE en materia de protección de datos, encontramos las dos directivas principales que se encargan de la protección de datos. En primer lugar la Directiva 95/46/CE del Parlamento Europeo y del Consejo, que es de 1995, anterior a la Carta pero con menos valor jurídico que ésta; hasta el momento es "el instrumento jurídico más importante sobre protección de datos jamás aprobado por la UE" (González Fuster, 2012: 52). La Directiva 95/46/CE surge como "consecuencia del movimiento iniciado a partir de la suscripción del Convenio de 1981" (Heckh y Cárdenas, 2012: 13) referente a la protección de datos y establece el marco común mínimo de protección a partir del cual cada Estado miembro es libre de desarrollar la regulación de protección de datos conforme los principios que describe la directiva.

En segundo lugar, la Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, que al ser formulada después de la Carta de Derechos Fundamentales de la UE, ya hace referencia a la disposición del derecho de protección de datos como derecho fundamental en su Preámbulo. El objetivo de esta segunda directiva es

"proteger y custodiar la intimidad de los abonados y usuarios de servicios de comunicaciones electrónicas, para lo cual se diseña un catálogo con sus derechos, así como con las obligaciones de los prestadores de servicios" (Heckh y Cárdenas, 2012: 14). Esta directiva ha sido modificada en dos ocasiones a partir de la Directiva 2006/24/CE y la Directiva 2009/136/CE.

La Directiva 2006/24/CE, 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, conocida como Directiva de Retención de Datos, modificaba la Directiva 2002/58/CE. Esta directiva afectaba a los datos de tráfico y de localización de los usuarios de Internet y surgió a raíz de la necesidad de prevenir, investigar y enjuiciar delitos graves (Heckh y Cárdenas, 2012). El 8 de abril de 2014, el Tribunal de Justicia de la Unión Europea (TJUE) sentenció[16] la nulidad de la Directiva 2006/24/CE por ser contraria a los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea, aquellos que se encargan del derecho a la vida privada y de la protección de datos respectivamente. El principal motivo por el que se ha anulado ha sido por su redacción, el TJUE no condena la retención de datos sino la carencia de límites y a la falta de precisión en la regulación que establecía la Directiva (*Diario Jurídico*, 2014).

Siete años más tarde de su entrada en vigor, se modifica el artículo 5.3 de la Directiva 2002/58/CE mediante la Directiva 2009/136/CE, conocida como la Directiva de las *cookies*. Concretamente, se establece la obligación por parte del responsable del tratamiento de datos de informar sobre el uso que darán a la información recopilada a través de cookies y de pedir el consentimiento de esa obtención de los datos mediante esa vía.

En un estadio legislativo inferior, encontramos el Reglamento CE/45/2001, que como todo reglamento supone la aplicación directa a la normativa de los Estados miembros sin dejar que éstos la traspongan como ellos convengan oportuno, es relativa al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. Permitió establecer los principios básicos de

[16] Sentencia del asunto C-293/12 del 8 de abril de 2014, por la que se anula la Directiva 2006/24/CE: http://curia.europa.eu/juris/liste.jsf?num=C-293/12&language=es#
Directiva 2006/24/CE:
http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.4-cp--Directiva-95-46-CE.pdf

actuación para garantizar los datos personales tratados por las instituciones y los organismos de la UE, además creó la figura del Supervisor Europeo de Protección de Datos, una autoridad europea independiente que controla el cumplimiento de la normativa relativa a la protección de datos en las instituciones y órganos europeos (Heckh y Cárdenas, 2012).

Las perspectivas de futuro apuntan hacia el cambio de la Directiva 95/46/CE principalmente por la necesidad de su actualización al paradigma digital vigente. En enero de 2012, la Comisión Europea presentó una propuesta legislativa para sustituir a la Directiva 95/46/CE y hacerla más efectiva (Palacios González, 2012), mediante una nueva Directiva y un nuevo Reglamento que "incluye disposiciones sobre su reconciliación con otros intereses y derechos, como el derecho a la libertad de expresión, aunque carece de un mecanismo específico de reconciliación con la protección de los derechos de autor" (González Fuster, 2012: 60). La nueva Directiva sustituiría además a la vigente Decisión Marco 2008/977/JAI, que protege los datos personales en casos que van a ser empleados en un proceso judicial y policial. Las autoridades componentes de los Estados miembros que han ratificado esa decisión únicamente pueden obtener y guardar los datos de las personas con determinados fines, explícitos y legítimos, y exclusivamente para el fin para el que han querido recopilarlos. Sólo podrán hacer uso de estos datos para otros fines cuando sea con el objetivo de prevenir, investigar o detectar otras infracciones penales, como norma general la persona de la que se obtienen los datos deberá estar informada, a no ser que se pasen los datos de un Estado a otro y el primero no desee que se informe al interesado, si se detecta que el interesado ha sufrido algún menoscabo en sus derechos y estos datos han sido utilizados ilícitamente podrá realizar un recurso judicial[17].

La exposición de la vida privada en las redes sociales se ha convertido en una preocupación institucional a nivel internacional, por este motivo se han realizado distintas recomendaciones dirigidas a los usuarios, a los fabricantes de software, a los proveedores de redes sociales y a los reguladores y administraciones públicas. En el nivel supranacional destaca el documento[18] elaborado por la European Network and Information Security Agency (ENISA), la *resolución relativa a la protección de la privacidad en los servicios de redes sociales, aprobada en la 30ª Conferencia*

[17] Decisión Marco 2008/977/JAI
[18] Security Issues and Recommendations for Online Social Networks, 2007.

Internacional de privacidad y Autoridades de protección de datos el 17 de octubre de 2008 en Estrasburgo y el documento de recomendaciones del Memorándum de Montevideo, adoptado en julio 2009, dando relevancia a la protección de la privacidad de los menores en la red. Las instituciones advierten de la necesidad de formación en el uso de las redes sociales, de mejorar el diseño de la plataforma web para que proteja más la privacidad y de introducir medidas tecnológicas que controlen la privacidad (Vilasau, 2009). La mayoría de instituciones coinciden en el deber que tienen las políticas de privacidad de regular este aspecto y en la obligación de información por parte de las empresas de comunicación social.

En el ámbito estatal español, en el marco jurídico de la protección de datos de carácter personal destaca, en primer lugar, la Constitución Española de 1978, en su artículo 18 relativo al derecho a la intimidad personal y familiar, en el que se reconoce la protección de datos. La LOPD 15/1999 es la normativa que desarrolla en España el derecho fundamental de protección de datos de carácter personal, traspuesta de la Directiva 95/46/CE. El Reglamento de Protección de Datos de Carácter Personal, aprobado en 2007, que regula la LOPD así como "aquellas cuestiones que, tras los primeros años de vigencia de esta Ley, se habían manifestado problemáticas o con una definición o regulación insuficiente" (Heckh y Cárdenas, 2012: 16).

Existen otras leyes que afectan también a la protección de datos, como la ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, la ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones y la ley General de Telecomunicaciones. Por su parte, el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de usuarios también regula las "obligaciones de los operadores y prestadores de servicios relativas a la protección de datos de carácter personal en la explotación de redes y en la prestación de servicios de comunicaciones electrónicas disponibles al público" (Heckh y Cárdenas, 2012: 17).

Finalmente, el Estatuto de la Agencia Española de Protección de Datos (AEPD) desarrolla la normativa por la que se rige la AEPD, organismo que tiene como objetivo el control del cumplimiento de la normativa de protección de datos vigente en el territorio español. En última instancia, se encuentran las normativas autonómicas existentes relevantes a la protección de datos, ya que algunas comunidades han dictado

sus propias normas relativas a la protección de datos e incluso han incorporado su propia agencia supervisora. Es el caso de Cataluña y la Autoridad Catalana de Protección de Datos, el País Vasco y la Agencia Vasca de Protección de Datos y Madrid y la Agencia de Protección de Datos de la Comunidad de Madrid (Heckh y Cárdenas, 2012).

2.2.3. Derecho al olvido

El derecho al olvido surge a partir de la necesidad de retirar cierta información veraz de Internet sobre la persona, perteneciente a un pasado, que no tiene ninguna justificación legal para continuar en línea, afectando con ello a su imagen digital. Es el derecho "para cribar aquellos datos personales susceptibles de minar los derechos de la personalidad: honor, intimidad e imagen" (Abril y Pizarro, 2014:10). Esto es, el "derecho del individuo a eliminar o hacer inaccesibles ciertos datos o información publicados en el entorno digital y que se encuentran indexados por buscadores de Internet" (Touriño, 2014: 140). El acceso y localización de la información se han vuelto sencillos y ágiles, permitiendo con ello encontrar cualquier dato publicado de una antigüedad considerable con una velocidad vertiginosa. Esto supone que los datos y hechos que están en la red, no se quedan en el pasado, si no que resurgen cada vez que están relacionados con la búsqueda que se realiza.

La petición del derecho al olvido nace en España, en el año 2010 promovida por Mario Costeja, un jurista afectado por la constante aparición de una noticia antigua, publicada en 1998, del periódico catalán "La Vanguardia" en la que se anunciaba la subasta del domicilio suyo y de su pareja por impago. El abogado reclamaba el retiro de dicha noticia del buscador Google alegando su protección a la privacidad y el perjuicio que le estaba causando. La persona había dejado aquel hecho atrás, ya no es moroso y tampoco tiene pareja, y cada vez que alguien consulta su nombre en la red aparece dicha noticia, impidiéndole así dejar atrás ese hecho y poder *empezar de cero* (Touriño, 2014). Este caso fue el que empezó con la demanda de este tipo de protección, pero en España hay más de 220 casos relacionados que están esperando ser resueltos por el TJUE (*El País*, 2014b). Tras la negativa del periódico a Costeja para retirar la información, éste acude a la Agencia Española de Protección de Datos (AEPD), quien realiza una resolución en la que reclama a Google Spain y a Google Inc. que retire la indexación de esta noticia en base a la protección del derecho al honor del afectado. Acto seguido, Google interpone un recurso ante la Audiencia Nacional reclamando la nulidad de la resolución de la

AEPD. El Tribunal de la Audiencia Nacional remite el caso al Tribunal de Justicia de la Unión Europea. El 25 de junio de 2013 se publican las conclusiones del Abogado General del TJUE, que propiciaban que la sentencia iba a ser a favor de Google y que Mario Costeja iba a perder la batalla. Esto fue debido a que según la legislación actual, el buscador no está obligado a controlar su contenido. El afectado tiene que dirigirse a la plataforma que haya publicado el contenido, no a quien lo indexa, para retirar tal información. Esto se fundamenta en que "el derecho comunitario no faculta a una persona para restringir o poner fin a la difusión de datos personales que considere lesivos o contrarios a sus intereses." (Touriño, 2014: 40)

Tabla nº5: Cronología del caso de Mario Costeja y el derecho al olvido

1998 La Vanguardia publica dos anuncios de una propiedad sacada a subasta a causa de un embargo por deudas a nombre de Mario Costeja
2009 Mario Costeja acude a la AEPD y reclaman a Google Spain y a Google Inc. que retire los datos solicitados por el demandante
2010 Google interpone un recurso ante la Audiencia Nacional. Reclama la nulidad de la resolución de la AEPD
2012 El Tribunal español remite al TJUE Propuesta de reforma de la Directiva de Protección de Datos por parte de la Comisión Europea donde se reconoce el derecho al olvido
2013 Se publican las conclusiones del abogado general del TJUE sobre el Derecho al Olvido por la Audiencia Nacional
2014 El TJUE dicta sentencia a favor de Mario Costeja, obligando a Google a implementar el Derecho al Olvido en la UE

Fuente: Elaboración propia

El derecho al olvido había sido hasta el momento un supuesto teórico y sigue sin estar desarrollado ni implementado en ninguna legislación ni reglamento. Estaba previsto que la UE lo reconociera por primera vez con la aprobación de la propuesta que presentó la Comisión Europea en 2012, donde se contempla este derecho. Sin embargo, finalmente,

sin ser esperada, la sentencia del 13 de mayo de 2014 del TJUE del caso de Mario Costeja [19] ha cambiado la situación actual. El TJUE le ha dado la razón a la AEPD, obligando a Google a retirar la información que perjudicaba al afectado.

Mientras se espera la aprobación de la reforma planteada por la Comisión, la sentencia del TJUE del caso de Mario Costeja ya ha supuesto un avance en la legislación de este derecho. Concretamente, en esta sentencia ha habido cuatro declaraciones:

1) La indexación de contenidos por el buscador es considerada como tratamiento de datos personales, recayendo el papel de responsable del tratamiento al buscador.

2) Será aplicada la normativa europea de protección de datos cuando el motor de búsqueda establezca una sucursal física en el Estado miembro para gestionar la venta de espacios publicitarios y dirigir su actividad a los ciudadanos del Estado miembro.

3) Para respetar los derechos de la personalidad, el buscador está obligado a eliminar de su lista de resultados, obtenida tras la búsqueda de un nombre en concreto, aquellos enlaces que contengan información vinculada al nombre de una persona y que demuestren ser perjudiciales para ella, si así lo solicita el interesado.

4) Se debe examinar si el interesado tiene derecho a eliminar esa información.

El derecho a la vida privada y a la protección de datos deben prevalecer al interés económico del buscador y del acceso al público. Sin embargo, pone como ejemplo de excepciones a las personas con cargo público, en cuyo caso la injerencia en sus derechos fundamentales está justificada por el interés del público y su derecho de acceso a la información.

Esta sentencia supone un hito histórico en el derecho al olvido, siendo la primera vez que este se reconoce en la UE. A partir de ahora, los usuarios se pueden dirigir directamente a Google para que elimine de su índice de resultados derivado de la búsqueda del nombre de la persona aquella información que sea perjudicial para ésta o que ya no sea relevante. En el caso de que el motor de búsqueda no realice este servicio, el usuario puede acudir a la autoridad de protección de datos independiente de su país

[19] Sentencia del asunto C-131/12 del día 13 de mayo de 2014, referente al caso de Mario Costeja y Google:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=260957

(la AEPD en España) para que intervenga en el proceso (*La Vanguardia*, 2014). Esto no significa que esa información vaya a ser eliminada de la red, sino que no aparecerá accesible a partir de la búsqueda. La eliminación del contenido no depende de Google sino del editor digital que haya publicado la información en su portal y es a esa persona a quien también habrá de acudir el interesado si quiere eliminar definitivamente cierta información. "Solo se elimina de los resultados de los buscadores para que los datos lesivos no permanezcan eternamente en Internet" (*El País*, 2014b)

Autores como Touriño (2014), abogado experto en Derecho en Internet, afirman que el derecho al olvido ha nacido muerto. Tales afirmaciones se deben a los múltiples inconvenientes que encuentra este derecho para poder ejercerse, como son el alcance limitado de su protección, ya que los problemas relacionados con la privacidad de datos quedaría al margen de esta protección por la aceptación de los términos y condiciones de uso del afectado. La información anónima también supondría un problema, ya que si se desconoce la fuente que lo ha publicado difícilmente se puede contactar con ella para proceder a su retirada. La censura sutil sería una posible consecuencia de la aplicación de este derecho, porque si las personas deciden eliminar cualquier información que no les interese, la información que quedase en la red no sólo sería incompleta, sino que estaría totalmente controlada. Existen diversas dificultades prácticas porque la sencillez con la que se comparten y multiplican los contenidos en Internet, no se puede asegurar el borrado de cierta información de toda la web (Abril y Pizarro, 2014).

