



UNIVERSIDAD DE OVIEDO

PROGRAMA DE DOCTORADO DE DERECHO

**EL OLVIDO EN LOS TIEMPOS
DE LAS FAKE NEWS**

Tesis doctoral presentada por **Víctor Escandón Prada**

Dirigida por el Doctor **Ignacio Villaverde Menéndez**

Oviedo, junio de 2019



UNIVERSIDAD DE OVIEDO

PROGRAMA DE DOCTORADO DE DERECHO

**EL OLVIDO EN LOS TIEMPOS
DE LAS FAKE NEWS**

Tesis doctoral presentada por **Víctor Escandón Prada**

Dirigida por el Doctor **Ignacio Villaverde Menéndez**

Oviedo, junio de 2019



RESUMEN DEL CONTENIDO DE TESIS DOCTORAL

1.- Título de la Tesis	
Español/Otro Idioma: EL OLVIDO EN LOS TIEMPOS DE LAS FAKE NEWS.	Inglés: THE RIGHT TO BE FORGOTTEN IN THE TIME OF FAKE NEWS.
2.- Autor	
Nombre: VÍCTOR ESCANDÓN PRADA	DNI/Pasaporte/NIE: -
Programa de Doctorado: DERECHO	
Órgano responsable: COMISIÓN ACADÉMICA	

RESUMEN (en español)

Con la llegada de Internet, se produce un fenómeno distinto en el que el mensaje es tan importante como el medio, ya que antes no era lo mismo que una información se publicase en el New York Times que en un periódico de ámbito local, el medio aumentaba el valor de la información, era una señal de calidad y la dotaba de credibilidad. Lógicamente, el término fake news es relativamente nuevo, pero siempre han existido los bulos, la diferencia es que los bulos eran noticias no contrastadas que no se apoyaban en ningún soporte mediático, lo que les confería una escasa temporalidad. La red ha maximizado el medio, ahora es global y universal, cualquier usuario tiene a su alcance un canal para difundir mensajes, un hecho que antes estaba reservado solo a los medios de comunicación, produciendo un efecto expansivo de gran calado. Los medios de comunicación ya no son solo los emisores de la noticia y el público el receptor, sino que ahora el propio público se convierte a su vez en emisor de una noticia cuando la comparte a través de Twitter, Facebook o Instagram. Eso potencia la inmediatez y hace que no se compruebe, lo que facilita y mucho la proliferación de las noticias falsas. Unas fake news que pueden atentar contra el derecho al honor, la intimidad y la propia imagen del sujeto. Por eso, ahora es más necesario que nunca que las personas pueden ejercitar su derecho al olvido, ya que su imagen no solo se va a poder ver dañada por noticias de su pasado sino por noticias falsas.

Las nuevas tecnologías han hecho que olvidar nuestro pasado se haya convertido en una ardua tarea, ya que siempre habrá un buscador o una red social que pueda recordar cualquier



episodio de nuestra existencia. Nuestra hipótesis de trabajo es que la red ha transformado la dogmática de la privacidad porque su núcleo ya no es el derecho a estar solo, por parafrasear al clásico americano (Warren/Brandeis), sino el derecho a ser olvidado.

El crecimiento acelerado de la sociedad de la información ubica a las nuevas tecnologías en un papel fundamental en la vida cotidiana, mientras la sociedad evoluciona, el derecho no puede quedarse rezagado y menos al margen de esa dinámica. En este sentido, sabiendo la dificultad de que las leyes se anticipen a los cambios sociales, lo que sí es necesario que se vayan adaptando y no vayan tan retrasadas. Nuestros ordenamientos jurídicos están diseñados para dar respuesta a las exigencias de la privacidad en ritmos especialmente lentos y manejando medios de comunicación y divulgación de la información limitados en su impacto y en su permanencia en el tiempo. Internet ha roto ese paradigma y ha acelerado hasta el paroxismo tanto la intensidad y extensión de la difusión de un dato o una información, como su perdurabilidad tempo-espacial. El derecho al olvido trata de dar respuesta a ese cambio de paradigma en el que el tiempo y el potencial irradiador de internet y los motores de búsqueda en la red han puesto en entredicho la eficacia de los mecanismos de garantía de la privacidad hasta ahora conocidos y recogidos en las constituciones y declaraciones de derecho.

La sentencia del TJUE, de 13 de mayo de 2014, contra Google ha puesto las bases de lo que puede ser en un futuro a corto plazo la reclamación de los usuarios en su derecho a ser olvidado. A raíz de dicha sentencia, la Audiencia Nacional ya ha dictado otras sentencias a favor de los implicados, exigiendo a los buscadores *desindexar* su información. Además, es importante señalar las acciones que han llevado a cabo, a raíz de esta sentencia, los principales motores de búsqueda, como Google, que ha puesto un departamento al servicio de los usuarios que quieran denunciar alguna de las informaciones relacionadas con ellos que aparecen en las búsquedas. La sentencia del TJUE, además, suscita al menos dos dudas esenciales: ¿quién es responsable de la difusión de la información en Internet? y ¿cuánto tiempo ha de transcurrir para que una información deje de tener interés público? Trataremos de dar respuesta a estas cuestiones y construir con la realización de esta tesis doctoral una dogmática del derecho al olvido en una sociedad líquida y deseosa de mayor transparencia, también en lo privado.



Con la entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que derogó la Directiva 95/46/CE que se había quedado obsoleta, se abre una nueva etapa en la que habrá que acometer la adaptación necesaria para dar seguridad jurídica a todo el flujo informativo que circula por la red y soluciones a la rápida evolución tecnológica que ha supuesto, a su vez, nuevos retos para la protección de datos. Este nuevo Reglamento reconoce por primera vez, en su artículo 17, el derecho al olvido. Eso sí, como un derecho de supresión. La instantaneidad y universalidad de acceso a la información plantea otra realidad. Una realidad en la que el derecho a la información y el derecho al olvido están muy presentes.

Además, trataremos de definir dogmáticamente qué es el derecho al olvido y cómo lo han ido perfilando las diferentes agencias de protección de datos, analizando las principales resoluciones que han emitido; y, desde luego, la jurisprudencia. Además, haremos una comparativa de las principales agencias en Europa (Francia, España e Italia). Debido a la diferente concepción de la *privacy* que tienen en Estados Unidos, realizaremos una comparativa entre la UE y EEUU, así como las respuestas que ha dado la Corte Iberoamericana de Derechos Humanos ante tal conflicto. Una vez sistematizado y analizado el acervo doctrinal, legal y jurisprudencial antedicho, el siguiente paso es la reconstrucción de la dogmática de la privacidad a partir del derecho al olvido como instrumento de regulación del flujo de información a través de las TICs.

Las nuevas tecnologías han hecho que olvidar nuestro pasado se haya convertido en una ardua tarea, ya que siempre habrá un buscador o una red social que pueda recordar cualquier episodio de nuestra existencia. Nuestra hipótesis de trabajo es que la red ha transformado la dogmática de la privacidad porque su núcleo ya no es el derecho a estar solo, por parafrasear al clásico americano (Warren/Brandeis), sino el derecho a ser olvidado.

El crecimiento acelerado de la sociedad de la información ubica a las nuevas tecnologías en un papel fundamental en la vida cotidiana, mientras la sociedad evoluciona, el derecho no puede quedarse rezagado y menos al margen de esa dinámica. En este sentido, sabiendo la dificultad de que las leyes se anticipen a los cambios sociales, lo que sí es necesario que se vayan



adaptando y no vayan tan retrasadas. Nuestros ordenamientos jurídicos están diseñados para dar respuesta a las exigencias de la privacidad en ritmos especialmente lentos y manejando medios de comunicación y divulgación de la información limitados en su impacto y en su permanencia en el tiempo. Internet ha roto ese paradigma y ha acelerado hasta el paroxismo tanto la intensidad y extensión de la difusión de un dato o una información, como su perdurabilidad tempo-espacial. El derecho al olvido trata de dar respuesta a ese cambio de paradigma en el que el tiempo y el potencial irradiador de internet y los motores de búsqueda en la red han puesto en entredicho la eficacia de los mecanismos de garantía de la privacidad hasta ahora conocidos y recogidos en las constituciones y declaraciones de derecho.

La sentencia del TJUE, de 13 de mayo de 2014, contra Google ha puesto las bases de lo que puede ser en un futuro a corto plazo la reclamación de los usuarios en su derecho a ser olvidado. A raíz de dicha sentencia, la Audiencia Nacional ya ha dictado otras sentencias a favor de los implicados, exigiendo a los buscadores *desindexar* su información. Además, es importante señalar las acciones que han llevado a cabo, a raíz de esta sentencia, los principales motores de búsqueda, como Google, que ha puesto un departamento al servicio de los usuarios que quieran denunciar alguna de las informaciones relacionadas con ellos que aparecen en las búsquedas. La sentencia del TJUE, además, suscita al menos dos dudas esenciales: ¿quién es responsable de la difusión de la información en Internet? y ¿cuánto tiempo ha de transcurrir para que una información deje de tener interés público? Trataremos de dar respuesta a estas cuestiones y construir con la realización de esta tesis doctoral una dogmática del derecho al olvido en una sociedad líquida y deseosa de mayor transparencia, también en lo privado.

Con la entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que derogó la Directiva 95/46/CE que se había quedado obsoleta, se abre una nueva etapa en la que habrá que acometer la adaptación necesaria para dar seguridad jurídica a todo el flujo informativo que circula por la red y soluciones a la rápida evolución tecnológica que ha supuesto, a su vez, nuevos retos para la protección de datos. Este nuevo Reglamento reconoce por primera vez, en su artículo 17, el derecho al olvido. Eso sí, como un derecho de supresión. La instantaneidad



y universalidad de acceso a la información plantea otra realidad. Una realidad en la que el derecho a la información y el derecho al olvido están muy presentes.

Además, trataremos de definir dogmáticamente qué es el derecho al olvido y cómo lo han ido perfilando las diferentes agencias de protección de datos, analizando las principales resoluciones que han emitido; y, desde luego, la jurisprudencia. Además, haremos una comparativa de las principales agencias en Europa (Francia, España e Italia). Debido a la diferente concepción de la *privacy* que tienen en Estados Unidos, realizaremos una comparativa entre la UE y EEUU, así como las respuestas que ha dado la Corte Iberoamericana de Derechos Humanos ante tal conflicto. Una vez sistematizado y analizado el acervo doctrinal, legal y jurisprudencial antedicho, el siguiente paso es la reconstrucción de la dogmática de la privacidad a partir del derecho al olvido como instrumento de regulación del flujo de información a través de las TICs.