Establecer una fecha de expiración en la red para ciertos contenidos es una de las posibilidades de actuación de este derecho que propone para este problema Jef Ausloos, investigador del Centro Interdisciplinario de Derecho y TIC de Holanda, aunque él mismo reconoce que esta posibilidad es inviable. Es decir, que la regulación del derecho al olvido incluyera la obligación de incluir esta fecha de caducidad en el sistema o plataforma digital, para asegurar la eliminación de ciertos contenidos con el paso del tiempo, sin necesidad de realizar una petición formal. Propone también la creación de gerentes de reputación, es decir, páginas web encargadas de controlar la información que hay disponible de una persona en la red y que tengan por objeto la defensa de su reputación online (Abril y Pizarro, 2014).

Podríamos considerar el derecho al olvido como un instrumento que ofrece la posibilidad de desarrollar el derecho de protección de datos de forma activa para el

afectado. Es decir, que todo ciudadano tendría no sólo un derecho protector (o pasivo) de sus datos, sino que también tendría la posibilidad de ejercer un derecho activo y eliminar aquella información que considere innecesaria o inapropiada, consiguiendo así un mayor control o dominio de los datos de dominio público que le afectan.

CAPÍTULO 3

LA POLÍTICA DE LA UNIÓN EUROPEA PARA LA PROTECCIÓN DE DATOS

En Europa, el derecho a la privacidad, a la intimidad y a la protección de datos son considerados como derechos fundamentales, derechos que cualquier Estado miembro debe garantizar a los ciudadanos. La protección de datos está desarrollada en un marco legislativo de distintos niveles de valor jurídico, como se ha visto en el capítulo 2, teniendo como principales referencias la Directiva 95/46/CE del Parlamento Europeo y del Consejo, que establece las pautas de gestión de los datos personales otorgando también derechos a los titulares de los datos; y la Directiva 2002/58/CE, sobre la privacidad y las comunicaciones electrónicas, que garantiza el tratamiento de los datos personales y la protección de la privacidad de las comunicaciones electrónicas, con sus correspondientes leyes que las desarrollan y finalmente las agencias nacionales de protección de datos.

Este marco legislativo, relativo a la protección de datos, se puso en revisión desde 2007 a 2010 por la Comisión Barroso II[20]. La intención era conseguir un modelo regulador comunitario que sea igual para todos los Estados miembros, ya que las Directivas actuales han sido traspuestas a los países comunitarios de forma muy diversa. Los objetivos de esta revisión eran "la modernización de dicho marco legal, teniendo en cuenta los cambios que resultan de la globalización y el uso de nuevas tecnologías, el fortalecimiento de los derechos de los individuos, y la mejora de la claridad y la coherencia de las numerosas normas europeas sobre tratamiento y protección de datos personales" (Gutiérrez Zarza, Michael Alexander y Sutton, 2012: 97). Durante el periodo de revisión se realizaron dos informes[21] que demostraron las disparidades con las que se habían traspuesto las Directivas en los distintos estados de la UE.

El proceso de revisión concluyó con la presentación de la propuesta de la Comisión Barroso II en 2012, que actualmente, en 2014, está siendo debatida por el Consejo y se

[20] Los miembros de la Comisión Barroso II (2010-2014), se pueden consultar en el siguiente enlace: http://ec.europa.eu/commission_2010-2014/members/index_en.htm

[21] European Commission. Report from the Commission. First report on the implementation of the Data Protection Directive (95/46/CE) COM (2003) 265 final.

European Commission. Communication from the Commission to the European Parliament an the Council on the follow up of the Work Programme for better implementation of the Data Protection Directive. COM (2007) 87 final.

prevé que será efectiva a partir de 2015-2016. Esta propuesta consiste en implantar una nueva Directiva que sustituya a la 95/46/CE y su correspondiente Reglamento. Con la aprobación del Reglamento y su consecuente regulación igualitaria de una legislación común entre los Estados miembros se podrán afrontar los problemas relacionados con la privacidad y la protección de datos a través de Internet con mayor facilidad al poseer normas comunes, ya que si ya es difícil lidiar con el alojamiento de los contenidos y las empresas y sus correspondientes jurisdicciones, tener distintas normativas dentro de la misma UE complica aún más el proceso de protección de datos.

Dentro de las instituciones comunitarias, es la Comisión Europea la encargada de elaborar la política de protección de datos, concretamente el área de Justicia y Derechos de los ciudadanos, donde cuentan con una sección especial para la regulación de la protección de datos.

Este capítulo se centra en la explicación de la política de la Unión Europea en lo relativo a la protección de datos. En primer lugar se abordan los actores responsables de definir y ejecutar la política. En segundo lugar, se realiza una descripción de la política europea que hay en vigor en 2014, concretamente se revisan las Directivas 95/46/CE y 2002/58/CE. En tercer lugar vemos qué instrumentos legislativos sostiene la política y cuáles son los mecanismos que habilita la regulación para poder hacerla efectiva. En cuarto lugar, se analiza quién la aplica y la controla. Y, finalmente, se hace una descripción de la situación actual a fecha de junio de 2014. Primero se describe a grandes rasgos qué supone la reforma de la política de protección de datos presentada por la Comisión Barroso II. A continuación, se profundiza en la nueva situación del Derecho al Olvido a raíz de la sentencia del TJUE del 13 de mayo de 2014 y, seguidamente, se explica la protección de datos dentro de la Estrategia 2020 y su programa de financiación, Horizonte 2020, en tanto que perspectivas de futuro.

3.1. ¿Quién es responsable de definir y ejecutar esta política?

La política de protección de datos de la Unión Europea es realizada por los distintos actores que intervienen en su legislación. La Comisión Europea[22] es el órgano ejecutivo, aunque tiene el derecho de iniciativa legislativa, es decir, es la organización que propone las leyes al Parlamento Europeo, organismo que finalmente quien debate y

[22] Actualmente presidida desde 2004 por el político portugués José Manuel Durão Barroso

aprueba la legislación europea junto con el Consejo Europeo. En la Comisión Barroso II, las políticas de protección de datos dependen del área de Justicia y Derechos de los ciudadanos[23], que se encarga de las políticas en materia de justicia, derechos fundamentales y ciudadanía. La Dirección General de Justicia de la Comisión Europea[24] (DG Justicia) es el departamento de la Comisión que se encarga del área política de Justicia. La Dirección General de Justicia está compuesta por cuatro Direcciones, de las cuales, la que se encarga de la protección de datos es la de Derechos Fundamentales y Ciudadanía de la Unión[25]. Es el director de cada DG quien informa al Comisario de la Unión Europea que está a cargo del área política correspondiente. Es decir, la Comisión es quien tiene la iniciativa legislativa y, por lo tanto, propone regulación a partir de las orientaciones del Consejo. En este sentido, una vez se ha dado a la Comisión el mandato de legislar sobre la protección de datos, es la Dirección General de Justicia de la Comisión quien, efectivamente, propone el marco legislativo, que debe ser aprobado por Parlamento y Consejo. No obstante, hay ciertos ámbitos en los que no sólo regula la protección de datos el DG Justicia, en los ámbitos de protección e intercambio de datos para la lucha contra el terrorismo interviene también la Dirección General de Interior, por ejemplo, en el acuerdo con EEUU sobre el registro de datos de pasajeros[26]. También es el caso de la estrategia de la Agenda Digital (que se tratará al final de este capítulo), donde se ha colaborado con la DG Connect para los temas que tienen que ver con la protección de datos[27].

La ejecución de la política depende tanto de la Comisión Europea, que vela por el cumplimiento de la legislación y su correcta aplicación en todos los Estados miembros, como de los Estados miembros. Sin embargo, cabe mencionar también al Tribunal de Justicia de la Unión Europea (TJUE), ya que no sólo se encarga de administrar justicia, sino que sienta precedentes legislativos con las distintas sentencias que versan sobre aspectos legales que o bien no están bien limitados o bien ni si quiera están definidos,

[23] La Comisaria del área de Justicia y Derechos de los ciudadanos de la Comisión Barroso II es Viviane Reding, política luxemburguesa que ostentaba además el cargo de Primera Vicepresidenta de la Comisión durante el periodo legislativo de 2010-2014. De ella dependía, pues, la Dirección General de Justícia, cuya directora es Françoise Le Bail, pero también dependían otras direcciones generales.

[24] La Directora General de Justicia de la Comisión Europea desde 2010 hasta la actualidad es Françoise Le Bail http://ec.europa.eu/justice/mission/director-general/index_es.htm

[25] Dentro de la Dirección de Derechos Fundamentales y Ciudadanía de la Unión, la persona encargada de la unidad de Protección de Datos es Marie-Hélène Boulanger, que ocupa su cargo desde 2009 hasta la actualidad http://ec.europa.eu/justice/about/files/organisation_chart_en.pdf

[26] http://europa.eu/rapid/press-release_MEMO-13-1054_en.htm

[27] http://ec.europa.eu/dgs/connect/en/content/dg-connect

como ha sido el caso del derecho al olvido, reconocido por primera vez por el TJUE y creando a partir de su fallo los principios legislativos de este derecho. Por lo tanto, aunque no constituya como tal un órgano legislativo, sus decisiones sí que son incorporadas a la legislación europea directamente.

3.2. ¿Cómo se define la política?

La política adoptada por la Unión Europea relativa a la protección de datos tiene dos pilares: la Directiva 95/46/CE sobre la protección de datos, que es su eje principal y de referencia; y la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas, que constituye la parte de la política referente a la protección de datos y la privacidad de las telecomunicaciones. Estas directivas son transpuestas por cada Estado miembro a su marco jurídico de la forma que estime más adecuada.

3.2.1. Directiva 95/46/CE

La Directiva 95/46/CE[28] establece las bases regulatorias de la protección de datos personales de la Unión Europea. Tiene como objeto conseguir que el tratamiento de los datos personales respeten las libertades y los derechos fundamentales, concretamente la intimidad. Además, debe "contribuir al progreso económico y social, al desarrollo de los intercambios así como al bienestar de los individuos" (considerando 2).

La política entiende como necesaria "la libre circulación de datos personales de un Estado miembro a otro" (considerando 3) y "la protección de los derechos fundamentales de las personas" (considerando 3). Los Estados deben garantizar que los datos no serán utilizados para "tomar medidas o decisiones contra cualquier persona" (considerando 29). Tiene en cuenta que ha aumentado y facilitado el tratamiento e intercambio de datos personales tanto en el sector de la actividad económica como en el social. Considera además los distintos niveles de protección de la intimidad y de los datos personales que existen en los Estados miembros, que suponen una dificultad para la transmisión de los datos de un Estado a otro, impidiendo así posibles actividades económica a escala comunitaria. Especifica que esta disparidad regulatoria no se puede

[28] Directiva 95/46/CE (en español):
http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/directivas/common/pdfs/B.4-cp--Directiva-95-46-CE.pdf
Síntesis de la legislación de datos personales en la UE (Directiva 95/46/CE):
http://europa.eu/legislation_summaries/information_society/data_protection/l14012_es.htm

solucionar solo con la actuación de los Estados miembros, justificando así la intervención legislativa de la Comunidad.

Sin disminuir la protección a la intimidad o al tratamiento de datos automatizado ya establecidas anteriormente en otros instrumentos legales de la Comunidad, esta Directiva pretende si acaso ampliar su regulación y garantizar la protección de los derechos y libertades de las personas. La Directiva regula todos los tratamientos de datos personales excluyendo aquellos efectuados por "una persona física en el ejercicio de actividades exclusivamente personales o domésticas, como la correspondencia y la llevanza de un repertorio de direcciones" (considerando 12).

La Directiva no afecta a lo referente a la seguridad pública, la defensa, la seguridad del Estado y las actividades del Estado en ámbito penal, es decir, el tratamiento de datos que se pueda realizar para "la salvaguardia del bienestar económico del Estado" (considerando 13), no está regulado bajo esta Directiva. Esto implica que los datos que pueden recoger, por ejemplo, las cámaras de videovigilancia, al ser recogidos con motivos de seguridad pública o defensa, no se puede aplicar la regulación de esta Directiva. Mientras que aquellos datos que se recojan con finalidades periodísticas o artísticas, sí que se aplican los principios legales establecidos en la Directiva 95/46/CE.

La Directiva 95/46/CE se encarga de la protección de datos personales entendiéndose estos como aquellos que identifican o hacen identificable a una persona, aplicándose dicha protección tanto al tratamiento automático como al manual. Estipula que todo tratamiento de datos personales debe realizarse forma lícita y leal con respecto al interesado, los cuales deben haber sido recogidos atendiendo a unos objetivos concretos explícitos y legítimos, especificados a la hora de obtener los datos. La información recolectada debe ser adecuada, pertinente y no excesiva para cumplir con los objetivos, consentidos por el interesado.

La Directiva reconoce y garantiza el derecho de acceso a los datos personales a los titulares de dicha información, así como el derecho a "conocer la lógica que subyace al tratamiento automatizado de los datos que la conciernan" (considerando 41). El derecho de oposición al tratamiento, siempre que esté basado en unos argumentos fundados y legítimos. Además, establece que en el caso de la persona sufra daños debido a un tratamiento ilícito, serán reparados por el responsable del tratamiento de datos. La Directiva sostiene que deben imponerse sanciones a todas aquellas personas que no

respete la regulación. En general, la Directiva permite que cada Estado miembro ponga las excepciones convenientes a cada derecho u obligación que estipula, siempre que sean debidamente justificadas y no vayan en contra de los principios generales de la regulación. Sin embargo sí que especifica que cuando se trasponga la Directiva en cada Estado miembro, éste añada en su legislación un recurso judicial para aquellos casos en los que el responsable del tratamiento de los datos personales no respete los derechos del afectado y los principios jurídicos establecidos.

La Directiva también impone la creación de una autoridad de control independiente del Estado que disponga de los medios necesarios para cumplir su función, es decir, que esté dotada de poder para investigar e intervenir en lo relativo a la protección de datos de su Estado. Asimismo, también establece la creación de un grupo de trabajo de protección de las personas (Grupo de Trabajo del Artículo 29), en lo referente a la protección de datos, de ámbito comunitario, independiente, con capacidad de asesorar a la Comisión y contribuir a la aplicación de las normas.

La Directiva regula diversos principios jurídicos que se deben aplicar a cualquier tratamiento automático de datos personales así como a cualquier tratamiento que implique almacenarlos. Los principios hacen referencia a la calidad de los datos, que tal y como estipula la Directiva deben ser tratados de manera lícita y leal, deben ajustarse a los fines para los que se recojan, que también deben ser explícitos y legítimos. Los datos procesados deben ser exactos y, si es necesario, actualizados. En lo que respecta a su conservación, se establece que debe ser de "forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente" (art. 6.1e).

Cuando se refiere a que el tratamiento ha de ser lícito y leal se refiere a que debe cumplir con una serie de características una vez el afectado haya dado el consentimiento de forma inequívoca. Entre ellas destaca la prohibición del tratamiento de datos personales sensibles (aquellos que revelan el origen racial o étnico, las creencias religiosas, sindicaciones políticas, la tendencia sexual, etc.), la confidencialidad y la seguridad que debe seguir el tratamiento (trabajar con datos que hayan sido cedidos previamente y adoptar las medidas necesarias que garanticen la protección de los datos).