RESUMEN (en Inglés)

With the advent of the Internet, the message started to be considered as important as the medium, unlike in previous times when there were clear differences about the consideration of information published in *The New York Times* or in the local newspaper. The medium contributed to increasing the value of the information, became a sign of quality and added credibility. Logically, the term *fake news* is relatively recent, although hoaxes have always existed as uncontrasted news which lacked any medium support, which gave them a sense of temporariness. The Internet has taken the medium to a maximum scale, it has become global and universal and any user has at his/her disposal a channel to spread messages, with huge possibilities for expansion. The media are not only senders of news and audiences, receivers, but the audience has become a sender of information when this is shared by Twitter, Facebook or Instagram as well. This boosts immediacy and likewise there is not time for proving its veracity. Therefore, fake news can threaten the right of honour, privacy and the individual's own image. Consequently, now the right to be forgotten is more needed than ever before, since the people's image could be damaged not only due to information about their past, but also by fake news.



To forget about one's past is now more difficult to achieve thanks to new technologies, because there will always be a search engine or a social medium that can recall any previous episode in one's life. Our hypothesis is based on the notion that the Internet has transformed privacy since its core is no longer the right to be alone, paraphrasing the American classic Warren/Brandeis, but the right to be forgotten.

The rapid growth of the information society has assigned new technologies a fundamental role in daily life, so that, while society evolves, laws cannot remain on the sidelines, and even less, out of the society's limits. In this sense, being aware of the difficulties carried out when the law anticipates social change, we can claim that it is necessary to adapt and to update the legislation. Our legal systems have been designed to provide a slow response to the demands of privacy, employing dissemination and information channels with some limited impact and time constraints. The Internet, however, has disrupted this paradigm and has accelerated both the intensity and the expansion of a data or a piece of information, in time and spatial terms.

The right to be forgotten aims at being the central element within this paradigm change in which time and the boosting effect of the Internet and the web search engines have questioned the efficacy of the mechanisms, so far known and included in constitutional and legal arrangements, which guarantee privacy.

The sentence of the Court of Justice of the European Union (CJEU), of 13 May 2014, against Google has laid the foundations of the likely future petition of consumers of their right to be forgotten. As a result of this sentence, the Spanish National Court, or *Audiencia Nacional*, has enacted several laws supporting the cause of the parties concerned, urging search engines *deindexing* personal information. Moreover, due to the afore-mentioned European sentence, it is important to highlight the actions carried out by the main search engine companies, like Google, which has created a department to deal with legal removal requests of users, when they denounce the use of personal information in search engines. The sentence of the Court of Justice of the European Union also brings up at least two serious doubts about, firstly, who is responsible of information dissemination on the Internet and, secondly, about how long information should be considered of public interest.



In the present doctoral thesis we aim at providing some answers to these questions and at building up a legal dogmatics of the right to be forgotten in a liquid society which aspires to gain more transparency, also in information privacy.

After the enforcement of the EU Rule 2016/679 of the European Parliament and the Commission, of 27 April 2016, on the protection of people with respect to the treatment of personal data and free circulation of these data, which has repealed the already outdated Directive 95/46/CE, a new period has arrived in which it will be necessary to make adjustments in order to guarantee legal security to all the content that is shared on the Internet and to propose solutions to face the rapid technological evolution which has entailed, in turn, new challenges for data protection. This new Regulation gives recognition, for the first time, to the right to be forgotten in article 17, as a right of abolition. The instantaneous and universal nature of information access, however, presents another reality in which the right of information and the right to be forgotten have gained significance.

In addition, we will attempt at defining, from a dogmatic point of view, what the right to be forgotten is and how the different data protection agencies have shaped it, while analysing the main legal resolutions and jurisprudence about it. Moreover, we will compare the main agencies in Europe (France, Spain and Italy) and we will pay particular attention to the situation in the United States and the United Kingdom, given the special concept of *privacy* in these countries, and to the replies of the Latin American Court of Human Rights with respect to this conflict. Once the doctrine, the legal and judiciary foundations have been examined, the next step is the dogmatics of privacy that originates from the right to be forgotten as an instrument to regulate information flow through new information and communication technologies.

A Jaime, por ser mi inspiración.

ÍNDICE

ABREVIATURAS	6
INTRODUCCIÓN	7
CAPÍTULO 1. LA SENTENCIA DEL TJUE CONTRA GOOGLE. EL NACIMIENTO DEL DERECHO AL OLVIDO	12
1.1. EL TJUE A FAVOR DEL DERECHO AL OLVIDO DIGITAL	14
1.1.1. Antecedentes de la sentencia	14
1.1.2. Mario Costeja vence a Google	19
1.1.3. Comentarios y críticas a la sentencia	22
1.2. EFECTOS DERIVADOS DE LA STJUE	29
1.2.1. Informe del Comité asesor de Google	29
1.2.2. Un formulario para que Google te olvide	31
1.3. EL TJUE RECHAZA EL DERECHO AL OLVIDO DE LOS DATOS DEL REGISTRO MERCANTIL	32
1.4. LA AUDIENCIA NACIONAL RECONOCE EL DERECHO AL OLVIDO	35
1.5. EL TRIBUNAL SUPREMO RECONOCE LA RESPONSABILIDAD DEL EDITOR DE UNA PÁGINA WEB	37
1.5.1. Google Spain, ¿es o no responsable del derecho al olvido?	42
1.6. LOS NOMBRES PROPIOS COMO CRITERIO DE BÚSQUEDA EN UNA HEMEROTECA DIGITAL VULNERAN EL DERECHO AL OLVIDO	47
1.7. LA IMPORTANCIA DE LA AEPD EN LA EVOLUCIÓN DEL DERECHO AL OLVIDO	51
CAPÍTULO 2. EL DERECHO AL OLVIDO, UNA REALIDAD SOCIAL	55
2.1. CONCEPTO Y CONTEXTUALIZACIÓN DEL DERECHO AL OLVIDO.....	62
2.2. EL DERECHO A LA MUERTE DIGITAL	68
2.3. NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS	73
2.4. LA PROBLEMÁTICA DE LOS BUSCADORES Y LAS REDES SOCIALES	76

2.5. EL MECANISMOS PARA HACER MÁS EFICAZ EL DERECHO AL OLVIDO.....	80
2.5.1. Aplicaciones tecnológicas para no dejar rastro y borrar el pasado	81
2.5.2. Derechos reconocidos: rectificación, cancelación, oposición y supresión	82
CAPÍTULO 3. EL DERECHO A LA INTIMIDAD ELECTRÓNICA	92
3.1. EL DERECHO A LA VIDA PRIVADA EN LAS REDES.....	92
3.1.1. Usurpación de la identidad y fraudes online	94
3.1.2. Régimen jurídico de la vida privada electrónica	99
3.1.3. El Registro del usuario de una red social, protección de la vida privada electrónica (y de la intimidad).....	103
3.1.4. Desactivación y eliminación del perfil del usuario, protección de la vida privada electrónica (y de la intimidad).....	107
3.1.5. Regulación de los criterios sobre vida privada en las redes sociales	108
CAPÍTULO 4. EL DERECHO AL OLVIDO, UN PROBLEMA GLOBAL.....	110
4.1. EL DERECHO AL OLVIDO EN EUROPA	110
4.1.1. Francia, un referente en el derecho al olvido.....	110
4.1.2. Italia apuesta por el principio de finalidad	115
4.2. IBEROAMÉRICA, UN ABÁNICO DE LEYES Y RESOLUCIONES	118
4.3. ESTADOS UNIDOS, LA ANTÍTESIS DEL DERECHO AL OLVIDO	125
CAPÍTULO 5. LA DOGMÁTICA DEL DERECHO AL OLVIDO	138
5.1. EL DERECHO AL OLVIDO, ¿ES UN DERECHO FUNDAMENTAL?	139
5.2. DIFERENCIAS ENTRE INTIMIDAD Y VIDA PRIVADA	147
5.3. EL DERECHO AL OLVIDO COMO DIMENSIÓN DEL CONTROL DE LOS DATOS PERSONALES	148
5.3.1. El derecho al olvido como seña de identidad personal.....	156
5.4. EL RECONOCIMIENTO DEL DERECHO AL OLVIDO COMO UN DERECHO DE SUPRESIÓN	158
5.5. LÍMITES DEL DERECHO AL OLVIDO	162

5.5.1. La libertad de información vs. Derecho al olvido	162
5.5.1.1. Las hemerotecas digitales como estandartes de la libertad de información	161
5.5.1.2. ¿La “tasa Google” vulnera la libertad de información?	174
5.5.2. La libertad de expresión vs. Derecho al olvido	176
5.5.2.1. Una nueva libertad de expresión a través de la red	177
5.5.2.2. Cuestiones de responsabilidad en el ejercicio de la libertad de expresión a través de Internet	185
5.5.3. La intimidad vs. Derecho al olvido	190
5.5.3.1. Los antecedentes penales, ¿forman parte de la intimidad y han de ser olvidados?	191
5.5.3.2. Las sanciones administrativas también prescriben	200
5.5.4. Interés público vs. Interés privado en la privacidad	201
5.6. LA PROTECCIÓN DE DATOS COMO LIBERTAD INFORMÁTICA	216
5.7. EL TRATAMIENTO DE LOS DATOS PERSONALES EN LA RED	220
5.7.1. El principio de reconocibilidad de la imagen	229
5.7.1.1. Las imágenes de menores en las redes	232

CAPÍTULO 6. EL AUGE DE LAS FAKE NEWS Y EL PROBLEMA DE CÓMO ABORDARLAS	234
6.1. UN CONCEPTO ACTUAL, PERO NO TAN NOVEDOSO	234
6.1.1. Antecedentes.....	237
6.1.2. Consecuencias de las fake news	241
6.2. LAS ELECCIONES PRESIDENCIALES ESTADOUNIDENSES DE 2016 COMO PUNTO DE PARTIDA	242
6.2.1. ¿HUBO O NO UN CONSUMO MASIVO DE FAKE NEWS?.....	243
6.3. EL PROBLEMA DE LA INMEDIATEZ DE LAS REDES SOCIALES	247
6.3.1. UN PERIODISMO LENTO COMO SOLUCIÓN.....	249
6.4. LA GRAN AMENAZA DE LAS DEMOCRACIAS ACTUALES.....	250
6.4.1. Los países, obligados a actuar	250
6.4.1.1. Alemania, primera ley europea contra las fake news	251
6.4.1.2. Sudamérica apuesta por regular Internet	254
6.4.1.3. Estados Unidos: las fake news frente a la libertad de expresión.....	260

6.5. PROPUESTAS PARA COMBATIR LAS FAKE NEWS. EL DERECHO AL OLVIDO COMO LIMITE A LAS FAKE NEWS	261
6.5.1. La responsabilidad de las redes sociales.....	261
6.5.2. Los algoritmos como solución al problema.....	266
6.5.3. El derecho al olvido: una eficaz respuesta a las fake news	268
CONCLUSIONES	271
JURISPRUDENCIA	279
BIBLIOGRAFÍA	285

ABREVIATURAS

AEPD	Agencia Española de Protección de Datos
AN	Audiencia Nacional
AP	Audiencia Provincial
Art.	Artículo
BOE	Boletín Oficial del Estado
CC	Código Civil
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos
CNIL	Comisión Nacional de la Informática y las libertades
FJ	Fundamento Jurídico
IP	Protocolo de Internet
LO	Ley Orgánica
LOPD	Ley Orgánica de Protección de Datos
LSSICE	Ley de Servicios de la Sociedad de la Información y Comercio Electrónico
NSA	Agencia de Seguridad Nacional
P2P	Red de Pares
PS	Procedimiento Sancionador
R	Resolución
RD	Real Decreto
SAN	Sentencia Audiencia Nacional
SAP	Sentencia Audiencia Provincial
STC	Sentencia Tribunal Constitucional
STJUE	Sentencia Tribunal de Justicia de la Unión Europea
STS	Sentencia Tribunal Supremo
STSJ	Sentencia Tribunal Superior de Justicia
TC	Tribunal Constitucional
TEDH	Tribunal Europeo de Derechos Humanos
TFUE	Tratado de Funcionamiento de la Unión Europea
TIC	Tecnologías de la Información y la Comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TS	Tribunal Supremo
UE	Unión Europea

INTRODUCCIÓN

Lo que ha conseguido Internet, además de la globalización de sus usuarios, es crear un mundo paralelo en el que existen enormes dificultades para identificar las fuentes de información, sus servidores, el flujo y almacenamiento de esa información, la identificación de responsables, la sanción de conductas antijurídicas y la efectiva garantía del derecho a ser olvidado como manifestación del derecho a la privacidad a través habida cuenta del tráfico de información que se aloja en servidores ubicados en terceros países. En esa tarea no cabe duda de que el diseño y acuerdo sobre una legislación universal que permita controlar ese flujo transfronterizo de la información, puede ser un instrumento de garantía de la privacidad de enorme utilidad y eficacia donde la rapidez y agilidad de la respuesta es esencial para reducir el daño.

Con las nuevas tecnologías se produce un fenómeno distinto en el que el mensaje es tan importante como el medio, ya que antes no era lo mismo que una información se publicase en el New York Times que en un periódico de ámbito local, el medio aumentaba el valor de la información, era una señal de calidad y la dotaba de credibilidad. Lógicamente, el término fake news es relativamente nuevo, pero siempre han existido los bulos, la diferencia es que los bulos eran noticias no contrastadas que no se apoyaban en ningún soporte mediático, lo que les confería una escasa temporalidad. La red ha maximizado el medio, ahora es global y universal, cualquier usuario tiene a su alcance un canal para difundir mensajes, un hecho que antes estaba reservado solo a los medios de comunicación, produciendo un efecto expansivo de gran calado. Los medios de comunicación ya no son solo los emisores de la noticia y el público el receptor, sino que ahora el propio público se convierte a su vez en emisor de una noticia cuando la comparte a través de Twitter, Facebook o Instagram. Eso potencia la inmediatez y hace que no se compruebe, lo que facilita y mucho la proliferación de las noticias falsas. Unas fake news que pueden atentar contra el derecho al honor, la intimidad y la propia imagen del sujeto. Por eso, ahora es más necesario que nunca que las personas pueden ejercitar su derecho al olvido, ya que su imagen no solo se va a poder ver dañada por noticias de su pasado sino por noticias falsas. De ahí que la protección de la vida privada y la reputación encuentren en el derecho al olvido un instrumento eficaz para limitar el daño que pueden provocar las noticias falsas divulgadas en las redes sociales, ya que, al hecho que conlleva la publicación de una

información falsa, se suma la intensificación de su capacidad para difamar al aprovechar la red para propagarse sin ningún límite físico de espacio y tiempo que pudiese minimizar el daño.

El objetivo de esta tesis es reconstruir la dogmática del derecho a la privacidad desde el paradigma del derecho al olvido en los flujos de información en la red. Aquí ya no se trata de definir la privacidad como el poder de decidir quién puede acceder a ella (dimensión positiva); sino como el poder de desaparecer del flujo informativo (dimensión negativa), incorporando un elemento prestacional a un derecho concebido tradicionalmente como derecho reaccional. Internet ha transformado la dogmática de la privacidad porque su núcleo ya no es el derecho a estar solo sino el derecho a ser olvidado.

Durante el trabajo, hemos desarrollado un método inductivo, por el que las conclusiones obtenidas han surgido del análisis de casos, sentencias y leyes. La base del trabajo se sustenta en el estudio de diferentes casos concretos para obtener globalmente unos principios básicos. Para entender correctamente el derecho al olvido, partimos de la sentencia, en el primer capítulo, del TJUE C-131/12, de 13 de mayo de 2014, caso *Google Spain, S.L. y Google Inc. v. AEPD y Mario Costeja González*, en el que, aunque sin nombrarlo, el Tribunal Europeo aborda por primera vez el problema del derecho al olvido.

También es importante para desarrollar nuestro concepto del derecho al olvido, conocer sus orígenes, su evolución. Es cierto que antes del auge de Internet, las informaciones de los medios de comunicación estaban en las hemerotecas al alcance de todas aquellas personas interesadas en acceder a ellas en formato papel. Una búsqueda laboriosa que sólo era realizada por quienes estaban muy interesados en un asunto concreto. Con la llegada de Internet, todas estas informaciones se han digitalizado y están al alcance de cualquiera desde un ordenador. Se abre una nueva etapa en la que habrá que acometer la adaptación necesaria para dar seguridad jurídica a todo el flujo informativo que circula por la red, ya que la Directiva CE/95/46 se había quedado obsoleta. Por este motivo, el Parlamento Europeo y el Consejo se han visto en la obligación de aprobar el Reglamento (UE) 2016/679, de 27 de abril de 2016, por la rápida evolución tecnológica que ha supuesto, a su vez, nuevos retos para la protección de datos. Analizaremos este

nuevo Reglamento y lo que supone que, en su artículo 17, reconozca el derecho al olvido. Eso sí, como un derecho de supresión. La instantaneidad y universalidad de acceso a la información plantea otra realidad. Una realidad en la que el derecho a la información y el derecho al olvido están muy presentes.

Estudiaremos las medidas que se han aplicado en diferentes países, referidas a la solicitud de los usuarios de que se les reconozca el derecho al olvido, y las diferencias entre el sistema *common law* y el civilista. Resulta curioso ver cómo, a pesar de que el principio de privacidad fue desarrollado por los norteamericanos Warren y Brandeis, ha sido en Europa, sobre todo en Francia, España e Italia, donde más se ha desarrollado el concepto de privacidad y se ha tratado de defender el derecho al olvido de sus ciudadanos, a través de sus agencias de protección de datos. Todo lo contrario a lo que sucede en los Estados Unidos, cuyas medidas de protección de la privacidad no se acercan a los objetivos de las leyes europeas en esta materia, en donde el derecho al olvido o, como denominan ellos, *right to be forgotten*, tendrá difícil cabida en su ordenamiento jurídico porque es difícil ajustarlo con la Primera Enmienda y el derecho a la libertad de expresión, debido a que el derecho al olvido puede ser interpretado como censura y así lo ha afirmado la Corte Suprema en varias sentencias que hemos analizado.

Hay que distinguir, para hacer un buen análisis del derecho al olvido, entre el concepto de privacidad o, como recoge el artículo 8 del CEDH, vida privada y el de intimidad, concretado por la CE en su artículo 18.1. El TEDH ha dado a la vida privada un concepto más amplio que, mientras que la CE garantiza la intimidad, entendida como el derecho de la persona a impedir cualquier intromisión sobre aquel ámbito de su vida privada que considera vetado a los demás.

A lo largo del trabajo, abordaremos los mecanismos para hacer más eficaz el derecho al olvido y examinaremos cuándo y por qué se puede solicitar. La primera de las medidas que se pueden adoptar es fijar, como apuntó Mayer-Schönberger, una fecha de caducidad a los contenidos, generando un derecho al olvido a priori. También estudiaremos las diferentes aplicaciones tecnológicas que existen para borrar el pasado y no dejar rastro y los derechos ya reconocidos, como son el de rectificación, cancelación, oposición y, desde la entrada en vigor del Reglamento (UE) 2016/679, de

27 de abril de 2016, también el de supresión, que pueden ser usados como elementos para regular el derecho al olvido.

Los derechos a la intimidad y a la protección de datos personales atribuyen a la persona los poderes necesarios y suficientes para hacer efectivo el derecho al olvido. Veremos la relación que existe entre el derecho al olvido y estos derechos fundamentales y los límites que éstos pueden poner a la hora de abordar un derecho que, como iremos desarrollando a lo largo de la tesis, no puede ser considerado como un derecho fundamental sino más bien podemos concluir que el derecho al olvido no es un derecho fundamental sino un derecho instrumental derivado de otros.