Tabla nº6: Principales características de la Directiva 95/46/CE

Directiva de la protección de datos (95/46/CE)
Se aplica a
"todos los tratamientos de datos personales cuando las actividades del responsable del tratamiento entren en el ámbito de aplicación del Derecho comunitario"
Los Estados miembros deben asegurar que los Datos Personales sean
-"Tratados de manera leal y lícita" (Art. 6.1a) -"Recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines" (Art. 6.1b) -"Adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente" (Art. 6.1c) -"Exactos y, cuando sea necesario, actualizados" (Art. 6.1d) -"Conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente" (Art. 6.1e)
Los Estados miembros deben garantizar el cumplimiento de los siguientes derechos
-Derecho de acceso -Derecho a la confirmación del tratamiento de datos -Derecho a recibir información sobre los propósitos del tratamiento -Derecho de rectificación, borrado o bloqueo de los datos -Derecho de oposición -Derecho a un recurso judicial en caso de violación de derechos -Derecho a recibir una reparación del responsable del tratamiento de los datos en caso de perjuicios por un tratamiento ilícito
El responsable del tratamiento deberá
-Garantizar el cumplimiento de estos principios -Informar a la persona sobre la identidad del responsable del tratamiento y los fines -Obligaciones: -Mantener la confidencialidad del tratamiento de los datos -Implementar medidas técnicas y de organización adecuadas para la protección de los datos -Notificar a la autoridad nacional de control un conjunto de información sobre el tratamiento de los datos previo a su realización
Los Estados miembros deberán establecer autoridades independientes para el control, investigación e intervención en procesos de protección de datos
La Directiva crea el Grupo de Trabajo del Artículo 29 para estudiar las cuestiones relativas a la aplicación de la Directiva

Fuente: Elaboración propia a partir del texto de la Directiva 95/46/CE

No obstante, antes de cualquier tratamiento e incluso antes de pedir cualquier consentimiento, el proyecto de tratamiento ha de ser comunicado a la autoridad de control nacional, que llevará a cabo un estudio en el que detecte posibles riesgos para la seguridad de los afectados.

El articulado de la Directiva 95/46/CE establece dos tipos de principios que deben considerarse para la protección de datos, los que hay que cumplir para recabar datos y los que hay que respetar para su tratamiento o procesamiento. Los primeros son los principios de lealtad, de finalidad e utilización no abusiva, de pertinencia, de exactitud, de derecho al olvido –localizados en el artículo 6-; y los principios de prohibición de tratamiento de datos personales relativos al origen racial, a las convicciones religiosas, a la pertenencia de sindicatos, a la sexualidad y al estado de salud –localizados en el artículo 8-. Los segundos son los principios de confidencialidad de los datos recogidos, de seguridad y consentimiento del interesado (Bru Cuadrada, 2007). En lo que respecta a las sanciones –capítulo III-, la Directiva deja esa responsabilidad a los Estados, dándoles libertad para establecer los recursos y sanciones necesarias (Bru Cuadrada, 2007).

Desde que se aprobó dicha directiva, el marco legal se ha ido ampliando y modificando, pero la Directiva 95/46/CE sigue estando en vigor y sigue siendo el acto legislativo principal en materia de protección de datos. La Directiva 2002/58/CE, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas, es un desarrollo de la Directiva 95/46/CE (González Fuster, 2012). La Directiva 2006/24/CE, 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 supone otra actualización de la normativa. La Directiva 2009/136/CE modifica el artículo 5.3 de la Directiva 2002/58/CE (Palacios González, 2012).

La Directiva 95/46/CE sigue en vigor a pesar de haber sido modificada y ampliada posteriormente por otras directivas. La nueva propuesta presentada por la Comisión Barroso II en enero de 2012 supondrá un cambio, que no modificación, de la directiva actual. Dicha propuesta tiene por objetivo proteger los datos personales en toda la UE, aumentar el control por parte los usuarios sobre sus propios datos y reducir los costes para las empresas. La directiva de 1995 ha sido transpuesta por los Estados miembros

de formas diversas, atendiendo cada uno a la adecuación de su marco jurídico. La propuesta legislativa de la Comisión, al contener un Reglamento, equivaldría a la unificación y administrativa de todos los países de la UE.

3.2.2. Directiva 2002/58/CE

La Directiva 2002/58/CE[29], sobre la privacidad y las comunicaciones electrónicas, se encarga de la protección de datos y la privacidad de los usuarios pero en el contexto específico de las comunicaciones que se establecen a partir de tecnologías electrónicas, como es el caso de aquellas que se realizan a través de Internet, móvil y aplicaciones digitales. Es decir, aborda la protección de datos en el ámbito de prestación de servicios de telecomunicaciones. Esta Directiva regula los requisitos que deben cumplir los operadores de telecomunicaciones, complementándose así a la Directiva 95/46/CE, ya que se aplica tanto al tratamiento de los datos como a los datos de tráfico y de localización.

La Directiva 2002/58/CE establece unas medidas de seguridad y control de las comunicaciones electrónicas que deben ser cumplidas por los proveedores de dichos servicios, que deben garantizar tanto la seguridad como la confidencialidad de los servicios y los datos personales. Se debe garantizar la privacidad de las comunicaciones, prohibiendo escuchar, interceptar o almacenar cualquier comunicación sin consentimiento previo. El proveedor debe garantizar que sólo aquellas personas autorizadas son las que acceden a los datos personales, protegiéndolos de cualquier alteración o pérdida. La Directiva también impone a los proveedores del servicio la obligación de prestar información suficiente a los usuarios e informar tanto al usuario afectado como a la autoridad nacional en el caso de violación de seguridad. Los proveedores pueden almacenar y tratar los datos de sus usuarios siempre que sean imprescindibles para la prestación del servicio. Dichos datos pueden ser utilizados para la promoción comercial del servicio sólo si el usuario ha dado el consentimiento previo para tal acción. En lo referente a la retención de datos, la Directiva permite conservar los datos de las comunicaciones sólo con la finalidad de proteger la seguridad nacional, de lo contrario, todo dato relativo al tráfico o localización del usuario debe borrarse o convertirse en anónimos una vez finalizada la comunicación. En el caso de que se

[29] Directiva 2002/58/CE: http://eur-lex.europa.eu/legal-content/es/ALL/?uri=CELEX:32002L0058
Síntesis legislativa de la protección de datos en el sector de las comunicaciones electrónicas:
http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_es.htm

quisieran conservar o tratar estos datos, el usuario debe ser informado y dar el consentimiento.

Esta Directiva también regula las comunicaciones electrónicas no solicitadas (comúnmente llamado spam), las cuales no deben enviarse sin el consentimiento previo del usuario, aunque también se han establecido excepciones. La Directiva también regula la publicación de datos personales en guías públicas, que sólo se puede hacer mediante autorización del usuario; y obliga a los Estados miembro a disponer de medidas de control mediante un régimen propio de sanciones. Las *cookies* también tienen cabida en esta Directiva, en la que también se exige el consentimiento previo para almacenar información a partir de ellas, pero será la Directiva 2009/136/CE la que se encargue propiamente de regularlas.

La Directiva 2002/58/CE fue modificada posteriormente por dos directivas: la Directiva 2006/24/CE, 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, conocida como Directiva de Retención de Datos; que fue abolida en abril de 2014 por el TJUE como se ha explicado en el capítulo anterior. Y la Directiva 2009/136/CE[30], conocida como la Directiva de las *cookies*, que rectifica a la Directiva 2002/58/CE actualizándola en el factor tecnológico, ya que esta directiva no sólo tiene en cuenta las cookies sino también los virus o programas espía, reforzando el derecho a la privacidad y a la protección de datos. Esta directiva, principalmente refuerza la obligación de los prestadores del servicio de informar al usuario antes de captar o tratar ningún dato o instalar cualquier tipo de programa que viole la intimidad del usuario.

[30] Directiva 2009/136/CE
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:es:PDF

Tabla nº7: Principales características de la Directiva 2002/58/CE

Directiva de la privacidad y las comunicaciones electrónicas (2002/58/CE)
Se aplica a
El tratamiento de datos de carácter personal en el marco de la prestación de servicios de comunicaciones electrónicas.
Seguridad del tratamiento. El proveedor del servicio está obligado a
-Garantizar el acceso a los datos únicamente a las personas autorizadas -Proteger los datos para evitar su pérdida o alteración accidental. En caso de violación, notificar al afectado. -Garantizar una política de seguridad para el tratamiento de los datos personales
Confidencialidad de las comunicaciones. Estados miembros deben
-Garantizar la confidencialidad de las comunicaciones realizadas a través de las redes públicas de comunicaciones electrónicas. -Prohibir el acceso y el almacenamiento a personas distintas de los usuarios sin el consentimiento de los afectados. -Garantizar la información al usuario en el caso de que su comunicación vaya a ser almacenada, así como el tratamiento posterior de sus datos.
Retención de datos
-Los datos relativos al tráfico y los datos de localización deben borrarse o volverse anónimos cuando dejen de ser necesarios para la comunicación o facturación, salvo en caso de que el abonado haya dado su consentimiento para cualquier otro uso. -En el caso de investigaciones policiales y de seguridad nacional, los Estados miembros pueden limitar el grado de protección de datos.
Comunicaciones comerciales no solicitadas (spamming)
Los usuarios han de dar su consentimiento previo antes de recibir este tipo de mensajes.
«Chivatos» (cookies)
-Los usuarios deben dar su consentimiento para que se almacene su información a través de las cookies. -Los usuarios deben ser informados de forma clara y precisa del objetivo de esa recopilación.
Guías públicas
-Los usuarios deben dar su consentimiento para que pueda aparecer su teléfono o dirección de contacto en las guías públicas
Controles. Los Estados miembros deben garantizar
-La determinación de un régimen de sanciones en caso de incumplimiento de la regulación establecida en la Directiva. -La capacidad de las autoridades nacionales para poder supervisar y controlar el cumplimiento de la regulación.

Fuente: Elaboración propia del autor a partir de la síntesis de la UE
http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_es.htm

3.3. ¿Qué referencias legislativas tiene la política de protección de datos?

Las referencias legislativas que tiene la política de protección de datos están recogidas en distintos documentos que se expondrán en orden descendente según su valor jurídico. Los del Consejo de Europa se han desarrollado en un subapartado aparte precisamente por su independencia de la Unión Europea.

Tabla nº8: Referencias legislativas de la política de protección de datos

	Referencias legislativas de la Unión Europea		**Referencias legislativas del Consejo de Europa**	
Tratados de la UE	Carta de los Derechos Fundamentales de la Unión Europea	Decisión Marco 2008/977/JAI	Convenio nº108	Convenio Europeo de Derechos Humanos (CEDH)
	Tratado de la Unión Europea (TUE)			
	Tratado de Funcionamiento de la Unión Europea (TFUE)			

Fuente: Elaboración propia

En primer lugar, están los tres Tratados de la Unión Europea que tienen relación directa con la protección de datos bien de forma específica o bien porque reconocen el derecho a la vida privada y familiar, del cual deriva la protección de datos. La Carta de los Derechos Fundamentales de la UE, firmada y proclamada en el año 2000, contiene dos artículos que hacen referencia a la protección de datos. El artículo 7, que reconoce el derecho al respeto de la vida privada y familiar, del domicilio y de las comunicaciones; y el artículo 8, que establece el derecho a la protección de datos personales, limitando el tratamiento a fines concretos y dependiendo del consentimiento de la persona afectada; también garantiza el derecho al acceso a los datos personales que conciernan a la persona y a su rectificación. Aparte de estos, el artículo 52, apela a los límites legítimos de los derechos de la propia Carta, que deberán estar establecidos por la ley y que deberán respetar el principio de proporcionalidad respecto a los derechos reconocidos.

En el Tratado de la Unión Europea (TUE), en su artículo 39, establece que es el Consejo quien fijará las normas sobre protección de datos de carácter personal de las personas físicas y el control y respeto de esa normativa corresponderá a una autoridad

independiente. En el Tratado de Funcionamiento de la Unión Europea (TFUE), en su artículo 16, reproduce el artículo 8 de la Carta, permitiendo así el desarrollo de la normativa relativa al derecho de la protección de datos y "reforzando de esta manera la necesidad de respetar el derecho fundamental a la protección de datos en la Unión Europea" (Gutiérrez Zarza, Michael Alexander y Sutton, 2012: 91). Este artículo otorga la potestad al Parlamento Europeo, al Consejo y a los Estados Miembros en su jurisdicción de legislar la protección de las personas físicas en relación al tratamiento de datos de carácter personal.

Como instrumento legislativo vigente en la UE, se encuentra la Decisión Marco 2008/977/JAI, que es relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal. Este instrumento complementa a la Directiva 95/46/CE, ya que esta no contempla la protección de datos en información policial ni judicial intercambiada entre Estados miembros u otras instituciones de la UE. Los principios que establece esta Decisión Marco son la legalidad, proporcionalidad, comprendida en la inmediatez y la gravedad de la amenaza, y finalidad del tratamiento, aunque en este caso la finalidad es entendida en este caso como la prevención, la investigación, la detección o el enjuiciamiento de otros delitos. Este instrumento legislativo también configura el principio de calidad de los datos, es decir, que aquellos que sean inexactos, incompletos o no actualizados deben ser rechazados. Se establecen los plazos de retención de datos, cuando prescriben los datos para dejar de ser usados para fines penales. Los derechos que reconoce la Decisión Marco 2008/977/JAI son el derecho a obtener información sobre los datos recopilados o tratados, el derecho de acceso, de rectificación, de supresión y de bloqueo, entre otros (Bayo Delgado, Gutiérrez Zarza y Michael Alexander, 2012).

3.3.1. Referencias legislativas del Consejo de Europa

El Consejo de Europa[31], dispone de dos instrumentos relativos a la protección de datos. El Convenio nº108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de sus datos de carácter personal, abierto a la firma de los Estados en 1981, entrado en vigor en 1985 y ratificado por más de 40

[31]El Consejo de Europa es una organización internacional independiente a la Unión Europea, formada por todas las naciones de la UE, a excepción de Bielorrusia. Su órgano más activo es el Tribunal Europeo de Derechos Humanos.
Web oficial del Consejo de Europa:
http://web.archive.org/web/20070427024811/http://www.coe.int/DEFAULTEN.ASP?

Estados. “Consciente de que la necesidad de proteger los datos personales no ha de limitarse a sólo al territorio europeo, el Convenio 108 omite deliberadamente el término «europeo» en su título, para motivar así la adhesión de países no europeos” (Gutiérrez Zarza, Michael Alexander y Sutton, 2012: 66). Este convenio garantiza la protección de los derechos fundamentales a las personas del territorio que lo ratifique, especificando el derecho a la vida privada con respecto al tratamiento automatizado de los datos de carácter personal. El Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (CEDH), que constituye el segundo instrumento por parte del Consejo de Europa, protege en su artículo 8, el derecho al respeto de la vida privada y familiar: «toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia». De este artículo derivan el resto de normas legales para el tratamiento y protección de datos personales.