Los límites que derechos fundamentales como la libertad de información, la libertad de expresión o la intimidad imponen al derecho al olvido son abordados a lo largo del trabajo. Si considerásemos el derecho al olvido como un derecho fundamental, habría que estudiar cada caso para dilucidar cuál debería prevalecer en el caso de que colisionasen ambos, pero, como hemos señalado, lo vemos más como un derecho instrumental, por lo tanto analizaremos como pueden encajarse ambos derechos en favor del ciudadano.

La consolidación de Internet ha producido un aumento de las conductas lesivas a través de ataques a la información patrimonial y de acceso a datos reservados, realizado con el objetivo de conseguir información personal o profesional. Relacionados con la intimidad, indagaremos en nuevos delitos como la interceptación de los correos electrónicos, la usurpación de la identidad y los fraudes online. Además, las nuevas tecnologías también han provocado una mayor vulnerabilidad del derecho al honor, intimidad y propia imagen. Con frecuencia, los usuarios captan y reproducen en las redes sociales imágenes de terceros en su vida cotidiana. Dicha captación y reproducción constituyen datos de carácter personal, de ahí que resulte necesario el consentimiento de sus titulares, veremos como la jurisprudencia ha partido del principio de reconocibilidad, lo que ha provocado que el hecho de que la imagen resulte un tanto borrosa no quita para que pueda existir intromisión si la reproducción permite la perfecta identificación de la persona. En el caso de los menores de edad, si el tratamiento de las imágenes se efectúa por parte de los padres, la aplicación de la ley no

tendrá efecto cuando la publicación de la imagen quede limitada al ámbito personal o familiar.

Abordaremos en nuestro estudio la problemática que suscita la confrontación entre el interés público de la información y el interés privado de la imagen a través de las sentencias del TC y del TS. Para ello, resultaba inevitable realizar una distinción entre personas públicas o privadas, ya que el tratamiento de las informaciones y la resolución a la confrontación entre el derecho a la información y el derecho a la propia imagen no sería la misma.

La universalidad de Internet hace que el artículo 10 del Convenio Europeo de los Derechos Humanos adquiera otro significado, ya que con Internet han desaparecido las fronteras y los comentarios circulan libremente por cualquier rincón del mundo. Contra lo que pudiese parecer, a medida que aumenta la libertad de expresión (foros, blogs) y la transparencia informativa, en la práctica, cada vez son más los casos en los que no se respetan los derechos fundamentales de las personas, ya sean desde las redes sociales o bien desde las propias Administraciones.

En la investigación, trataremos también de averiguar, partiendo de la base de que las comunicaciones electrónicas fomentan el derecho de acceso a la información, el cual es un elemento de la transparencia, si la radical transparencia que favorece la comunicación electrónica tiene un coste tan elevado que, en la práctica, si el Derecho tarda en reaccionar, muchos de esos costes serían inasumibles en el terreno de los derechos personales. Además, los excesos en la transparencia pueden ser tan negativos como las prácticas opacas cotidianas, tanto de la Administración Pública como del sector privado.

Para finalizar, en cuanto a las redes colaborativas hemos analizado la evolución en la jurisprudencia española al respecto, pasando de considerar que los links no son delito a la ilicitud de los enlaces que publican en su web por tratarse de comunicaciones públicas no autorizadas. Veremos si Google puede pasar de ser un mero índice de contenidos de búsqueda y aplicársele el mismo trato que a las redes colaborativas.

CAPÍTULO 1. LA SENTENCIA DEL TJUE CONTRA GOOGLE. EL NACIMIENTO DEL DERECHO AL OLVIDO

¿Quién no ha buscado alguna vez su nombre en Google? El resultado de búsqueda, a veces, da lugar a sorpresas y vemos nuestro nombre asociado a situaciones que creíamos olvidadas y para las que igual no estamos preparados para afrontar o, en el peor de los casos, hechos vinculados a noticias falsas, que circulan por la red. Cómo hacer que esas informaciones desaparezcan si ya pensábamos que lo habíamos hecho o que no existían.

“Somos la generación Google”, así de tajante se muestra Solove que cree que “sin motores de búsqueda, Internet sería una interminable extensión digital de balbuceo, y el hallazgo de cualquier pieza particular de información sería similar a la localización de un grano de arena en el desierto del Sahara”. En estos tiempos ya “no es necesario contratar a un investigador privado, sólo se tiene que ir Google, escribir un nombre en el cuadro de búsqueda, pulsar el botón...y listo, tienes una lista de páginas web con información sobre ese individuo. Todo el mundo está en Google y todo el mundo busca en Google”¹.

No todos los autores creen que Google sea sólo un buscador. Alejandro Suárez deja en el aire una reflexión: “si piensas que Google es un buscador de Internet, estás equivocado. Incluso si piensas que es el buscador por antonomasia, debo decirte que sigues estando equivocado, ya que, en realidad, Google es una de las empresas más grandes, más ambiciosas y más poderosas del mundo. Es un gigante ocasionalmente descontrolado que no sólo domina a sus anchas la red de redes, sino que además tiene intereses en muchas otras industrias”².

¹ SOLOVE, D. J. (2007). *The future of reputation: Gossip, rumor, and privacy on the Internet*. Yale University Press, pág. 9. Véase también PRENSKY, M. (2001). Digital natives, digital immigrants. *MCB University Press*. Vol. 9, nº5; BRINGUÉ, X. y SÁDABA-CHALEZQUER, C. (2009). *La generación interactiva en España. Niños y adolescentes ante las pantallas*. Colección Fundación Telefónica. Cuaderno nº22. Ariel; y AZURMENDI ADARRAGA, A. (2014). *Derecho de autodeterminación informativa y el derecho al olvido: la generación “Google” del derecho a la vida privada*. A decade of transformations. Proceedings of the 10th International Conference on Internet, Law & Politics. Universitat Oberta de Catalunya. Huygens. Barcelona.

² SUÁREZ SÁNCHEZ-OCAÑA, A. (2012). *Desnudando a Google. La inquietante realidad que no quieren que conozcas*. Deusto, pág. 12.

La AEPD comenzó en el año 2007 a recibir las primeras reclamaciones sobre el ejercicio del derecho al olvido para evitar la difusión de sus datos en Internet. En 2013, el número de reclamaciones resueltas fueron de 226, de las cuales 157 se han dirigido frente a los prestadores de servicios de búsqueda en internet. El ejercicio de los citados derechos no supone un reconocimiento automático, sino que es necesario valorar las circunstancias concurrentes en cada caso³.

La Audiencia Nacional se personó y planteó varias cuestiones prejudiciales ante el Tribunal de Justicia de la Unión Europea en lo relativo al contencioso existente entre Google y la AEPD. El TJUE con su sentencia C-131/12, de 13 de mayo de 2014, caso *Google Spain, S.L. y Google Inc. v. AEPD y Mario Costeja González*, respaldó la opinión de la AEPD contra Google, aunque es conveniente destacar que el TJUE en ningún momento utiliza la expresión derecho al olvido. Por tanto, se puede intuir que esta sentencia no es más que un punto de inicio de un concepto que, aunque no explícitamente, ha sido reconocido, por primera vez, por la jurisprudencia, aunque bien es cierto que culpabilizar, en este caso, a Google sobre el tratamiento de la información, exigiéndole su retirada puede generar un conflicto, ya que, no deja de ser un mero buscador de información que aglutina todos aquellos contenidos relacionados con la búsqueda. Por lo que, lo correcto, para poder hablar de un verdadero derecho al olvido, sería que se exigiese la retirada a la fuente original.

Uno de los errores más comunes al analizar la STJUE es que, como apunta Víctor Seisdedos, “el derecho al olvido se trata de un nuevo derecho surgido a partir de la STJUE. Esto es total y absolutamente erróneo y necesita ser matizado. El derecho al olvido es la proyección en internet de derechos ya existentes, porque tanto la LOPD como la Directiva CE/95/46 ya regulaban los derechos de cancelación y el derecho de oposición. Por lo tanto no es un derecho surgido por mandato del TJUE. Lo único que el

³ *Memoria de la AEPD 2013*. Agencia Española de Protección de Datos. Madrid, 2014, pág. 33. Además, en la memoria se detalla que “el promedio de resoluciones estimatorias de las reclamaciones de los ciudadanos ascendió al 26,10%, porcentaje que es superior en relación con los Boletines y diarios oficiales (45,65%) e inferior respecto de los buscadores en internet (22,29%) y los medios de comunicación (13,04%)”.

derecho al olvido es revolucionario es en la desvinculación de los enlaces de la lista de resultados con el nombre en concreto”⁴.

1.1. EL TJUE A FAVOR DEL DERECHO AL OLVIDO DIGITAL

El Caso Costeja ha puesto sobre la mesa algo que nadie se había planteado hasta ahora, el derecho al olvido digital. Hasta ahora se producía un olvido físico y temporal porque el medio era material, lo provocaba las limitaciones físicas del medio para que se pudiese recordar y acceder a él, pero Internet ha roto esas barreras, lo que hace que el olvido ahora tenga sentido, porque antes ya se olvidaba por dichas limitaciones. Con esta sentencia del TJUE se empezó a popularizar el derecho al olvido y su reconocimiento se formalizó con la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos.

1.1.1. Antecedentes de la sentencia

El 5 de marzo de 2010, Mario Costeja González presentó ante la AEPD una reclamación contra el periódico La Vanguardia y contra Google Spain y Google Inc, ya que al introducir su nombre en Google, obtenía como resultados de búsqueda en los dos primeros lugares, dos *links* que conducían a dos artículos de La Vanguardia (19 de enero y 9 de marzo de 1998) en las que figuraba un anuncio de una subasta de inmuebles relacionada con un embargo por deudas a la Seguridad Social, que mencionaba el nombre de Mario Costeja González.

El reclamante solicitaba a la AEPD, por un lado, que se exigiese a La Vanguardia eliminar o modificar la publicación para que no apareciesen sus datos personales, o

⁴ SEISDEDOS POTES, V. (2014). Derecho al olvido. Jaque a Google en Europa. *Cuadernos de Derecho Actual* nº2, pág. 111. Puede verse también en: FERNÁNDEZ GARCÍA-ARMERO, P. (2018). El derecho al olvido. *Cuadernos de Derecho Actual* nº9, págs. 421-439; ARENAS RAMIRO, M. (2014). Unforgettable: a propósito de la STJUE de 13 de mayo de 2014. Caso Costeja (Google vs. AEPD). *Revista Teoría y Realidad Constitucional*, nº3, págs. 537-558; y GARCÍA-ATANCE Y GARCÍA DE MORA, M.V. (2011). *Derechos y libertades en la Constitución Española de 1978*. Editorial Sanz y Torres. Madrid.

utilizar las herramientas facilitadas por los motores de búsqueda para proteger estos datos. Por otro lado, solicitaba que se exigiese a Google Spain o a Google Inc. que eliminaran u ocultaran sus datos personales para que dejaran de incluirse en sus resultados de búsqueda y dejaran de estar ligados a los enlaces de La Vanguardia. En este sentido, Costeja afirmaba que el embargo al que se vio sometido en su día estaba totalmente solucionado y resuelto desde hace años y carecía de relevancia actualmente⁵.

La AEPD desestimó la reclamación en lo referente a La Vanguardia, al considerar que la publicación que ésta había llevado a cabo estaba legalmente justificada, dado que había tenido lugar por orden del Ministerio de Trabajo y Asuntos Sociales y tenía por objeto dar la máxima publicidad a la subasta para conseguir la mayor concurrencia de licitadores. En cambio, estimó la reclamación dirigida contra Google Spain y Google Inc. al considerar que quienes gestionan motores de búsqueda están sometidos a la normativa en materia de protección de datos, dado que llevan a cabo un tratamiento de datos del que son responsables y actúan como intermediarios de la sociedad de la información. La AEPD consideró que estaba facultada para ordenar la retirada e imposibilitar el acceso a determinados datos por parte de los gestores de motores de búsqueda cuando considere que su localización y difusión puede lesionar el derecho fundamental a la protección de datos y a la dignidad de la persona entendida en un sentido amplio, lo que incluye la mera voluntad del particular afectado cuando quiere que tales datos no sean conocidos por terceros. El director de la AEPD instó a Google

⁵ En este sentido, NOVAL LLAMAS, J. J. (2012). Algunas consideraciones sobre la futura regulación del Derecho al olvido. *Revista de la contratación electrónica* nº120. Octubre-diciembre, págs. 29-30; recoge que “hasta el presente, las fronteras de la privacidad estaban defendidas por el tiempo y el espacio. El primero procuraba, con su transcurso, que se evanescieran los recuerdos de las actividades ajenas, impidiendo, así, la configuración de una historia lineal e ininterrumpida de la persona; el segundo, con la distancia, que imponía, hasta hace poco difícilmente superable, impedía que tuviésemos conocimiento de los hechos que, protagonizados por los demás, hubieran tenido lugar lejos de donde nos hallábamos. El tiempo y el espacio operaban, así, como salvaguarda de la privacidad de la persona. Uno y otro límite han desaparecido hoy, las modernas técnicas de comunicación permiten salvar sin dificultades el espacio, y la informática posibilita almacenar todos los datos que se obtienen a través de las comunicaciones y acceder a ellos en apenas segundos, por distante que fuera el lugar donde transcurrieron los hechos, o remotos que fueran estos”.

“para que adopte las medidas necesarias para retirar los datos de su índice e imposibilite el acceso futuro a los mismos”⁶.

La AEPD basó su decisión, amparándose en la Ley 34/2002 de 11 de julio, dictada para el desarrollo de la Directiva 2000/31/CE, en la que se incluye a los buscadores como servicio de la sociedad de la información, en concreto como un “servicio de intermediación”. La AEPD, amparándose en su condición de autoridad competente y aplicando los artículos 8 y 17 de dicha Ley, establece que puede “exigirle al buscador la retirada de los datos personales del afectado que atenten o pueden atentar contra determinados principios (entre ellos la dignidad de la persona) o cuando tengan conocimiento efectivo que de la información que remiten puede lesionar derechos de tercero susceptibles de indemnización”.

Google Spain y Google Inc. interpusieron sendos recursos contra dicha resolución ante la Audiencia Nacional, que abordó la aplicación territorial de la normativa comunitaria y nacional en materia de protección de datos. La AN estableció como criterios de conexión el artículo 4 de la Directiva 95/46/CE⁷ y el art. 2.1 a) y c) de la LOPD 15/1999, dictada para transponer al derecho español dicha norma comunitaria. Tras analizar el caso decidió suspender el procedimiento y plantear al TJUE diferentes

⁶ R/01680/2010 AEPD, de 30 de julio de 2010.

⁷ Directiva 95/46/CE. Artículo 4. Derecho nacional aplicable: “**1.** Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: **a)** el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable. **b)** El responsable del tratamiento no esté establecido en el territorio del Estado miembro, sino en un lugar en que se aplica su legislación nacional en virtud del Derecho internacional público. **c)** El responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea. **2.** En el caso mencionado en la letra c) del apartado 1, el responsable del tratamiento deberá designar un representante establecido en el territorio de dicho Estado miembro, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento”.

cuestiones prejudiciales⁸. Por otro lado, también se formularon una serie de preguntas vinculadas a la actividad de los buscadores como proveedores de contenidos en relación con la Directiva 95/46/CE de Protección de Datos⁹.

⁸ Cuestiones formuladas al TJUE. **1.** ¿Debe interpretarse que existe un establecimiento, en los términos descritos en el art. 4.1.a) de la Directiva 95/46/CE, cuando concorra alguno o algunos de los siguientes supuestos: cuando la empresa proveedora del motor de búsqueda crea en un Estado Miembro una oficina o filial destinada a la promoción y venta de los espacios publicitarios del buscador, que dirige su actividad a los habitantes de ese Estado; o cuando la empresa matriz designa a una filial ubicada en ese Estado miembro como su representante y responsable del tratamiento de dos ficheros concretos que guardan relación con los datos de los clientes que contrataron publicidad con dicha empresa; o cuando la oficina o filial establecida en un Estado miembro traslada a la empresa matriz, radicada fuera de la Unión Europea, las solicitudes y requerimientos que le dirigen tanto los afectados como las autoridades competentes en relación con el respeto al derecho de protección de datos, aun cuando dicha colaboración se realice de forma voluntaria? **2.** ¿Debe interpretarse el art. 4.1.c) de la Directiva 95/46/CE en el sentido de que existe un recurso a medios situados en el territorio de dicho Estado miembro cuando un buscador utilice arañas o robots para localizar e indexar la información contenida en páginas web ubicadas en servidores de ese Estado miembro o cuando utilice un nombre de dominio propio de un Estado miembro y dirija las búsquedas y los resultados en función del idioma de ese Estado miembro? **3.** ¿Puede considerarse como un recurso a medios, en los términos del art. 4.1.c) de la Directiva 95/46/CE, el almacenamiento temporal de la información indexada por los buscadores en internet? Si la respuesta a esta última cuestión fuera afirmativa, ¿puede entenderse que este criterio de conexión concurre cuando la empresa se niega a revelar el lugar donde almacena estos índices alegando razones competitivas? **4.** Con independencia de la respuesta a las preguntas anteriores y especialmente en el caso en que se considerase por el Tribunal de Justicia de la Unión que no concurren los criterios de conexión previstos en el art. 4 de la Directiva: ¿debe aplicarse la Directiva 95/46/CE en materia de protección de datos, a la luz del art. 8 de la Carta Europea de Derechos Fundamentales, en el país miembro donde se localice el centro de gravedad del conflicto y sea posible una tutela más eficaz de los derechos de los ciudadanos de la Unión Europea?

⁹ **1.** En relación con la actividad del buscador de la empresa Google en internet, como proveedor de contenidos, consistente en localizar la información publicada o incluida en la red por terceros, indexarla de forma automática, almacenarla temporalmente y finalmente ponerla a disposición de los internautas con un cierto orden de preferencia, cuando dicha información contenga datos personales de terceras personas: ¿debe interpretarse una actividad como la descrita comprendida en el concepto de tratamiento de datos contenido en el art. 2.b de la Directiva 95/46/CE? **2.** En caso de que la respuesta anterior fuera afirmativa y siempre en relación con una actividad como la ya descrita: ¿Debe interpretarse el artículo 2.d) de la Directiva 95/46/CE, en el sentido de considerar que la empresa que gestiona el buscador Google es responsable del tratamiento de los datos personales contenidos en las páginas web que indexa? **3.** En el caso de que la respuesta anterior fuera afirmativa: ¿Puede la autoridad nacional de control de datos (en este caso la Agencia Española de Protección de Datos), tutelando los derechos contenidos en el art. 12.b) y 14.a) de la Directiva 95/46/CE, requerir directamente al buscador de la empresa Google para exigirle la

Respecto al alcance del derecho de cancelación y/o oposición en relación con el derecho al olvido se plantea la siguiente pregunta: ¿Debe interpretarse que los derechos de cancelación y bloqueo de los datos, regulados en el art. 12.b) y el de oposición, regulado en el art. 14.a) de la Directiva 95/46/CE comprenden que el interesado pueda dirigirse frente a los buscadores para impedir la indexación de la información referida a su persona, publicada en páginas web de terceros, amparándose en su voluntad de que la misma no sea conocida por los internautas cuando considere que puede perjudicarlo o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?” (Auto AN 19/2012, de 27 de febrero. Sala de lo Contencioso. Sección 1ª).