3.4. ¿Quién la aplica y la controla?

La política de protección de datos europea es aplicada en cada uno de los 28 Estados miembros. Cada país debe trasponer a su legislación propia las políticas establecidas por la UE, encargándose de que se cumpla la regulación comunitaria. No obstante, éste no es el único método que utiliza la Unión Europea para asegurar el cumplimiento de su jurisprudencia. En el caso concreto de la protección de datos personales, la UE ha creado tres organismos responsables de esta misión: las Autoridades Nacionales de Protección de Datos[32], el Supervisor Europeo de Protección de Datos[33] y el Responsable de la Oficina de Protección de Datos de la Comisión Europea[34]. El primero se refiere a las entidades de cada país que se encargan de la protección de datos, como pueda ser en España la Agencia de Protección de Datos. El segundo organismo es independiente, se responsabiliza del tratamiento de los datos de la Unión Europea, es decir, su poder es como el de las autoridades nacionales, pero a nivel europeo. El tercero, Data protection Officer of the EU, hace referencia al conjunto de responsables de la protección de datos de cada institución u organismo de la UE que trabajan para el Supervisor Europeo de

[32] National Data Protection Authorities
http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[33] European Data Protection Supervisor (EDPS)
http://ec.europa.eu/justice/data-protection/bodies/supervisor/index_en.htm

[34] European Commission’s Data Protection Officer
http://ec.europa.eu/justice/data-protection/bodies/officer/index_en.htm

Protección de Datos; se encargan de asegurarse del cumplimiento del correcto tratamiento de los datos internos en las instituciones de la UE.

La figura del Supervisor Europeo de Protección de Datos[35] es una institución europea cuya finalidad es garantizar que los derechos fundamentales y las libertades, en concreto el derecho a la vida privada y la protección de datos, sean cumplidos por las instituciones y órganos de la Unión Europea, pero no el tratamiento de esos datos en los Estados miembros. Esta autoridad está regulada en el Reglamento (CE) 45/2001. Los objetivos del Supervisor Europeo de Protección de Datos son la supervisión, la consulta y la cooperación.

El Grupo de Trabajo Europeo de Protección de Datos del Artículo 29[36], constituye otra figura independiente que también participa en el control de la protección de datos. Es denominado así por contemplarse su creación en el artículo 29 de la Directiva 95/46/CE de protección de datos, constituye un órgano consultivo independiente que investiga y realiza dictámenes, recomendaciones y documentos de consulta relativos a la protección de datos y a la aplicación de la normativa existente en los distintos Estados miembro. Está compuesto por un representante de las autoridades supervisoras designado por cada Estado miembro (las Autoridades de Protección de Datos), un representante de las autoridades establecido por las instituciones y organismos europeos (el Supervisor Europeo de Protección de Datos) y un representante de la Comisión Europea. Los objetivos que persigue esta organización son a) proporcionar opiniones de expertos en cuestiones de protección de datos; b) promocionar la aplicación uniforme de los principios generales de la Directiva en todos los Estados miembros a través de la cooperación entre las autoridades supervisoras de la protección de datos; c) aconsejar a la Comisión en cualquier medida comunitaria que afecte a los derechos y libertades de las personas en relación con el tratamiento de datos personales y privacidad; d) y hacer recomendaciones al publico en general y en particular a las instituciones comunitarias en materia de protección de datos y privacidad en la Comunidad Europea.

[35] El actual Supervisor Europeo de Protección de Datos es Peter Hustinx, que ostenta el cargo desde 2004. https://secure.edps.europa.eu/EDPSWEB/edps/EDPS?lang=es

[36] Actualmente el Grupo de Trabajo del Artículo 29 está presidido por Isabelle Falque-Pierrotin. Como vicepresidentes están Gérard Lommel y Wojciech Rafał Wiewiórowski y como secretaria Marie-Hélène Boulanger (encargada de la unidad de protección de datos de la Dirección General de Justicia de la Comisión). En el siguiente enlace se puede consultar la lista de representantes de cada Estado miembro que forman parte de dicho grupo de trabajo.
http://ec.europa.eu/justice/data-protection/article-29/structure/members/index_en.htm

En el ámbito estatal español, la autoridad nacional en materia de protección de datos es la Agencia Española de Protección de Datos (AEPD)[37], cuya misión es controlar el cumplimiento de la legislación de protección de datos y su aplicación. En relación con los ciudadanos afectados, atiende sus peticiones y reclamaciones además de informarles de sus derechos reconocidos por ley. La AEPD también promueve campañas de difusión para concienciar a la ciudadanía. En relación con los responsables del tratamiento de los datos, tiene la función de emitir las autorizaciones necesarias para ello así como sancionar y ordenar el cese del tratamiento o cancelación de los datos a una organización. En lo que respecta a su potestad reguladora, la AEPD dicta instrucciones y recomendaciones. Dentro del ámbito nacional hay algunas comunidades autónomas que sí que disponen de su propia agencia de protección de datos, como es el caso de Cataluña[38] y el País Vasco[39].

3.5. Estado de la cuestión en junio de 2014 y perspectivas de futuro

La regulación vigente comunitaria se encuentra muy limitada y anticuada en relación con la evolución tecnológica y la práctica actual. Han pasado casi dos décadas desde que se formuló la Directiva 95/46/CE, que es la política principal de referencia de la protección de datos. En este periodo el crecimiento de los datos y las diversas aplicaciones de tratamientos han aumentado de forma exponencial. Con la digitalización y el volcado sistemático de información que se realiza constantemente en la red, ya sea de forma pública o en una "nube" personal, además de aquellos datos que generamos sólo con la utilización de la red, se ha convertido Internet en un gran espacio donde se alojan datos de todo tipo y formato que necesitan ser protegidos.

Si nos centramos en las redes sociales, para ejemplificar esta limitación regulatoria, podemos detectar diversas problemáticas. En primer lugar, está la recogida de datos personales de estas plataformas, que tanto el tipo de datos como la cantidad no terminan de ajustarse al mínimo que dice la normativa, ya que exigen una gran cantidad de datos sensibles tales como el género, la fecha de nacimiento o la localización para poder formar parte de la red, considerando estos datos como excesivos. En segundo lugar, está la cuestión del almacenamiento y eliminación de datos personales de los usuarios, concretamente con el tiempo que la red social conserva la información de los usuarios y

[37] Agencia Española de Protección de Datos: http://www.agpd.es/portalwebAGPD/index-ides-idphp.php
[38] Autoridad Catalana de Protección de Datos: http://www.apd.cat/es
[39] Agencia Vasca de Protección de Datos: http://www.avpd.euskadi.net/s04-5213/es/

la capacidad de éstos de poder eliminarlos definitivamente (en el caso de Facebook, lo que elimina el usuario lo elimina de su visión, no de la base de datos que esta empresa posee). En tercer lugar, se encuentra la visibilidad de los datos y la configuración por defecto de la privacidad, el usuario puede configurar el nivel de privacidad de sus contenidos, pero para eso debe saber configurarlo. Desde la UE se recomienda que estas plataformas vengan configuradas con defecto con un alto grado de privacidad para que después, si el usuario desea compartir con más personas lo que suba a la red, cambie la configuración atendiendo a sus consecuencias. Finamente, también destaca la falta de transparencia del tratamiento de datos con integración con terceros, es decir, las aplicaciones que se alojan en la plataforma pero que constituyen una empresa diferente, las cuales llegan a conseguir en algunas ocasiones el permiso del usuario para no sólo acceder a sus datos, sino también a los de sus contactos (Telefónica, 2012). Ligada a esta cuestión se encuentra también la ausencia de una distinción en los formularios de consentimiento, es decir, que es necesaria una comunicación más directa que asegure que cuando el usuario da permiso al tratamiento de sus datos está siendo consciente de lo que se va a hacer con ellos y de sus posibles consecuencias.

3.5.1. Necesidad de actualización legislativa

La regulación principal de protección de datos está datada de 1995 y son muchos los avances y consecuentes cambios de uso los que le han seguido, configurando así un nuevo escenario. La Directiva 95/46/CE ha sentado los principios básicos sobre la protección de datos y siguen siendo válidos hoy en día, pero es necesario el cambio para poder ajustar la legislación a la sociedad actual. En 1995 Internet no había llegado a todo el mundo y el uso no se había hecho ni común ni cotidiano; sin embargo, hoy en día, más de 250 millones de personas[40] usan Internet a diario en Europa. Además, el hecho de que cada Estado miembro haya traspuesto esta Directiva adoptando distintas formas (debido a la libertad que tiene cada país para trasponer una Directiva de la UE), ha generado grandes diferencias en la legislación dentro del territorio europeo.

Según un sondeo de opinión elaborado por la UE, el Eurobarómetro especial 359, publicado en junio de 2011, sobre las actitudes de los europeos ante la protección de datos y la identidad digital, el 40% de los ciudadanos de la Unión Europea utiliza Internet. El 60% de esta población usuaria de la red, compra y vende utilizando este

[40] Según la UE: http://ec.europa.eu/justice/data-protection/minisite/

medio y participa en redes sociales. En lo que respecta al tipo de información que facilitan en el espacio digital, el informe señala que casi el 90% de esta población revela información biográfica en redes sociales y comercio electrónico, un 50% también revela información social y un 10% también revela información sensible. Esto es debido principalmente, tal y como demuestra la estadística, a que mayoritariamente (74% de la población encuestada) se tiende a naturalizar la revelación de datos personales pensando que este hecho forma parte del funcionamiento de la Sociedad de la Información. De hecho, un 70% de usuarios han afirmado ser conocedores del tratamiento de sus datos por parte de las empresas, admitiendo tener sólo un control parcial de ellos. Aunque también hay usuarios que piensan que controlan completamente sus datos personales (26% usuarios de redes sociales y 18% compradores online). No obstante, los usuarios sí que demandan una mejora en la legislación, el 74% de los usuarios quieren el consentimiento específico antes de la captación y tratamiento de sus datos personales, un documento entendible y que precise qué se va a hacer con sus datos y qué implicaciones tiene aceptar su política de protección de datos. El 43% de los usuarios aseguran haber sido preguntados por más información personal que la necesaria, pero sólo uno de cada tres europeos era conocedor de la existencia de una autoridad pública nacional responsable de la protección de datos a la que podía acudir para reportar los abusos. En general, la mayoría de europeos (90%) quiere la misma regulación de protección de datos en toda la UE (Comisión Europea 2012a, 2012b).

Tabla nº9: Actitud de los europeos sobre la protección de datos

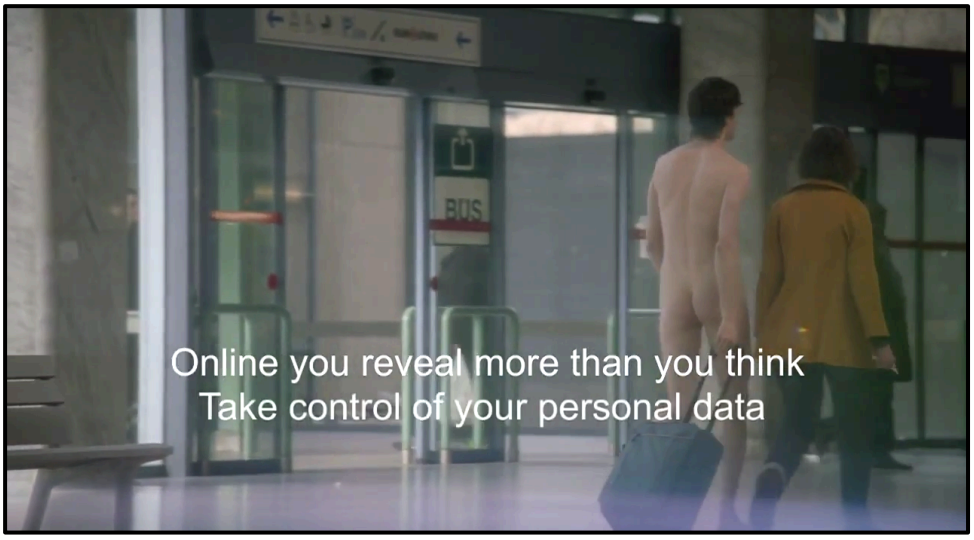
- **60%** de los internautas participan en Comercio-e y Redes Sociales
    - Revelan información **biográfica**: casi el **90%**
    - Revelan información **social**: casi el **50%**
    - Revelan información **sensible**: casi el 10%
- **74%** entiende la revelación de información personal como norma
- **70%** admite tener sólo un control parcial de sus datos
- Creen que **controlan completamente sus datos personales**
    - **26%** en Redes Sociales; **18%** en Comercio-e
- **74%** quiere el **consentimiento específico** antes de procesar sus datos
- **43%** ha sido preguntado por más información personal que la necesaria
- **1/3** conoce la autoridad pública nacional de protección de datos
- **90%** quiere la **misma regulación** de protección de datos en toda la UE

Fuente: Elaboración propia a partir de Comisión Europea (2012a y 2012b)

Tanto la Comisión Barroso II como el Supervisor Europeo de Protección de Datos coinciden en que es necesario un mayor fortalecimiento y concienciación del control del individuo sobre sus datos personales, además de realizar una campaña de sensibilización respecto a este tema para que los más jóvenes sean conscientes de los riesgos que corren en Internet.

Tras un periodo de casi tres años (de 2007 a 2010) de consultas públicas realizadas por la UE en el que participaron "autoridades públicas, asociaciones empresariales, organizaciones de consumidores y organizaciones no gubernamentales" (Heckh y Cárdenas, 2012: 18) con el objetivo de determinar la necesidad de realizar una reforma de la legislación vigente. Después de dicho periodo, el Consejo Europeo pidió a la Comisión Europea que evaluase el marco jurídico actual y presentase una propuesta de reforma. Finalmente, la Comisión Europea, el 25 de enero de 2012, propuso una actualización de la regulación de la protección de datos para enfrentarse a los retos de la Sociedad de la Información. Los objetivos principales que la Comisión ha tenido en cuenta para actualizar la legislación han sido reforzar los derechos individuales, mejorar el comercio interno, asegurar una mejora de protección de datos en todas las áreas, y establecer unos estándares de protección de datos de referencia global (Comisión Europea, 2012a). Esta reforma ya ha sido aprobada por el Parlamento, y debe ser aprobada por el Consejo para su entrada en vigor[41].