Previo a la resolución del TJUE, el Abogado General asignado al caso, Niilo Jääskinen, emitió sus conclusiones. En primer lugar, respecto a la cuestión de la aplicabilidad territorial de la normativa nacional en materia de protección de datos señaló que es “de aplicación a un proveedor de un motor de búsqueda cuando éste establece en un Estado miembro, a fines de promover y vender espacios publicitarios en su motor de búsqueda, una oficina que orienta su actividad hacia los habitantes de dicho Estado”. En cuanto a la situación jurídica de Google como proveedor de servicios de motor de búsqueda en Internet afirmó que “una autoridad nacional de protección de datos no puede requerir a un proveedor de servicios de motor de búsqueda en Internet que retire información de su índice, salvo en los supuestos en que el proveedor de servicios no ha respetado los códigos de exclusión o en los que no se ha dado cumplimiento a una solicitud emanada de la página web relativa a la actualización de la memoria oculta”. Por tanto, en su opinión, este supuesto no parece pertinente en relación con el presente asunto, ya que “la existencia de un procedimiento de detección y retirada que afecte a enlaces de las páginas web fuente con contenidos ilícitos o inapropiados es una cuestión regulada por el Derecho nacional, la responsabilidad civil basada en motivos distintos de la protección de datos personales”. Por último, la Directiva 95/46/CE “no establece ningún derecho al olvido generalizado. Por tanto, no puede invocarse tal derecho frente a

retirada de sus índices de una información publicada por terceros, sin dirigirse previa o simultáneamente al titular de la página web en la que se ubica dicha información? 4. En el caso de que la respuesta a esta última pregunta fuera afirmativa, ¿se excluiría la obligación de los buscadores de tutelar estos derechos cuando la información que contiene los datos personales se haya publicado lícitamente por terceros y se mantenga en la página web de origen?

proveedores de servicios de motor de búsqueda sobre la base de la Directiva, aun cuando ésta se interpreta con arreglo a la Carta de los Derechos Fundamentales de la Unión Europea”. En conclusión, “es posible que la responsabilidad secundaria de los proveedores de servicio de motor de búsqueda con arreglo al Derecho nacional implique la existencia de deberes que exijan bloquear el acceso a páginas web de terceros con contenidos ilegales, como las páginas web que vulneran derechos de propiedad intelectual o que muestran información injuriosa o delictiva. En cambio, solicitar a los proveedores de servicios de motor de búsqueda que eliminen información legítima y legal que se ha hecho pública traería consigo una injerencia en la libertad de expresión del editor de la página web. En su opinión, equivaldría a una censura del contenido publicado realizada por un particular”¹⁰.

1.1.2. Mario Costeja vence a Google

El TJUE, desoyendo el informe del Abogado General, expresa en su sentencia C-131/12, de 13 de mayo de 2014, que la actividad de un motor de búsqueda, en este caso Google, “consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado. Por tanto, debe calificarse de «tratamiento de datos personales», en el sentido que se recoge en el artículo 2.b)¹¹, cuando esa información contiene datos personales, y, por otro, el gestor de un motor de búsqueda debe considerarse «responsable» de dicho tratamiento, en el sentido del artículo 2.d)¹²”.

¹⁰ Conclusiones del Abogado General, Niilo Jääskinen, en el asunto C-131/12 que enfrenta a Google Spain, S.L. y Google Inc. contra la Agencia Española de Protección de Datos y Mario Costeja González , de 25 de junio de 2013.

¹¹ Directiva 95/46/CE. Artículo 2.b). Tratamiento de datos personales: “cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción”.

¹² Directiva 95/46/CE. Artículo 2.d). Responsable del tratamiento: “la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos personales; en caso de que los fines y los medios del tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable

Google justificaba su defensa en que su sede radica en un país extracomunitario (Estados Unidos), pero en este sentido, el Tribunal recalca que no se puede “discutir que Google Spain se dedica al ejercicio efectivo y real de una actividad mediante una instalación estable en España. Además, al estar dotada de personalidad jurídica propia, es de este modo una filial de Google Inc. en territorio español”¹³, y, por lo tanto, puede ser juzgada por el TJUE.

En este caso, en el que “se refiere a la presentación, en la lista de resultados que el internauta obtiene al efectuar una búsqueda a partir del nombre del interesado con ayuda de Google Search, de vínculos a dos páginas de archivos en línea de un periódico que contienen anuncios que mencionan el nombre de esta persona y relativos a una subasta inmobiliaria vinculada a un embargo por deudas a la Seguridad Social, es preciso considerar que, teniendo en cuenta el carácter sensible de la información contenida en dichos anuncios para la vida privada de esta persona y de que su publicación inicial se remonta a 16 años atrás, el interesado justifica que tiene derecho a que esta información ya no se vincule a su nombre mediante esa lista. Por tanto, en la medida en que en el caso de autos no parece existir razones concretas que justifiquen un interés preponderante del público en tener acceso a esta información en el marco de tal búsqueda, lo que no obstante incumbe comprobar al órgano jurisdiccional remitente, el interesado puede exigir que se eliminen estos vínculos de la lista de resultados” (Punto 98).

Para respetar los derechos que establecen los artículos 12.b)¹⁴ y 14.1.a)¹⁵, “siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de

del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario”.

¹³ STJUE C-131/12, de 13 de mayo de 2014. Punto 19.

¹⁴ Directiva 95/46/CE. Artículo 12.b). “Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable de tratamiento: la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos”.

¹⁵ Directiva 95/46/CE. Artículo 14.1.a). “Los Estados miembros reconocerá al interesado el derecho a: oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de

búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, también en el supuesto de que este nombre o esta información no se borren previa o simultáneamente de estas páginas web y, en su caso, aunque la publicación en dichas páginas sea en sí misma lícita”. Además, “se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado”.

La sentencia concluye que, según los derechos reconocidos en los artículos 7¹⁶ y 8¹⁷ de la Carta de los Derechos Fundamentales de la UE, “el interesado puede solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, no sería el caso si resultara, por razones concretas, como pudiese ser el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener acceso a la información de que se trate”.

Esto no supone más que un primer intento de abordar un concepto nuevo como es el derecho al olvido, aunque en ningún momento se denomina, y permite a las personas

tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos”.

¹⁶ Carta de los Derechos Fundamentales de la UE. Artículo 7. “Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones”.

¹⁷ Carta de los Derechos Fundamentales de la UE. Artículo 8. “1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente”.

solicitar directamente al motor de búsqueda¹⁸, que tendrá que estudiar cada caso, la eliminación de referencias que les afecten, aunque la información no haya sido eliminada de la web de origen. Eso sí, siempre que los datos sean irrelevantes o haya algún error en la información. El problema surge a la hora de determinar la relevancia o no de dichos datos, intentando resolverlo mediante el papel que desarrolla el interesado en la vida pública. Además, la sentencia sólo se aplicará en los países de la Unión Europea, por lo que Google no tendrá obligación de eliminar la información en las lista de búsqueda de, por ejemplo, Estados Unidos.

En nuestra opinión, la sentencia lejos de lo que vienen a pensar muchos autores no coarta la libertad de expresión, ya que el TJUE actúa directamente contra Google no contra el medio de comunicación (La Vanguardia) que es quien publicó la noticia. Por tanto, la sentencia no deja de ser más que un mero instrumento para ocultar los datos, no para borrarlos, ya que lo que se ha conseguido es que introduciendo en Google: Mario Costeja, se haya desvinculado su nombre de las informaciones de su embargo por deuda con la Seguridad Social, pero si se usan otras palabras clave, los artículos seguirán apareciendo en el buscador. Además, resulta paradójico que lo que buscaba el demandante, Mario Costeja, que era borrar su pasado, le haya puesto en un primer plano con esta sentencia y todos conozcan su nombre y la situación que con tanto ahínco trató de que se olvidase.

1.1.3. Comentarios y críticas a la sentencia

Para Pere Simón, la STJUE incorpora dos manifestaciones que no han dado lugar a la crítica. Por un lado, resulta “coherente que la empresa gestora de un motor de búsqueda quede sujeta a la normativa europea de protección de datos, ya que si no cualquier empresa que operase en Internet y tuviese su sede matriz fuera de la Unión Europea,

¹⁸ Pero en este caso concreto, como apunta AZURMENDI, la sentencia del TJUE “va un paso más allá del mero hecho de solicitar directamente al buscador la eliminación del contenido, declarando que, en el examen de proporcionalidad entre los derechos en conflicto, los derechos a la vida privada y a la protección de datos «en principio» prevalecen tanto sobre el interés económico buscado por los gestores de los motores de búsqueda, como sobre el interés del público en acceder a la información obtenida por éstos”. AZURMENDI ADARRAGA, A. (2015). Por un derecho al olvido para los europeos: aportaciones jurisprudenciales de la sentencia del Tribunal de Justicia Europeo del caso Google Spain y su recepción por la Sentencia de la Audiencia Nacional española de 29 de diciembre de 2014. *Revista de Derecho Político* nº92. UNED, págs. 303-304.

podría tratar datos para finalidades ilegítimas o ilícitas”. En segundo lugar, “la decisión de calificar la actividad de los motores de búsqueda como un tratamiento de datos”. La mayor crítica a la sentencia es “considerar al gestor del motor de búsqueda como responsable del tratamiento de datos personales al considerar que este establece los fines y los medios de esa actividad, ya que no queda del todo claro el por qué se atribuye esa responsabilidad de manera propia y autónoma a los buscadores sin tener en cuenta la eventual responsabilidad de los editores de las páginas web fuente”, destaca Simón, que no entiende como el TJUE extiende “la responsabilidad a los buscadores por los contenidos generados por terceros, cuando los primeros ni tan siquiera realizan distinciones, en su función de rastreo, conservación en indexación, entre los datos personales *strictu sensu* y las demás palabras compartidas en la red, sólo puede enmarcarse en el contexto de una decisión tomada a espaldas de su propia naturaleza”¹⁹. Lo que no le queda claro es “cómo implementarán los motores de búsqueda la obligación de proceder al borrado de las informaciones susceptibles del derecho al olvido, o cuál es el margen de interpretación del que disponen los buscadores para decidir qué información es susceptible de ser eliminada y desindexada por afectar al derecho al olvido”²⁰.

Las principales debilidades de la sentencia son, como puntualiza Rallo, “las dificultades tecnológicas para evitar el rastreo futuro de datos borrados”, debido a que, aunque el TJUE fundamenta “la eliminación de datos personales del índice de búsqueda, los *webmasters* pueden no haber eliminado en las webs de origen dichas informaciones, las arañas del buscador que periódicamente rastrean Internet podrán volver a indexar dichos datos”. Por lo tanto, la STJUE “implicaría un ejercicio periódico de borrado siempre de los mismos resultados de búsqueda si el buscador, como ha argumentado Google, no dispusiera de la tecnología necesaria para evitar el rastreo futuro de datos ya eliminados

¹⁹ SIMÓN CASTELLANO, P. (2015). *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*. Bosch, págs. 262-264. Véase también: MUÑOZ, J. (2014). El llamado «derecho al olvido» y la responsabilidad de los buscadores. Comentario a la sentencia del TJUE de 13 de mayo 2014. *Diario La Ley* nº 8.317; GRAUER RODOY, I. (2014). Bases para una jurisprudencia unificada sobre desindexación de contenidos en Internet. *Diario la Ley*, nº8374; GUERRERO ZAPLANA, J. (2014). La sentencia del asunto Google. Configuración del derecho al olvido realizada por el TJUE. *Revista Aranzadi Doctrinal* nº4, págs. 135-146; y ORDÓÑEZ SOLÍS, D. (2014). El Derecho al olvido en internet y la Sentencia Google Spain. *Unión Europea Aranzadi* nº6, págs. 27-50.

²⁰ SIMÓN CASTELLANO, P. (2015). *El reconocimiento... ob. cit.*, pág. 26.

de los índices”. Por ese motivo, habría que interpretar la sentencia en un amplio sentido y considerar “el derecho al olvido como derecho a eliminar los resultados de las búsquedas implica, también que los motores de búsqueda impidan el rastreo y futura indexación de resultados ya eliminados”²¹.

Otro factor que debe ser ponderado, en este caso, como señala Pazos es “la relevancia pública, bien de la persona sobre la que trata la información, bien de la información propiamente dicha. En la medida en que la persona tenga una exposición pública y su

²¹ RALLO LOMBARTE, A. (2014), *El derecho al olvido en Internet. Google versus España*. Centro de Estudios Políticos y Constitucionales, pág. 283. En LÓPEZ PORTAS, M^a. B. (2015), La configuración jurídica del derecho al olvido en el derecho español a tenor de la doctrina del TJUE. *Revista de Derecho Político* nº93. UNED, págs. 169-172; la autora señala que la sentencia “no crea un nuevo derecho si no que confirma las disposiciones normativas anteriores. La principal novedad que introduce la resolución judicial del tratamiento de los datos en la web”. Con la entrada en vigor del Reglamento Europeo de Protección de Datos, el TJUE “se ha visto en la necesidad de redefinir las características que identifican el ámbito jurídico relativo al derecho sobre la intimidad de usuarios de Internet. Éste es el primer asunto en el que se solicita a dicho Tribunal que interprete la Directiva de protección de datos en relación con los motores de búsqueda en Internet”. En conclusión, “el reconocimiento del derecho al olvido ha supuesto un relativo avance en la garantía de los derechos de los usuarios de Internet. Desde el punto de vista material, la información personal disponible en la web debe presentar los elementos señalados de licitud, pertinencia y actualización. En caso contrario, sólo es posible eliminar su indexación pero no borrar los datos de la fuente principal”. Para BOIX PALOP, A. (2015), El equilibrio entre los derechos del artículo 18 de la Constitución, el «Derecho al olvido» y las libertades informativas tras la sentencia Google. *Revista General de Derecho Administrativo* nº38, pág. 30; “la ponderación es el medio para resolver estos conflictos. Ponderación que, además, en primera instancia, realizará una empresa privada (Google) y que, además, realizará sin guía de ningún tipo sobre los criterios que han de ser aplicados más allá de las muy vagas consideraciones de la sentencia respecto de la necesidad de tener en cuenta el valor social de la información o datos publicados y el efecto del paso del tiempo sobre la misma. Por tanto, es el único elemento que aporta cierta seguridad tras la decisión del TJUE sobre el caso Costeja, lo que permite colegir que en todos los supuestos de hecho que se entiendan semejantes una resolución en esta misma línea es acorde a Derecho”. Al respecto, BUISÁN GARCÍA, N. (2014). El derecho al olvido: el nuevo contenido de un derecho antiguo. *El Cronista del Estado Social y Democrático de Derecho* nº46, pág. 33; señala que “es evidente que la falta de reglas plantea excesivas incertidumbres e inseguridad jurídica a todos los operadores de estos mercados, expuestos a resoluciones caso a caso que, además, plantean la duda de por qué, una vez aceptado este procedimiento ponderativo para analizar la efectiva calidad de los datos tratados en cada supuesto de hecho, a la luz de las exigencias de calidad y finalidad de la Directiva, esta revisión y ponderación habría de limitarse únicamente al efecto corrosivo de paso del tiempo sobre el interés”.

conducta entre dentro de lo que se considera de interés general, o bien los hechos relatados sean sucesos noticiables y de interés público, es más probable que prevalezca el derecho a la información sobre los derechos de la personalidad... Los motores de búsqueda no son ajenos a estas consideraciones, por lo que cuando se trate de personajes públicos o de información de interés general, es más probable que esté amparada una gran accesibilidad a la información que afecta a la intimidad o a la reputación de esa persona, a través de los buscadores generalistas”²².

El grupo *Article 29 Data Protection Working Party*²³ reconoce que “teniendo en cuenta el importante papel que los motores de búsqueda juegan en la difusión y accesibilidad

²² PAZOS CASTRO, R. (2016). El derecho al olvido frente a los editores de hemerotecas digitales. A propósito de la STS (Pleno de la Sala 1ª) de 15 de octubre de 2015. *Revista InDret* nº 4, págs. 13-14. Pazos en este artículo también aboga por cambiar el nombre a “derecho a la oscuridad digital”, ya que dicho derecho “goza también de autonomía con respecto a las acciones que puedan dirigirse contra los responsables de la página web fuente alegando la vulneración de los derechos a la intimidad y al honor. De hecho, el oscurecimiento de la información adquiere su máxima utilidad cuando la publicación de la información es lícita y no se tiene derecho a que dicha información sea eliminada... Esto es consecuencia de que el derecho a la oscuridad digital no impide que la página web en cuestión no sea indexada por el motor de búsqueda, sino simplemente que la muestre a aquellos internautas que hayan escogido como términos de búsqueda el nombre de la persona que ha ejercitado su derecho a la oscuridad digital. En definitiva, el efecto no es hacer que la persona sea olvidada, sino simplemente dificultar el acceso a la información que le concierne”, págs. 7-8. En este sentido, BERROCAL LANZAROT, A. I. (2017). *Derecho de supresión de datos o derecho al olvido*. Madrid, pág. 208; reconoce que el derecho al olvido lo que pretende es “oscurecer la información, dificultando mucho la obtención de información relevante empleando el nombre de una persona como término de búsqueda; si bien esta medida no supone la eliminación de la información contenida en la fuente original –se trata de información lícita–, ni tampoco de las réplicas que de esa publicación originaria se puedan contener en otros sitios webs”. Pero no son los únicos, GARRIGA DOMÍNGUEZ, A. (2015). *Nuevos retos para la protección de datos personales*. Dykinson. Madrid, pág. 240; lo califica como “derecho al borrado”.

²³ Este grupo se creó en virtud del artículo 29 de la directiva 95/46/CE. Se trata de un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea y sus cometidos son: a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de dicha directiva con vistas a contribuir en su aplicación homogénea; b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad Europea y en terceros países; c) asesorar a la Comisión sobre cualquier proyecto de modificación de dicha directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro

de la información publicada en Internet y las expectativas legítimas que los webmasters puedan tener con respecto a la indexación de la información en respuesta a las consultas de los usuarios, instamos encarecidamente a los motores de búsqueda a que publiquen sus propios criterios de exclusión de la lista de búsquedas”. Un primer análisis de las quejas de los interesados, tras ser rechazadas sus peticiones por los motores de búsqueda, ha permitido a las Autoridades Europeas de Protección de Datos a establecer “una lista de criterios comunes para evaluar si se ha cumplido o no la ley de protección de datos por parte de los buscadores, pudiendo así evaluar las quejas sobre una base”. Eso sí, dicha lista de criterio “debe ser vista como una herramienta de trabajo flexible que les ayudará en su proceso de toma de decisiones. Los criterios se aplicarán de conformidad con la legislación nacional pertinente. Cada criterio tiene que aplicarse a la luz de los principios establecidos por el TJUE y, en particular, a la luz del interés del público para acceder a la información”²⁴. Aquí nos encontramos con un problema de perspectiva, ya que muchos autores esperan de la STJUE algo que no se le pregunta ni es asunto suyo. La sentencia hay que analizar resolviendo aquellos aspectos que se le preguntan y no satisfaciendo las expectativas que se habían puesto en ella.

Mientras algunos autores ven en esta sentencia el comienzo de una nueva era con el reconocimiento del derecho al olvido digital, otros, como Víktor Mayer-Schönberger, señalan que “la omisión de datos no es derecho al olvido ni el fin de Google”. Los usuarios no pueden solicitar que se eliminen enlaces a Google y que estos lo hagan sin más. Lo que es necesario “es un equilibrio cuidadoso de todos los derechos involucrados, incluyendo el derecho a la información, por lo que se limita la aplicación a un pequeño número de casos”. Hoy en día, “con memoria digital, un acceso mundial a Internet y la fácil recuperación de datos a través de motores de búsqueda como Google, el pasado ha empezado a perseguirnos y todas nuestras malas acciones serán recordadas”. A lo largo de la historia, “el olvido ha sido fácil para los seres humanos, mientras que recordar era más difícil. Eso ayudó a que las personas evolucionasen, pero

proyecto de medidas comunitarias que afecte a dichos derechos y libertades; y d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.

²⁴ *Directrices para la aplicación por el Tribunal de Justicia del fallo de la UE: “Google Spain and Inc. frente a la AEPD y Mario Costeja”,* adoptadas el 26 de noviembre de 2014, págs. 10-12.

si ya no podemos olvidar, nos convertiremos en una sociedad que no puede perdonar”²⁵. Algo muy similar a lo que piensa Noval Llamas, para quien esta sentencia “no se trata de una carta blanca para reescribir la propia historia a voluntad del interesado, sino una serie de limitaciones para la perdurabilidad de esa información en internet dando lugar así a los distintos límites y facultades de este nuevo derecho”²⁶.