Imagen nº1:Fotograma del anuncio sobre la protección de datos de la Unión Europea

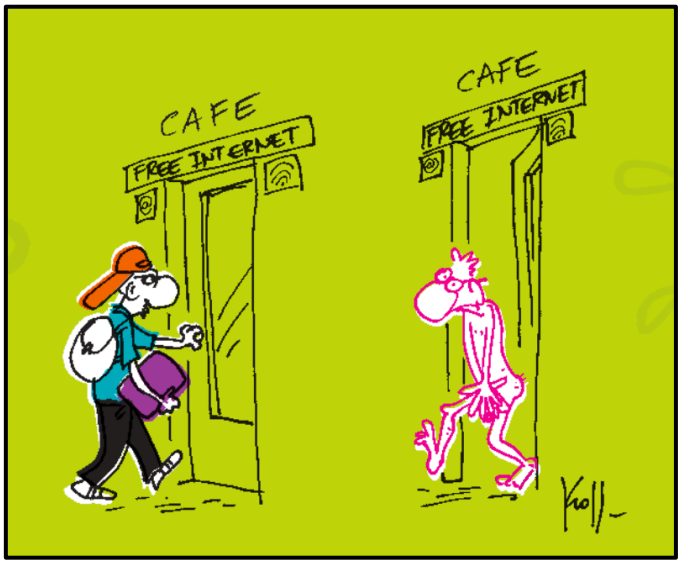


Fuente: Anuncio de la protección de datos de la Unión Europea

[41] http://europa.eu/rapid/press-release_MEMO-14-186_en.htm

Desde la Comisión Barroso II, concretamente desde el DG de Justicia, se está realizando una campaña de difusión y sensibilización sobre la protección de datos en distintos formatos. La Imagen nº1 es un frame que forma parte del vídeo anuncio que se está difundiendo a través de Internet para concienciar a los ciudadanos[42]. En esta imagen se muestra cómo representa la Unión Europea el actual estado de protección que tenemos en Internet. En el vídeo[43] podemos observar cómo los protagonistas, al utilizar Internet, se quedan desnudos, sirviendo esto de metáfora de la seguridad y la protección de datos en la esfera digital. Este anuncio sirve como "denuncia" o como "reclamo" para que los ciudadanos se conciencien sobre la importancia de la protección de datos y la seguridad en la red. El mismo tipo de simbolismo lo tenemos en la Imagen nº2, que es la portada del folleto divulgativo[44] que explica los factores relevantes de la propuesta que ha presentado la Comisión. En esta imagen se puede ver cómo a la salida de un cibercafé o de un lugar con red wifi gratis supone salir *desnudo* a la calle. Con esto, la Comisión quiere representar cómo la falta de protección actual puede provocar dejarnos expuestos en la red, cómo puede despojarnos de nuestros datos y de nuestra protección, identificada en este caso con la ropa.

Imagen nº2: Portada del folleto divulgativo de la Propuesta de la Comisión



Fuente: Comisión Europea (2012c)

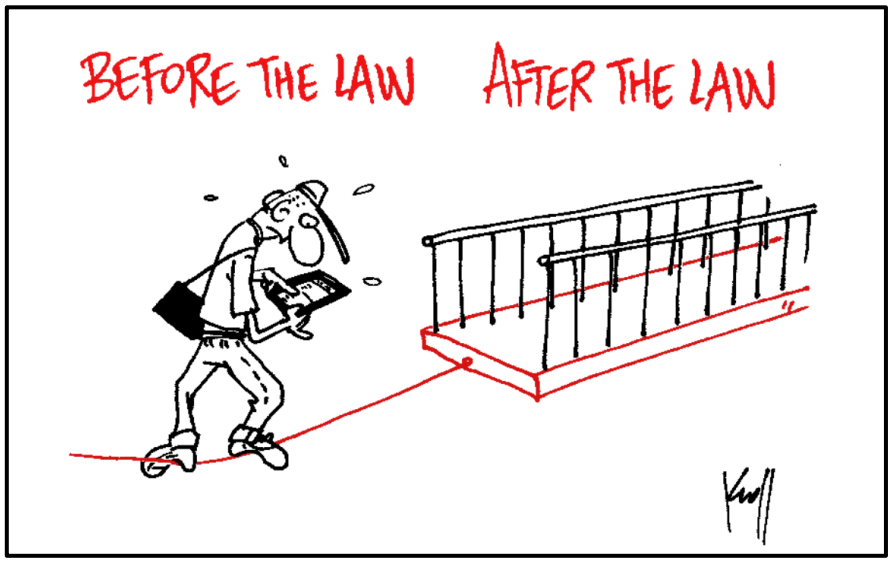
[42] La web de difusión del estado actual de la UE y la reforma de la regulación de la protección de datos es esta: http://ec.europa.eu/justice/data-protection/minisite/

[43] El enlace del vídeo es el siguiente: https://www.youtube.com/watch?v=5ByVaZ0rg8U&feature=plcp&context=C3ed3efbUDOEgsToPDskKv6OkHCqpA-QrcRZUHyZSQ

[44] En el siguiente enlace podéis consultar el folleto ilustrado que contiene los puntos más importantes de la propuesta de la Comisión. http://ec.europa.eu/justice/data-protection/document/review2012/brochure/dp_brochure_en.pdf

En la Imagen nº3 también encontramos otra ilustración que pertenece al mismo folleto divulgativo en la que muestra el estado actual de inseguridad que hay actualmente, y lo poco perceptible que es para los usuarios. Muestra la reforma como una medida necesaria que garantizará la seguridad para el ciudadano. La Unión Europea adopta esta serie de acciones divulgativas para transmitir a los ciudadanos la importancia que tiene para ellos la nueva reforma. Esta acción demuestra el interés existente de la Unión Europea por la protección y sensibilización del ciudadano.

Imagen nº3: Una representación gráfica del folleto divulgativo de la Propuesta de la Comisión



Fuente: Comisión Europea (2012c)

3.5.2. Propuesta de reforma legislativa de la Protección de datos de la Comisión Europea.

La propuesta de la Comisión Europea está compuesta por una nueva Directiva[45] y su correspondiente Reglamento[46]. La Directiva sustituiría a la actual Directiva 95/46/CE y a la Decisión Marco 2008/977/JAI, formulando una nueva política en lugar de realizar una modificación a la vigente como ha ocurrido en ocasiones anteriores. Esta Directiva fijaría las normas de protección de datos incluyendo esta vez en la política el ámbito judicial y policial. El Reglamento, que a diferencia de las directivas, por ser un acto

[45] Propuesta de Directiva de la Comisión Europea: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A52012PC0010

[46] Propuesta de Reglamento de la Comisión Europea: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52012PC0011

legislativo vinculante, debe ser aplicado directamente en cada Estado miembro sin darles margen de adecuación a su legislación nacional. Esto supone la unificación del marco jurídico en todos los países de la UE (Heckh y Cárdenas, 2012).

En lo que respecta al ámbito de aplicación del Reglamento, éste establece que no sólo se aplicará a los responsables y encargados del tratamiento de la UE, sino también de aquellas empresas extranjeras que ofrezcan servicio a Europa. La transferencia de datos a terceros países serán realizadas con mayor sencillez y flexibilidad, disminuyendo las cargas administrativas. Aunque los mecanismos utilizados deberán ser previamente aprobados por una Autoridad de Protección de Datos (APD). El nuevo Reglamento, en su artículo 2 especifica que no se aplicará al tratamiento de datos personales por parte de instituciones, órganos y organismos de la UE, por lo que en este aspecto seguiría vigente el Reglamento (CE) 45/2001. Asimismo también señala que no se aplicará el Reglamento al tratamiento de datos por parte de las autoridades con fines judiciales o policiales, en este caso quedarían regulados por la nueva Directiva que también propone la Comisión (Gutiérrez Zarza, Michael Alexander y Sutton, 2012).

Este nuevo Reglamento establece como principios la transparencia, refiriéndose a la información clara y correcta que se le debe proporcionar a la persona en lo referente a la captación y proceso de sus datos; la minimización de los datos, es decir, que la captación de los datos debe ser mínima y no debe abarcar más de lo que se necesita para la finalidad que se persigue, además el tratamiento de los datos no puede derivar del fin marcado con el que se recogieron; el consentimiento, que debe ser informado, otorgado libremente, específico y claro; la obligación de informar sobre infracciones en materia de seguridad; y el principio del tratamiento de datos sensibles, que sólo pueden procesarse en casos excepcionales (Gutiérrez Zarza, Michael Alexander y Sutton, 2012). El Reglamento reconoce el derecho de la portabilidad de datos, es decir, la capacidad de importar los datos personales de una aplicación a otra. Establece también mecanismos de recurso colectivo (arts. 73 y 76), con la finalidad de permitir a agruparse o asociarse a las personas que cuya protección de datos haya sido dañada y puedan presentar un recurso conjunto como colectivo afectado.

El Reglamento especifica e introduce cambios en el tratamiento de los datos de los menores de 13 años en servicios de Sociedad de la Información, en cuyo caso será obligatorio el consentimiento o autorización por parte de los padres o tutores legales

para proceder a cualquier tratamiento. Las obligaciones de los responsables y los encargados del tratamiento de datos que estipula el nuevo Reglamento, entre las cuales destaca la adopción de las políticas y medidas necesarias para garantizar y demostrar que el tratamiento de datos personales está cumpliendo las condiciones establecidas en el Reglamento. En el caso de empresas públicas o de compañías de más de 250 empleados, ésta habrá de designar un delegado de protección de datos que figure como responsable. Si hubiese una violación de datos personales, el responsable debe notificar en un plazo de 24h a la APD o aportar una justificación razonable a esta si se excede del plazo. Si no se han tomado medidas de seguridad ante tal violación el responsable deberá notificarlo también a los afectados. El Reglamento elimina la comunicación previa al tratamiento por parte del responsable a la APD.

Lo que destaca de esta nueva política son los seis cambios principales que introduce. En primer lugar, una regulación de protección de datos comunitaria aplicada por igual en todos los Estados miembros y a todos los servicios y compañías online independientemente del país del que procedan. En segundo lugar, el derecho al olvido. En tercer lugar, la mejora de acceso a los datos propios (derecho de portabilidad). En cuarto lugar, la capacidad de decisión sobre cómo serán usados los datos personales correspondientes. En quinto lugar, el derecho a saber cuándo la seguridad de la empresa que tiene tus datos ha sido violada. Y en sexto y último lugar, la privacidad por defecto.

Por ejemplo, la entrada en vigor de este nuevo reglamento supondría poder borrar de forma efectiva los datos de una red social. Actualmente es posible que una red social continúe almacenando datos de los cuales ya habías solicitado su eliminación, así como una gran cantidad de información que el usuario no es del todo consciente. El Nuevo Reglamento no sólo obliga a estas plataformas a minimizar el volumen de datos personales que obtienen de sus usuarios sino que también están obligadas a eliminar de forma permanente toda aquella información que el usuario solicite, a no ser que exista algún motivo legal para almacenarlos.

3.5.3. Derecho al Olvido

El reconocimiento del Derecho al olvido como parte del derecho de supresión (art.17) es una de las novedades que presenta el Reglamento. Este derecho incluye como obligación la eliminación sin retraso de la información y el aviso por parte del

responsable del tratamiento a las empresas terceras vinculadas a las que éste haya podido ceder los datos.

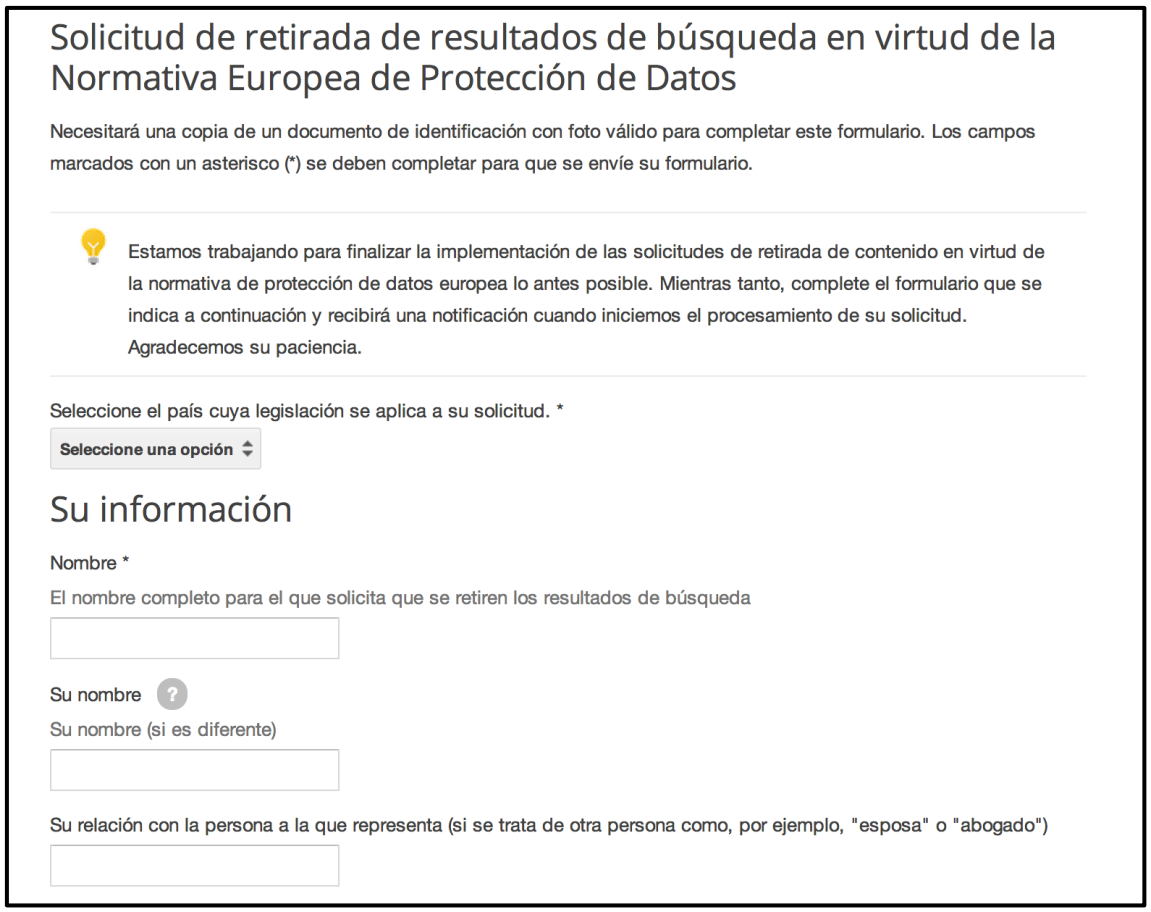
Se establecen cuatro posibles condiciones para que el interesado ejerza su derecho al olvido exigiendo la supresión de los datos personales: a) los datos proporcionados en su momento ya no son necesarios para los fines que fueron recogidos; b) el afectado retira el consentimiento que se otorgó en su momento o ha finalizado el plazo establecido en él; c) oposición al tratamiento; d) incumplimiento de los principios de la Directiva por parte del tratamiento. El responsable no deberá retrasar la supresión de dichos datos a no ser que éstos sean necesarios para la libertad de expresión, para el interés público en el ámbito de la salud pública, para una investigación histórica o para el cumplimiento de una obligación legal.

Asimismo, no se eliminará directamente, sino que se limitará el tratamiento de los datos personales cuando el afectado pida la eliminación por inexactitud de los datos, cuando el responsable ya no los necesite, cuando el tratamiento sea ilícito y el interesado se haya opuesto a él y cuando el afectado solicite la transmisión de sus datos.

Como se explicaba en el capítulo anterior, el TJUE dictó una sentencia el día 13 de mayo de 2014 en la que se reconocía por primera vez el derecho al olvido y estipulaba las primeras normas jurídicas al respecto. Constituyendo así la sentencia la vía rápida para la regulación de dicho derecho, ya que la propuesta de la Comisión aun está en proceso de ser aprobada por el Consejo para entrar en vigor.

Dos semanas más tarde de la publicación de esta sentencia, Google pone a disposición del ciudadano un formulario a partir del cual se puede solicitar la eliminación del vínculo existente entre la búsqueda y la página en la que está alojada la información que la persona afectada desea retirar. El motor de búsqueda asegura que cada caso será analizado teniendo en cuenta no sólo el derecho a la privacidad sino también el derecho a la información (*El País*, 2014c). Si la empresa no contestase o no hiciera caso del bloqueo o cese de dicha información, el usuario puede acudir entonces a la AEPD, quien le ayudará a comenzar la batalla legal para reclamar su derecho. No obstante, el hecho de que Google, una empresa privada, sea quien debe juzgar si una información es o no de interés público, si debe o no seguir en línea para la consulta pública, ejerciendo el derecho de información, es bastante inquietante.

Imagen nº4: Modelo de solicitud a Google de retirada de datos [47]



Solicitud de retirada de resultados de búsqueda en virtud de la Normativa Europea de Protección de Datos

Necesitará una copia de un documento de identificación con foto válido para completar este formulario. Los campos marcados con un asterisco (*) se deben completar para que se envíe su formulario.

Estamos trabajando para finalizar la implementación de las solicitudes de retirada de contenido en virtud de la normativa de protección de datos europea lo antes posible. Mientras tanto, complete el formulario que se indica a continuación y recibirá una notificación cuando iniciemos el procesamiento de su solicitud. Agradecemos su paciencia.

Seleccione el país cuya legislación se aplica a su solicitud. *

Seleccione una opción

Su información

Nombre *

El nombre completo para el que solicita que se retiren los resultados de búsqueda

Su nombre

Su nombre (si es diferente)

Su relación con la persona a la que representa (si se trata de otra persona como, por ejemplo, "esposa" o "abogado")

Fuente: Google, 2014

Precisamente para evitar estas dudas sobre la fiabilidad de su juicio, Google ha creado un comité asesor de expertos que colabore con la empresa para el análisis de estos casos. Este comité está compuesto por el expresidente de Google, Eric Schmidt, que liderará el equipo, Jimmy Wales, director de Wikipedia, además de otros académicos y representantes de organismos reguladores de protección de datos, como es el caso de José Luis Piñar, exdirector de la AEPD y catedrático de Derecho Administrativo de la Universidad San Pablo CEU (*El País*, 2014c).

[47] Parte del formulario de Google a disposición del usuario para hacer efectivo su derecho al olvido. Para completar el envío del formulario, hay que enviar el DNI o Pasaporte escaneado de la persona solicitante, esa es la única medida que solicita Google para poder hacer efectiva la solicitud. Aunque también permite que dicho documento nacional que identifique a la persona solicitante puede estar manipulado, es decir, que puede borrar información de dicha imagen siempre y cuando deje la información básica para su identificación. Google se responsabiliza también de eliminar esta copia enviada una vez haya sido tramitado su caso, a no ser que sea necesario conservarla por ley. Enlace del formulario: https://support.google.com/legal/contact/lr_eudpa?product=websearch

3.5.4. La confianza y la seguridad como un pilar de la Agenda Digital para Europa

Preservar la privacidad y la seguridad en la esfera digital es uno de los objetivos que podemos vislumbrar en el marco de actuación de la Unión Europea, dentro de la estrategia Europa 2020[48]. Ésta es la gran estrategia para el crecimiento y el empleo de la Comisión Europea, es decir, es el gran marco de lo que deben ser las políticas de la UE de aquí a 2020. Esta estrategia tiene cinco objetivos clave que deben estar cumplidos en la Unión Europea en 2020. Concretamente, en primer lugar está el empleo, cuya tasa debe llegar al 75% de las personas de 20 a 64 años de la UE. En segundo lugar está la Investigación y el Desarrollo (I+D), cuya inversión debe ser del 3% del PIB de la UE. En tercer lugar está el cambio climático y la sostenibilidad energética, cuyos propósitos son la reducción de un 20% o 30% de las emisiones de gases de efecto invernadero en relación a los niveles de 1990, un 20% de energías renovables y un aumento del 20% de la eficiencia energética. En cuarto lugar está la educación, que tiene por metas reducir la tasa de abandono escolar a una cifra inferior del 10% y que un 40% de las personas de entre 30 y 34 años de edad hayan completado los estudios superiores. En quinto y último lugar, está la lucha contra la pobreza y la exclusión social, cuyo fin es reducir al menos en 20 millones el número de personas en situación o riesgo de pobreza y exclusión social. Estos objetivos están pensados que se cumplan mediante medidas nacionales y europeas, además, están relacionados entre sí[49], lo que hace mucho más fácil alcanzarlos.

Para cumplir estos objetivos se han establecido unas metas nacionales[50]. En el caso de España, concretamente se han establecido como objetivos que en 2020 la tasa de empleo de las personas de entre 20 y 64 años sea del 74%, la inversión en I+D sea el 3% del PIB, la reducción de CO_2 sea de un -10%, debe haber un 20% de energías renovables, debe aumentar la eficiencia energética 25'20Mtep, el abandono escolar no puede superar el 15%, la enseñanza superior debe ser del 44% de la población y finalmente reducir entre 1.400.000 y 1.500.000 personas la situación de pobreza o exclusión social.

[48] http://ec.europa.eu/europe2020/index_es.htm
[49] Si mejora el nivel educativo mejora la empleabilidad y la reducción de la pobreza. Si aumenta la inversión en I+D mejorará la competitividad y crecerá el empleo. Finalmente, el fomento por la utilización de energías renovables no sólo mejorará el medio ambiente sino que creará nuevos puestos de trabajo y modelos de negocio.
[50] http://ec.europa.eu/europe2020/pdf/targets_es.pdf

La estrategia Europa 2020 incluye siete *iniciativas emblemáticas,* para cumplir los objetivos anteriormente señalados, que se dividen en tres áreas. En primer lugar, está el crecimiento inteligente, que se encarga de la educación, la investigación y la innovación y la sociedad digital. En segundo lugar está el área de crecimiento sostenible, que engloba las iniciativas que tienen por objetivo que la economía sea más verde, más competitiva y que utilice eficazmente los recursos. En tercer y último lugar, el crecimiento integrador, cuyas iniciativas persiguen conseguir una economía con un alto nivel de empleo que favorezca la cohesión económica, social y territorial.

Las iniciativas emblemáticas que utiliza la UE para impulsar el crecimiento inteligente son tres: la Agenda Digital para Europa, cuya misión es conseguir un mercado único digital que fomente el crecimiento inteligente, sostenible e integrador; la Unión por la Innovación, que tiene por objetivo mejorar las condiciones de financiación y acceso a la investigación; y la Juventud en Movimiento, cuya meta es que la educación y las oportunidades de movilidad experimentadas garanticen a los jóvenes el acceso a su primer empleo.

Atendiendo al objeto de estudio de esta investigación, nos centraremos en la iniciativa de la Agenda Digital para Europa[51], que entre las acciones que tiene planteadas destacamos la de *consolidar la confianza y la seguridad en línea*, cuya misión es luchar contra la ciberdelincuencia y la pornografía infantil en línea, además de combatir la falta de respeto de la intimidad y los datos personales. Para conseguir consolidar la confianza y la seguridad en línea se ha propuesto como objetivos dieciséis acciones[52]:

1- Reforzar la política de Seguridad en las Redes y la Información. Esta acción se llevará cabo mediante la actualización de la Agencia Europea de Seguridad de las Redes y la Información (EINSA) y las medidas que permiten reacciones rápidas en casos de ciberataques.

2- Combatir los ciberataques contra los sistemas de información. Este objetivo se consiguió en 2013 con la aprobación de la Directiva 2013/40/UE, ya que suponía la creación de reglas de jurisdicción del ciberespacio, a niveles europeo e internacional.

[51] http://europa.eu/legislation_summaries/information_society/strategies/si0016_es.htm
[52] http://ec.europa.eu/digital-agenda/en/our-goals/pillar-iii-trust-security

3- Establecer una plataforma europea de ciberdelincuencia. En enero de 2013, este objetivo se cumplió al entrar en funcionamiento el Centro Europeo de Ciberdelincuencia (EC3), que recoge la información sobre ciberataques y realice informes estadísticos regulares sobre la ciberdelincuencia.

4- Analizar la utilidad de crear un centro europeo de ciberdelincuencia. Esta acción se realizó en marzo de 2012, resultado de la cual fue continuar con la creación del Centro Europeo de Ciberdelincuencia. Consistía en estudiar las fuentes de financiación además de las ventajas e inconvenientes de su fundación.

5- Reforzar la lucha contra la ciberdelincuencia y los ciberataques a nivel internacional. Esta medida supone por una lado, crear un Foro Europeo para los Estados miembros para estimular la discusión sobre este tema entre las autoridades nacionales correspondientes. Por otro lado, se perseguirá una colaboración internacional con EEUU para mejorar la resistencia y la estabilidad de la red.

6- Preparación de ejercicios de apoyo en ciberseguridad en toda la UE. Esta acción esta planteada porque los europeos no utilizan aquellas herramientas en las que no confían, por eso la UE fomenta debates sobre ciberseguridad que evalúen el estado de la Red y los sistemas de Información en Europa.

7- Explorar la ampliación de notificaciones de violaciones de seguridad. Este objetivo se ha tenido en cuenta en la propuesta de la Comisión Barroso II presentada en 2012, que pretende actualizar el marco regulatorio de la protección de datos personales. Esta medida se ha tenido en cuenta en la propuesta de la Comisión presentada en 2012.

8- Guía para la aplicación de la normativa sobre la privacidad de telecomunicaciones. Esta medida, finalizada en 2011, implicaba dar orientaciones para la implementación del nuevo sistema de telecomunicaciones considerando la protección individualizada de privacidad y datos personales.

9- Realizar informes de contenidos ilegales online y campañas de sensibilización sobre la seguridad online para niños. Este objetivo consiste en difundir información sobre actividades destinadas a concienciar sobre la seguridad digital, realizadas por Centros de Seguridad de Internet de toda Europa. En mayo de 2012 la estrategia europea para una Internet mejor para los niños tenía por objetivo enseñar a los niños las habilidades y herramientas digitales que necesitan para garantizar su seguridad en la red.

10- Fomentar la autorregulación en el uso de los servicios online. Esta iniciativa pretende promover el diálogo y la autorregulación de los proveedores de servicios europeos, teniendo en cuenta el uso que hacen los niños de sus servicios.

11- Los Estados miembros establecerán equipos paneuropeos de respuesta a emergencias informáticas. Este objetivo implica fomentar la utilización de la red europea para resolver los ciberataques, cuyas reacciones suelen ser lentas. En 2013 se presentó una propuesta legislativa sobre la mejora de la seguridad de la red y la información en la UE.

12- Los Estados miembros llevarán a cabo simulaciones de ataque cibernético. Esta medida fue puesta en práctica dos veces, en 2010 y 2012. En 2014 la Agencia Europea de Seguridad de las Redes y la Información (EINSA) tiene previsto realizar otro simulacro.

13- Los Estados miembros implementarán alertas de contenido perjudicial. Esta acción consiste en aplicar líneas directas de emergencia para denunciar contenido ilegal, organizar campañas de sensibilización sobre seguridad online para niños, ofrecer enseñanza gratuita online y animar a los proveedores a implementar medidas de autorregulación atendiendo a la seguridad de los menores.

14- Los Estados miembros establecerán plataformas nacionales de alerta. Esta medida, que implicaba adaptar plataformas a la plataforma de ciberdelincuencia de la Europol, ha sido cumplida. Las plataformas se integraron en 2012 y en 2013, con el lanzamiento del EC3, se reforzó esta acción.

15- Proponer una Directiva de seguridad de la red y la información. Este objetivo fue cumplido en febrero de 2013, cuando se propuso la Directiva. La finalidad es resistir y mantener la estabilidad de las redes y la información es esencial para el buen funcionamiento de la UE, sobre todo para el comercio interior.

16- Estrategia de Ciberseguridad europea. Esta estrategia fue adoptada en 2013. Es necesaria una cooperación entre los Estados miembros, ya que afrontar esta situación de manera fragmentada hace mayor el desafío.

17- Expandir la Alianza Global contra el abuso sexual infantil online: Esta acción pretende cooperar con los investigadores entre los Estados miembros y contribuir a la alianza en contra del abuso sexual infantil online.

Finalmente, dentro de la Estrategia Europa 2020, el gran marco de todas las políticas de la UE, nos encontramos el Horizonte 2020 (H2020)[53], un Programa Marco de financiación de la Unión Europea que comprende los objetivos de investigación e innovación durante el periodo 2014-2020. Este programa de acción está dividido en tres pilares. El primero es la *Ciencia Excelente*, cuya financiación estará destinada al desarrollo científico de la UE. El segundo es el *Liderazgo Industrial*, cuyo objetivo es financiar el desarrollo de tecnologías y sus aplicaciones para mejorar la competitividad europea. El tercero está centrado en los *Retos Sociales*, que consiste en fomentar la investigación sobre aquellas cuestiones que afectan a los ciudadanos, tales como el cambio climático, la salud, la energía, el transporte, la seguridad informática, etc.

La financiación relacionada con la protección de datos personales estaría ubicada en el tercer pilar. Concretamente, está el área de *Sociedades seguras: Protección de la libertad y seguridad de Europa y sus ciudadanos*[54], cuyo desafío es realizar actividades de investigación e innovación que protejan a los ciudadanos, a la sociedad, a la economía y, en general, al bienestar. Los principales objetivos de este sector son mejorar la resistencia de la sociedad ante las catástrofes naturales y humanas (medidas para salir de la crisis, soluciones para infraestructuras, etc.); combatir el crimen y el terrorismo; mejorar la seguridad en la frontera (frontera marítima, políticas de seguridad exterior de la UE, fomentar la paz); y proporcionar una mejor ciberseguridad (intercambio seguro de información y nuevos modelos de aseguramiento). En este sentido, proyectos vinculados a la protección de datos pueden recibir financiación del H2020 si se ajustan a las características que proponen en el programa. Esto demuestra cómo las políticas se complementan con otras medidas para ampliar su cobertura y agilizar el proceso de actualización y protección frente a la cambiante esfera digital.

[53] http://www.eshorizonte2020.es/que-es-horizonte-2020
[54] http://ec.europa.eu/programmes/horizon2020/en/h2020-section/secure-societies-%E2%80%93-protecting-freedom-and-security-europe-and-its-citizens

CONCLUSIONES

El análisis sobre la privacidad en el escenario digital y el estudio de las políticas de la Unión Europea sobre la protección de datos de la ciudadanía nos permiten presentar un conjunto de conclusiones, que se detallan a continuación estructuradas en tres bloques temáticos.

El primer aspecto que hemos abordado es el concepto de espacio público en la esfera digital, que todavía se encuentra en una fase inicial de definición por su carácter cambiante y sobre el cual la academia todavía no tiene definiciones definitivas. Ante este escenario, este trabajo ha podido delimitar el término del siguiente modo: no hemos obtenido una definición que especifique qué es o qué conforma el espacio público en Internet. Por esta razón, este concepto ha sido definido por esta investigación el espacio digital público se constituye como el conjunto de páginas web o plataformas sociales que contienen información de libre acceso y que disponen de un foro de discusión o un espacio de participación que constituye un medio para la ciudadanía para debatir y comunicarse. Para enmarcarla, se ha tomado como punto de partida el concepto tradicional de espacio público, entendido como espacio de debate de temas de interés público, para trasponerlo a la esfera digital.

Los rasgos más característicos del espacio público digital son, en primer lugar, una mayor facilidad de acceso a este espacio y permite, en segundo lugar, una mayor pluralidad. Como consecuencia, la esfera pública digital consigue ofrecer un lugar con una oferta más equitativa y abierta.

Esto no quiere decir que el espacio público digital sea perfecto, en él se observan algunos inconvenientes o dificultades.. No sólo se produce lo que se conoce como la brecha digital, que señala la desigualdad ante el acceso a la red, esto es, que no todo el mundo tiene la mismas posibilidades de que el contenido que publique en la red llegue a toda la audiencia potencial de Internet. Así pues, otra de las características identificadas es que el espacio público digital no es neutro, se remarca su personalización y la consecuente individualización que crea, por tanto se demuestra que la apreciación de objetividad de la búsqueda en la red es falsa.

Acorde a este modo de funcionamiento de la red, existe una adaptación del espacio público al usuario, creada como consecuencia de la interacción de éste con la red. En

función de la personalización presente en la red, se han establecido dos tipos de espacios. En primer lugar está el espacio personalizado de forma involuntaria, que supone una perspectiva prefabricada, construida a partir de la información que se ha extraído de los hábitos de uso del usuario. Y, en segundo lugar, el espacio personalizado de forma voluntaria, que atiende a una personalización activa, escogida directamente por el usuario, como pueda ser la subscripción a un tipo de noticias en concreto que respondan a las características que el usuario desea consumir.

Los peligros que se encuentran en este espacio virtual vinculados a la privacidad son causa de la estructura y funcionamiento de la red, que posibilita la opción de registrar los movimientos virtuales de un usuario, permitiendo así establecer un estado de vigilancia. La huella digital, tanto su versión activa como la pasiva, generan muchos datos sobre los usuarios, convirtiéndoles en personas identificables y controlables. A partir del avance en las tecnologías de extracción de datos en la red, aumenta la dificultad para salvaguardar la privacidad en la esfera digital. Esto demuestra la necesidad que tienen los ciudadanos de conocer el funcionamiento de la red para ser conscientes de cómo gestionar su privacidad y a qué se exponen cada vez que navegan por la red.

Atendiendo a uno de los objetivos del trabajo, se ha presentado el estado de la intimidad y la privacidad en Internet para entender qué ocurre con los límites entre el espacio público y el espacio privado. Entorno a ello se ha llegado a la conclusión de que existe una convergencia del espacio público y el espacio privado en la esfera digital. Para justificar este hecho, se ha de tener en cuenta primero tres condicionantes de la red. El primero es que el uso de la esfera digital es multidisciplinar y heterogéneo, se entiende como un espacio donde todo tiene cabida. El segundo es la falta de unas reglas comunes para todos los usuarios, más allá del sentido común que diga qué se debe publicar y qué no, que diga el dónde y el cómo. El tercero es la configuración de la identidad digital, públicamente consultable, que condiciona también las publicaciones de las personas. Esta situación conlleva la convergencia del espacio público digital y el espacio privado digital.

Para entender los límites entre espacio público y privado, hemos tenido que recurrir al estudio del concepto de intimidad y privacidad en la red. La intimidad, por definición, en la red no existe. Por el contrario lo que equivale a la intimidad en la red es la

privacidad. Es decir, la adaptación de este concepto a la esfera digital se convierte en privacidad por tratarse de una información íntima introducida en la red dentro de en un espacio controlado. Con la filosofía de Internet, la cultura de compartir y la comunicación en digital sacrifica la intimidad y la privacidad para ser noticia. El miedo a ser excluido, a ser olvidado, es más fuerte que el sentimiento de privacidad. La necesidad de nutrir y crear un perfil en una red social fomenta la publicación de información personal, incluso íntima. La extimidad define la tendencia de publicar abiertamente las intimidades en Internet, la conversión de lo íntimo en éxtimo. Este tipo de conducta pertenece de forma mayoritaria a las redes sociales, en las que la cantidad de información personal a compartir parece no tener límite.

La digitalización y la actividad en la red ha supuesto la creación de un nuevo paradigma para el derecho. No obstante, esta nueva esfera de actuación es controlable por la legislación previa a la era de Internet. Es decir, la legislación referente a los derechos que protegen la esfera privada del ciudadano se ha adaptado a la red ampliando la cobertura de la legislación ya existente que protegía los derechos de la personalidad (imagen, intimidad, honor y autodeterminación informativa) y el derecho de protección de datos. No se ha creado una ley específica que regule la esfera digital. Al tratarse de un mismo concepto en distintos espacios lo que se ha hecho es ampliar su protección.

La adaptación de los derechos existentes ha sido sencilla en el sentido de que se ha traspuesto la concepción que se tenía como agravio a la personalidad a la esfera digital. No obstante, en este nuevo paradigma los ataques contra la privacidad personal, la imagen y el honor se han multiplicado y tomado distintas formas. El derecho intenta solventar estos problemas con la legislación actual pero es cierto que aun queda mucho recorrido para cubrir todas las necesidades. Se están empezando a desarrollar derechos que cubren aspectos que estaban desprotegidos debido a su origen digital. Ejemplo de ello es el caso del derecho al olvido, entrado en vigor hace un mes, en mayo de 2014.

Como demuestra el caso de Mario Costeja, este derecho se llevaba reclamando por vía judicial desde hace casi cinco años. El derecho a ser olvidado, que nace como consecuencia de la estructura y el uso de la red, surge por el problema que supone el descontrol de la información en la red que alude directamente a una persona. El Tribunal de Justicia Europeo ha decidido que los ciudadanos deben ser capaces de decidir qué es lo que hay de ellos en Internet siempre y cuando esto no suponga ir en

contra de la ley. Hasta hace un mes, el ciudadano estaba desprotegido frente a esto. La entrada en vigor de este derecho significa una mayor cobertura jurídica para todos los ciudadanos y una mayor protección en la red.

Google ya ha incorporado las medidas necesarias para que cada ciudadano pueda ejercer su derecho al olvido. Sin embargo, la ausencia de una regulación más específica o una unidad de control que vigile la efectividad de este derecho hace que pueda suscitar dudas de sus efectos. Esto es debido a que este derecho podría tener como consecuencia la censura de noticias, información o comentarios que manchasen la imagen de una persona o una empresa, gracias a la eliminación de este tipo de información, cualquier persona que buscase información referente a estas demandantes de olvido tan solo encontraría un currículo intachable. La legislación avanza lento, y, como es lógico, se crea a posteriori de detectar una necesidad. La complejidad y la magnitud de la red también hacen inabarcables para el derecho muchos de sus aspectos. La legislación española no podía como tal no podía establecer el derecho al olvido, y si podía, le habría costado mucho. Gracias al TJUE, toda la Unión Europea reclama a Google la posibilidad del ciudadano de ejercer este derecho.

Tras el análisis del caso europeo, se puede afirmar que la política de protección de datos de la Unión Europea tiene como eje central al ciudadano. Mientras que otros países como EEUU apuestan por una regulación mucho más laxa en lo que respecta a la protección de la esfera privada del ciudadano, la UE antepone la privacidad y protección de datos personales, blindándolos como un derecho fundamental.

La propia Comisión Europea (Barroso II) ha admitido que para mantener el nivel de protección es necesaria una renovación de la legislación actual para poder cubrir todas las garantías y derechos de los ciudadanos. Después de varios años de revisión de la legislación actual y de realización de estudios sobre el sentimiento de seguridad en Internet de los europeos, la Comisión Barroso II lanzó una propuesta legislativa que sustituiría a la actual Directiva 95/46/CE. En ella se modifica la política de protección de datos adaptándola a la actual esfera digital y añadiendo como elemento innovador el derecho al olvido. En estos momentos, esta propuesta está en fase de discusión en el Parlamento Europeo.

A pesar de las distintas modificaciones que se han creado para la Directiva de 1995, la Unión Europea no ha conseguido adaptar su política de protección de datos a las nuevas

demandas que se desprenden del uso masivo y cotidiano que se realiza del entorno digital. El funcionamiento interno de las instituciones europeas pone de relieve el ritmo lento en la toma de decisiones que hace que tras casi tres años de duración, aun no ha sido aprobado por el Consejo. Este tipo de medidas provocan que el TJUE tenga que entrar en acción y regular el derecho al olvido, estando ya descrito en la propuesta de la Comisión de 2012.

Dicha propuesta resolvería la disparidad con la que está traspuesta en los Estados miembros de la Unión Europea la Directiva 95/46/CE. Esto es debido a que no sólo proponen una Directiva sino que también desarrollan su correspondiente Reglamento, que supondría la unificación de la legislación de protección de datos en toda la UE. La Comisión Barroso II ha sabido detectar y solventar los problemas que había en la política de protección de datos. No obstante, no ha visto cumplidos sus objetivos finales dado a que el proceso de aprobación de dicha propuesta sigue abierto.

El marco de actuación de la UE se complementa en el ámbito de la protección de la privacidad con la estrategia Europa 2020, que tiene una de las preocupaciones en la seguridad digital y por consiguiente la protección de datos. La 'Agenda Digital para Europa' constituye una de sus iniciativas adoptadas para consolidar la confianza y la seguridad en Internet. Esto demuestra la preocupación de la UE por mejorar sus sistemas de protección y de seguridad en Internet. Una de sus prioridades para la lucha contra la ciberdelincuencia ha sido crear el Centro Europeo de Ciberdelincuencia (EC3), institución que investigue y recopile información sobre los ciberdelitos europeos.

El análisis que ha realizado este trabajo ha dejado sin poder tratar algunos aspectos relativos a la protección de la privacidad que podía ser objetos de futuras investigaciones con este tema. En esta línea, se podría profundizar en dos aspectos clave que afectan directamente a la privacidad en la esfera digital. En primer lugar, indagar en la concepción de la privacidad que tienen los usuarios para entender los usos que se dan de ella en la actualidad. En segundo lugar, observar las políticas de privacidad que aplican los distintos sitios web para establecer categorías que los diferencie y ver cuál es la relación entre el grado de privacidad que aplica la página web y la cantidad de usuarios que tiene.

Asimismo este trabajo podría ampliarse con una comparación directa con la política de protección de datos de EEUU, teniendo en cuenta no sólo los aspectos legislativos sino

también los culturales. Además, el seguimiento de la evolución del derecho al olvido puede ser muy interesante, debido a su novedad existen aspectos sin conocer, como por ejemplo qué tipo de personas lo pueden pedir o qué tipo de contenidos desean retirar, si son cosas que publicaron en su adolescencia o son documentos publicados por un tercero, etc. Por último, también sería interesante realizar un seguimiento de la propuesta de la Comisión de Barroso II para ver su implementación en los Estados miembros de la UE.

BIBLIOGRAFÍA

ABRIL, P. S. Y PIZARRO, E. (2014) La intimidad europea frente a la privacidad americana. *InDret. Revista para el Análisis del Derecho*, 1 [Recuperado el 14/03/14 de http://www.indret.com/pdf/1031.pdf]

ACEDO, A (2012). El derecho al olvido en internet como componente esencial del derecho al honor en el siglo XX. En Savaris, J. A. Y Strapazzon, C. L. (coords.). *Direitos fundamentais da pessoa humana: um diálogo latino-americano* (191-219). Curitiba, Brasil: Alteridade Editora

ALMEIDA, J. (2002). Convergencia tecnológica, espacio público y democracia [En línea]. En *Coloquio Internacional Globalismo y Pluralismo*. Grupo de Investigación Interdisciplinaria sobre la Comunicación, la Información y la Sociedad. Quebec: Universidad de Quebec [Disponible en: http://www.er.uqam.ca/nobel/gricis/actes/bogues/Almeida.pdf]

ALONSO, C. (2013, 25 se Septiembre). De paseo por la Deep Web. [Entrada de blog]. Consultado el 9 de Junio de 2014. Recuperado de: http://www.elladodelmal.com/2013/09/de-paseo-por-la-deep-web.html

ALUJA, T. (2001). La minería de datos, entre la estadística y la inteligencia artificial. *Qüesttió*, 25, 3, 479-498

ARAMBURU, M. (2008). Usos y Significados del Espacio Público. *Arquitectura, Ciudad y Entorno*, 3(8), 143-150.

BAUMAN, Z. Y LYON, D. (2013) *Vigilancia líquida*. Buenos Aires: Paidós

BAYO DELGADO, J., GUTIÉRREZ ZARZA, Á. Y MICHAEL ALEXANDER, P (2012). Intercambio de información, protección de datos y cooperación judicial penal. En GUTIÉRREZ ZARZA, Á. (Coord). *Nuevas tecnologías, protección de datos personales y proceso penal : manual para jueces y fiscales europeos. Especial referencia al ordenamiento jurídico español* (192-295). Madrid :: La Ley

BERGMAN, M. K. (2001) White Paper: The Deep Web: Surfacing Hidden Value. *Journal of Electronic Publishing,* 7,1. [en línea] Disponible en: http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104

BOZDAG, E. (2013). Bias in algorithmic filtering and personalization. *Ethics and information technology*, 15(3), 209-227.

BROCOS FERNANDEZ, J. M. Y SALINAS PARDO, C. (2006) Selección de recursos de información disponibles en el Web invisible. *ACIMED*, 14, 3. [en línea] Disponible en: http://scielo.sld.cu/pdf/aci/v14n3/aci09306.pdf [Consultado el 7 de Junio de 2014]

BRU CUADRADA, E. (2007). La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad. *Revista de Internet, Derecho y Política*, 5, 78-92.

CALIFANO, B. (2012). Comunicación, Estado y políticas públicas: apuntes para la investigación. *Questión*, 1, 35, 38-52.

CARRILLO, M. (2007). Internet: la respuesta del derecho al espacio público virtual. *Quaderns del CAC*, 29, 63-70

CASACUBERTA, D. (2008). Reclaim the backbone: Repensar Internet como espacio público. *Arte y arquitectura digital, net-art y universos virtuales,* 41-48. Barcelona: Universitat de Barcelona / Grupo de investigación "Arte, Arquitectura y Sociedad digital". [Recuperado el 23 de enero de 2014, de: http://www.artyarqdigital.com/fileadmin/user_upload/PDF/Publicaciones_Jornada_III/D_Casacuberta.pdf]

CASTELLS, M. (2012). *Redes de indignación y esperanza: los movimientos sociales en la era Internet.* Madrid: Alianza.

CASTELLS, M. (2013). El impacto de internet en la sociedad: una perspectiva global. En OPENMIND BBVA (ed.) *C@mbio: 19 ensayos clave acerca de cómo Internet está cambiando nuestras vidas*. [en línea] Disponible en: https://www.bbvaopenmind.com/wp-content/uploads/2014/04/BBVA-OpenMind-libro-Cambio-19-ensayos-fundamentales-sobre-c%C3%B3mo-internet-est%C3%A1-cambiando-nuestras-vidas-Tecnolog%C3%ADa-Interent-Innovaci%C3%B3n.pdf

COMISIÓN EUROPEA (2012a) Factsheet: *Why do we need an EU data protection reform?* Disponible en: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

COMISIÓN EUROPEA (2012b) Factsheet: *How will the EU's reform adapt data protection rules to new technological developments?* Disponible en: http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/8_en.pdf

COMISIÓN EUROPEA (2012c) *Take control of your personal data*. Disponible en: http://ec.europa.eu/justice/data-protection/document/review2012/brochure/dp_brochure_en.pdf

CORBETTA, P. (2007). *Metodología y técnicas de investigación social*. Madrid: McGraw Hill Interamericana de España.

CRUSAFON, C. (2012). *La nueva era mediática: las claves del escenario global*, Barcelona: Bosch Comunicación

CULLELL - MARCH, C. (2010). *La política del espectro radioeléctrico en la Unión Europea: la armonización del Dividendo Digital en el Reino Unido y España*. Tesis doctoral. Barcelona: Universidad Internacional de Catalunya. Recuperado el 21 de junio de 2014, de http://www.tdx.cat/handle/10803/9352

DAVOLI, A. (2014) *Fichas técnicas sobre la Unión Europea: La protección de los datos personales*. [En línea] Disponible en: http://www.europarl.europa.eu/ftu/pdf/es/FTU_5.12.8.pdf

DIARIO JURÍDICO (2014, 11 de Abril). Anulación de la Directiva de Retención de Datos: consecuencias prácticas. *Diario Jurídico.com*. Recuperado el 20 de Mayo de 2014, de: http://www.diariojuridico.com/anulacion-de-la-directiva-de-retencion-de-datos-consecuencias-practicas/

DIPAOLA, E. (2008). La aparición del "yo total" y el desplazamiento de la intimidad: consideraciones acerca de los usos de la intimidad en los blogs y fotologs. *Argumentos. Revista de crítica social*, (9). [Disponible en: http://revistasiigg.sociales.uba.ar/index.php/argumentos/article/view/77/72]

EL PAÍS (2013, 27 de Diciembre). Snowden, el delator que removió los cimientos de la Inteligencia de EE UU. Recuperado el 10 de junio de 2014, de http://internacional.elpais.com/internacional/2013/12/27/actualidad/1388161985_409246.html

EL PAÍS (2014a, 4 de Enero). El fin del fin de la privacidad. Recuperado el 10 de junio de 2014, de http://ccaa.elpais.com/ccaa/2014/01/03/catalunya/1388777473_016642.html

El País (2014b, 13 de Mayo). La UE obliga a Google a retirar enlaces con información lesiva. Recuperado el 21 de mayo de 2014, de http://sociedad.elpais.com/sociedad/2014/05/12/actualidad/1399921965_465484.html

El País (2014c, 30 de Mayo). Google comienza los trámites para respetar el 'derecho al olvido'. Recuperado el 31 de mayo de 2014, de http://tecnologia.elpais.com/tecnologia/2014/05/30/actualidad/1401435080_160337.html

El País (2014d, 7 de Junio) Lo que Google no ve. Recuperado el 7 de junio de 2014 de http://sociedad.elpais.com/sociedad/2014/06/06/actualidad/1402082139_266819.html

Fernández, D. G. (2010). El derecho a la intimidad y el fenómeno de la extimidad. *Dereito: Revista xuridica da Universidade de Santiago de Compostela*, *19*(2), 269-284.

Fornas Carrasco, R. (2003) La cara oculta de Internet [en línea]. *Hipertext.net*, 1. [Consultado el 7 de Junio 2014]. Disponible en: http://www.upf.edu/hipertextnet/numero-1/internet.html

Franganillo, J. (2009). Implicaciones éticas de la minería de datos. *Anuario ThinkEPI*, 4, 320-324.

García Ull, F. J. (2013). Las cookies en los principales cibermedios generalistas de España. *Miguel Hernández Communication Journal*, 4, 233-261. Disponible en: http://mhcj.es/index.php?journal=mhcj&page=article&op=view&path[]=52

González Fuster, G. (2012). Elquilibrio entre propiedad intelectual y protección de datos: el peso oscilante de un nuevo derecho. *Revista de Internet, Derecho y Política*, 14, 47-60.

Gozálvez Pérez, V. (2011). Educación cívica en la cultura digital. Una aproximación crítica a la socialización-en-red. *Revista Iberoamericana de Educación*, *55*(2), 10.

Gutiérrez Zarza, Á., Michael Alexander, P. y Sutton, G. (2012). Conceptos básicos. Marco legal europeo sobre protección de datos en material penal. En Gutiérrez Zarza, Á. (Coord). *Nuevas tecnologías, protección de datos personales*

y proceso penal : manual para jueces y fiscales europeos. Especial referencia al ordenamiento jurídico español (51-130). Madrid :: La Ley

HAN, B. (2013) *La sociedad de la transparencia*. Barcelona: Herder

HECKH, N. Y CÁRDENAS ARTOLA, I. (2012). *Protección de datos*. Madrid: Francis Lefebvre.

HERNÁNDEZ SAMPIERI, R.; FERNÁNDEZ COLLADO, C. Y BAPTISTA, P. (2010), *Metodología de la Investigación.* México: McGraw-Hill. (Quinta edición)

HERRÁN ORTIZ, A. I. (2010) Las redes sociales digitales: ¿hacia una nueva configuración de los derechos fundamentales en Internet?. *Revista Vasca de Administración Pública. Herri-Arduralaritzako Euskal Aldizkaria,* 87, 521-566.

INTERNET.ORG (2013). A Focus on Efficiency: A whitepaper from Facebook, Ericsson and Qualcomm. Disponible en: https://fbcdn-dragon-a.akamaihd.net/hphotos-ak-ash3/851560_196423357203561_929747697_n.pdf

JARVIS, J. (2012). *Partes públicas*. *Por qué compartir en la era digital mejora nuestra manera de trabajar y vivir*. Barcelona: Gestión 2000

JUST, N., & PUPPIS, M. (Eds.). (2012). *Trends in Communication Policy Research: New Theories, Methods and Subjects*. Bristol: Intellect Books.

KAUFFER, E. (2002). Las políticas públicas: algunos apuntes generales. *Ecofronteras*, 16, 2-5.

LA VANGUARDIA (2014, 13 de Mayo). La Justicia europea reconoce el derecho al olvido defendido por España ante Google. Recuperado el 22 de mayo de 2014, de http://www.lavanguardia.com/tecnologia/internet/20140513/54406876512/ue-respalda-derecho-olvido-espana-ante-google.html

LLÁCER MATACÁS, M. R. (2011). *Protección de datos personales en la sociedad de la información y la vigilancia*. Las Rozas (Madrid): La Ley.

LLORCA ABAD, G. (2005). Comunicación interpersonal y comunicación de masas en Internet. Emisor y receptor en el entorno virtual. En LÓPEZ GARCÍA, G. (Ed.), *El ecosistema digital: Modelos de comunicación, nuevos medios y público en Internet* (21- 30). Valencia: Servei de Publicacions de la Universitat de València.

LÓPEZ GARCÍA, G. (2005). *Modelos de comunicación en Internet*. Valencia: Tirant lo Blanch

LÓPEZ GARCÍA, G. (2006). Comunicación en red y mutaciones de la esfera pública. *Zer: Revista de estudios de comunicación*, (20), 231-249.

MADDEN, M. ET AL. (2007). *Digital Footprints: Online identity management and search in the age of transparency*. Washington, DC: Pew Internet & American Life Project. [Disponible en: http://www.pewinternet.org/files/old-media/Files/Reports/2007/PIP_Digital_Footprints.pdf.pdf]

MAJÓ, J. (2012). Evolución de las tecnologías de la comunicación. En Moragas, M. (Ed.), *La comunicación: de los orígenes a Internet* (65-90). Barcelona: Gedisa.

MATTELART, A. (1993). *La comunicación-mundo: historia de las ideas y de las estrategias*. Madrid: Fundesco

MCLUHAN, M. Y B. R. POWERS (1995). *La aldea global: transformaciones en la vida y los medios de comunicación mundiales en el siglo XXI*. Barcelona: Gedisa

MOLINA FÉLIX, L. C. (2002). Data Mining: Torturando los datos hasta que confiesen. *Fundación Oberta de Cataluña (FUOC)*. Recuperado el 20 de enero de 2014, de http://www.uoc.edu/web/esp/art/uoc/molina1102/molina1102.pdf

MORAL, F. (2001). Aspectos psicosociales de la comunicación y de las relaciones personales en Internet. *Anuario de psicología*, *32*(2), 13-30. Disponible en: http://www.eqdpsicologos.com/componentes/documento/616651PB.pdf

MOROZOV, E. (2012). *El desengaño de internet*. *Los mitos de la libertad en la red.* Barcelona: Ediciones Destino.

MURILLO DE LA CUEVA, P. L. (2007). Perspectivas del derecho a la autodeterminación informativa. *Revista de Internet, Derecho y Política*, 5, 18-32.

NEGROPONTE, N. (1995). *Being digital*. London : Hodder and Stoughton

PALACIOS GONZÁLEZ, M. D. (2012). El poder de autodeterminación de los datos personales en internet. *Revista de Internet, Derecho y Política*, 14, 61-74.

PAUWELS, C., KALIMO, H., DONDERS, K., VAN ROMPUY, B. (eds). (2009). *Rethinking European Media and Communications Policy*. Bruselas: Brussels University Press.

REAL ACADEMIA ESPAÑOLA. (2001). Intimidad. En *Diccionario de la lengua española* (22.ª ed.). Recuperado de http://lema.rae.es/drae/?val=intimidad el 15 de marzo de 2014

RENDUELES, C. (2013). *Sociofobia. El cambio político en la era de la utopía digital*. Madrid: Capitán Swing

RHEINGOLD, H. (2004). Multitudes inteligentes. La próxima revolución social. Barcelona: Gedisa.

RIQUELME, J. C., RUIZ, R., Y GILBERT, K. (2006). Minería de datos: Conceptos y tendencias. Revista Iberoamericana de Inteligencia Artificial, 10(29), 11-18.

ROSSI CARLEO, L. (2011). La sociedad de la información: el ciudadano frente al poder de decisión ajeno. En Llácer Matacás, M. R. (Coord.) *Protección de datos personales en la sociedad de la información y la vigilancia* (23-39). Las Rozas (Madrid): La Ley

SABATER PICAÑOL, J. (2013). *Big Data*. Proyecto final de carrera. Universitat Politècnica de Catalunya. [Disponible en: http://upcommons.upc.edu/pfc/handle/2099.1/20144]

SALGADO SEGUIN, V. (2010). Nuestros derechos, en riesgo. Intimidad, privacidad y honor en Internet. *Telos: Revista de pensamiento sobre tecnología y sociedad,* 85, 69-79

SALVAT, G. Y SERRANO, V. (2011). Periodismo ciudadano y espacio público en la Sociedad de la Información. *Anàlisi*, 41, 69-85.

SÁNCHEZ BRAVO, A. A. (1998). *La protección del derecho a la libertad informática en la Unión Europea* (Vol. 75). Sevilla: Universidad de Sevilla.

SÁNCHEZ DÍAZ, M. Y VEGA VALDÉS, J.C. (2003). Algunos aspectos teórico-conceptuales sobre el análisis documental y el análisis de información. *Ciencias de la Información*. 34, 2, 49-60

SÁNCHEZ MUÑOZ, L. M. (2012). *El viajero en las redes sociales: hacia una visualización rica y móvil de la huella digital*. Proyecto final de carrera de la Escuela Politécnica Superior Ingeniería en Informática. Madrid: Universidad Carlos III de Madrid [Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/16041/PFC_EVELRS-LMS.pdf?sequence=2]

SARIKAKIS, K. (ed.). (2007). *Media and Cultural Policy in the European Union. European Studies - An Interdisciplinary Series in European Culture, History and Politics*, vol. 24. Amsterdam – Nueva York: Rodopi.

SERRANO JIMÉNEZ, P. (2013). *La comunicación jibarizada. Cómo la tecnología ha cambiado nuestras mentes*. Barcelona: Península.

SIBILIA, P. (2008). *La Intimidad como espectáculo*. Buenos Aires: Fondo de Cultura Económica.

SIBILIA, P. (2009). En busca del aura perdida: Espectacularizar la intimidad para ser alguien. *Psicoperspectivas*, *8*(2), 309-328.

SIERRA CABALLERO, F. (2006). *Políticas de comunicación y educación. Crítica y desarrollo de la sociedad del conocimiento*. Barcelona: Gedisa.

SNIJDERS, C., MATZAT, U., Y REIPS, U. D. (2012). "Big Data": Big Gaps of Knowledge in the Field of Internet Science. *International Journal of Internet Science*, 7, 1, 1-5.

SOLOVE, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 3, 477-564.

SOLOVE, D. J. (2008). Data mining and the security-liberty debate. *The University of Chicago Law Review*, 74, 1, 343-362.

SUÁREZ CANDEL, R. (2009). *Las políticas públicas de la televisión digital terrestre en la Unión Europea. Estudio comparado de Suecia y España*. Tesis doctoral. Barcelona: Universitat Pompeu Fabra. Recuperado el 21 de junio de 2014, de http://repositori.upf.edu/handle/10230/16201

SUNSTEIN, C. R. (2003). República. com. Internet, democracia y libertad. Barcelona: Paidós.

TASCÓN, M. (2013). Big Data. Pasado, presente y futuro. *Telos: Cuadernos de comunicación e innovación*, 95, 47-50.

TELEFÓNICA, F. (2012). *El debate sobre la privacidad y seguridad en la Red: Regulación y mercados* (Vol. 36). Fundación Telefónica.

TELLO DÍAZ, L. (2013). Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook. *Comunicar*, *21*(41), 205-213.

THURMAN, N., Y SCHIFFERES, S. (2012). The future of personalization at news websites. *Journalism Studies*, 13(5-6), 775–790.

TOURIÑO, A. (2014). *El Derecho al olvido y a la intimidad en Internet*. Madrid: Los Libros de la Catarata.

TREMBLAY, G. (2006). Economía Política del espacio público y mutaciones mediáticas. *CIC Cuadernos de Información y Comunicación*, *11*, 223-240.

URZÚA BASTIDA, V. (2012). El espacio público y el derecho a excluir. *Athenea Digital (Revista de Pensamiento e Investigación Social)*, 12, 1, 159-168.

VAN CUILENBURG, J. Y MCQUAIL, D. (2003). Cambios en el paradigma de política de medios. Hacia un nuevo paradigma de políticas de comunicación. *European Journal of Communication*, 18, 2, 181-207.

VEGA MONROY, J. M. (2013). Big Data: las oportunidades profesionales que vienen. *Bit*, (193), 53-55.

VILASAU, M. (2009). *¿Hasta dónde deben regularse las redes sociales?*. Revista Española de Protección de datos, 6, 105-136.

WINOCUR, R. (2001). Redes virtuales y comunidades de internautas: nuevos núcleos de sociabilidad y reorganización de la esfera pública. *Perfiles latinoamericanos: revista de la Facultad Latinoamericana de Ciencias Sociales, Sede México*, (18), 75-92.

WU, D., *et al.* (2003). A framework for classifying personalization scheme used on e-commerce websites. In R. SPRAGUE (ed.), *Proceedings of the 36th Hawaii International Conference on System Science.* January 2003. Los Alamitos, California: IEEE Computer Society Press