La STJUE plantea, como explica Martínez Otero, algunas dudas, ya que, por un lado, “resulta dudoso que un buscador sea responsable del tratamiento de datos, en la medida en que es un mero intermediario del contenido, que ni conoce ni valora. Además, en caso de ser responsable, podría acogerse a su derecho a la libertad de empresa y a sus derechos comunicativos, ya que contribuye indudablemente al acceso a la información por parte de los internautas. En este caso, en la medida en que su tratamiento sirve a intereses legítimos, no tiene porqué recabar el consentimiento del afectado. En tercer lugar, encomendarle que como sujeto privado realice la ponderación de los intereses en juego —tratándose de derechos fundamentales— resulta imponerle una potestad arbitral cuestionable, así como una carga de trabajo desproporcionada. Finalmente, también se ha planteado si la resolución del TJUE no estará abriendo la puerta a una censura

²⁵ MAYER-SCHÖNBERGER, V. (2014). *Omission of search results is not a 'right to be forgotten' or the end of Google*. Disponible en: <http://www.theguardian.com/commentisfree/2014/may/13/omission-of-search-results-no-right-to-be-forgotten>. En este sentido, PAZOS CASTRO, R. (2015). El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible? *Revista InDret* n° 1, pág. 46; considera que “la propia naturaleza de Internet, la sobrecarga de información que caracteriza a la sociedad de nuestro tiempo y la limitada capacidad de atención y memoria del ser humano hacen que cuando una persona retiene una información comprometedor para otra se deba a que su interés en ello es alto, hasta el punto de que ese interés probablemente supere el de la persona a la que se refiere la información. Si el interés de la sociedad es realmente bajo, no hace falta proclamar la prevalencia de los derechos de la persona identificada por los datos personales, ya que la propia sociedad olvidará la información con su desinterés por acceder a ella”.

²⁶ NOVAL LLAMAS, J. J. (2012). Algunas consideraciones sobre... *ob. cit.*, pág. 31. También se ha pronunciado al respecto MINERO ALEJANDRE, G. (2014). A vueltas con el “derecho al olvido”. Construcción normativa y jurisprudencia del derecho de protección de datos de carácter personal en el entorno digital. *Revista Jurídica* n°30. Universidad Autónoma de Madrid. Dykinson, págs. 129-155; y BOTANA GARCÍA, G. A., y OVEJERO PUENTE, A. Mª. (2014). Claves de la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 en la cuestión prejudicial planteada en el caso Google. *Actualidad Civil*, 9 de junio de 2014. Editorial La Ley.

privada del contenido de Internet, donde el acceso a determinadas informaciones dependerá del juicio de conveniencia realizado por un agente privado”²⁷.

Si analizamos la sentencia, lo primero con lo que nos encontramos es que realmente no hay una cancelación de la información que solicita el demandante, simplemente se desindexan en el buscador su nombre y apellidos, en este caso, sólo en Google. Por lo tanto, si se busca con otros parámetros en el mismo buscador o con el nombre y apellidos en otros buscadores, el listado de búsquedas nos llevará a la noticia del periódico. Lo que pedí el demandante que era retirar la noticia del periódico no se ha llevado a cabo al imponerse la libertad de información. La sentencia deja en el aire también varios aspectos claves. En primer lugar, definir qué es de interés público y que no para que los motores de búsqueda puedan mantenerlo indexado y, en el segundo aspecto, el tiempo que ha de pasar para que una información pierda interés. Por último, no queda claro ante quién hay que recurrir, si ante el buscador o ante un tribunal, ya que el formulario que ha creado Google es insuficiente y lo que provoca, en muchos casos, es una pérdida de tiempo para el demandante y, el tiempo, en un medio como Internet, es fundamental por la rapidez e inmediatez de la difusión de las informaciones.

²⁷ MARTÍNEZ OTERO, J. M. (2015). El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs. AEPD y Mario Costeja. *Revista de Derecho Político* nº93. UNED, pág. 138. La posibilidad como apunta VILASAU SOLANA, M. (2014), El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido (análisis de la STJUE de 13 de mayo de 2014). *Revista de Internet, Derecho y Política* nº18, págs. 30-31; “de acudir directamente al buscador en cuanto responsable del tratamiento, comporta que se abra un nuevo escenario respecto al ejercicio de los derechos del afectado y que un buscador deba llevar a cabo una ponderación en los términos marcados por la sentencia del TJUE. Por lo que es preciso que se establezcan criterios y parámetros, ya sea por las autoridades de protección de datos, ya sea por el propio legislador, para que el buscador tenga una referencia externa. Estas pautas de actuación son también indispensables para garantizar que, bajo la alegación de la protección de datos, y en algunos casos ante el temor de posibles sanciones, el acceso a la información en internet no quede lastrado”, reconociendo que “una de las principales críticas que cabe hacerle al fallo del Tribunal de Luxemburgo es que se olvida de la otra parte, de la fuente de la información. Recuérdese que, al admitir la pretensión del afectado, se está eliminando un enlace, pero no la información misma”. Véase también BROTONS MOLINA, O. (2013). Caso Google: Tratamiento de datos y derecho al olvido. Análisis de las conclusiones del abogado general, asunto C-131/12. *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº33, págs. 107-126.

1.2. EFECTOS DERIVADOS DE LA STJUE

1.2.1. Informe del Comité asesor de Google

La primera consecuencia de la sentencia del TJUE fue la creación por parte de Google de un Comité asesor de expertos sobre cómo aplicar la sentencia europea de derecho al olvido. Después de varios meses de trabajo, elaboraron un informe en el que consideran premisa fundamental que, a la hora de decidir si eliminar o no los enlaces, sea “determinante el daño potencial que le pueda causar a un sujeto el acceso a través de los buscadores a información relativa a él”. Eso sí, sosteniendo que “el derecho al olvido no debería ser interpretado como una legitimación del límite del acceso a la información”. Además, identificaron cuatro criterios básicos para evaluar las solicitudes de exclusión de los datos de la lista de búsquedas, llegando a la conclusión de que “ninguno de estos cuatro criterios es determinante por sí solo, y no hay una jerarquía estricta entre ellos. Además, los cambios sociales o técnicos pueden causar que estos criterios evolucionen con el tiempo”²⁸.

El primer paso en la evaluación de una solicitud de exclusión debe ser determinar el papel del individuo en la vida pública. En general, como se señala en el informe, los individuos se encuentran en una de las siguientes tres categorías –dichas categorías no son nuevas, ya que el TC en su sentencia 192/1999, de 25 de octubre ya las había delimitado–:

- Personas de relevancia en la vida pública (políticos, líderes religiosos, estrellas del deporte, artistas, intérpretes...). Las solicitudes de cancelación de este grupo son menos factibles y difíciles de justificar, ya que el público tendrá un gran interés primordial en buscar información sobre ellos a través de una búsqueda basada en el nombre.
- Personas sin ninguna relevancia en la vida pública. La eliminación de los datos de estos individuos de la lista de búsqueda es más sencilla de justificar.
- Y por último, las personas con un papel limitado en la vida pública (directores de escuela, empleados públicos, diferentes profesionales...). Aquí habría que valorar si el contenido específico de la información tiene más

²⁸ *Report of the Advisory Committee to Google on the Right to be Forgotten*. Disponible en: <https://drive.google.com/file/d/0B1UgZshetMd4cEI3SjlvV0hNbDA/view?pref=2&pli=1>. 6 de febrero de 2015, págs. 4-14.

valor, por su relación con el desempeño de las funciones de los individuos, que su exclusión de la lista de búsqueda.

En segundo lugar, habría que considerar la naturaleza de la información. El informe distingue entre los tipos de información que tienen un interés público (información relacionada con el discurso político, contrato ciudadano o gobernanza; discurso religioso o filosófico; con la salud pública y la protección al consumidor; actividad criminal; investigación científica y expresión artística; información que contribuye a un debate sobre un problema de interés general; información verdadera y exacta; e información del registro histórico) y los que pertenecen a la vida privada del individuo (vida sexual, información financiera, datos personales, información personal sensible, información sobre menores e información falsa o inexacta).

El tercer criterio sería la entidad de la fuente que publica la información. No es lo mismo que sea publicada por un medio de comunicación o un organismo público que por un *blogger*. Además, habría que tener en cuenta la información que es publicada por el sujeto, la cual puede quitarse con relativa facilidad directamente de la página web original, por ejemplo, suprimiendo su comentario en una red social. Y finalmente, el último criterio a valorar tendría que ver con el tiempo que hace que se publicó dicha información. En este sentido, hay tipos de información para las cuales el criterio temporal no puede ser relevante, como es el caso de los crímenes contra la humanidad.

Podemos concluir que el informe de expertos no aporta nada nuevo, ya que se basa en los intentos clásicos de la libertad de información que “aseguran a la persona diferentes modos de intervenir en el proceso para poner en circulación en él pretensiones o expectativas jurídicas o para acceder a las que circulan”²⁹. El alcance del derecho a la información debe ser desarrollado para que pueda permitir a los individuos reclamar dicho derecho.

²⁹ VILLAVARDE MENÉNDEZ, I. (2007). *Ciberconstitucionalismo*. Las TIC y los espacios virtuales de los derechos fundamentales. *Revista catalana de Dret Públic* n°35, pág. 27.

1.2.2. Un formulario para que Google te olvide

El buscador decidió poner en marcha, como consecuencia de la sentencia del TJUE, un formulario que permite a los internautas solicitar el borrado de algunos resultados de búsqueda relacionados con ellos. Google valorará cada una de las peticiones de forma individual y tratará de mantener un equilibrio entre el derecho de protección de datos y el derecho a recibir y reproducir información. Eso sí, sólo eliminará los links de sus servicios en los países de la Unión Europea, Islandia, Noruega, Liechtenstein y Suiza, no siendo aplicable al dominio www.google.com.

En el formulario, el interesado tendrá que seleccionar el país cuya legislación se aplica a su solicitud y, a partir de ahí, incluir “el nombre utilizado para realizar las búsquedas, el nombre completo del solicitante y los resultados de búsqueda que quiere que se retiren de la lista de resultados, indicando la URL de la página web”. Para cada URL, el solicitante tendrá que “explicar los motivos por los que la página se refiere a él y por qué la inclusión de esa URL en los resultados de búsqueda resulta irrelevante, obsoleta o inadecuada”³⁰.

Desde que Google pusiese en marcha el formulario de solicitud el 29 de mayo de 2014, Google ha revisado y procesado 1.255.449 URLs, de las que han retirado el 42.8% (537.121). En el caso concreto de España, han sido retiradas 40.630 URLs (38.1%) de las 106.621 peticiones³¹. La página web que más solicitudes recibe para que sus resultados sean retirados de la lista de búsqueda de Google es Facebook.

Esta medida no deja de ser un intento inicial de cumplir con la sentencia del TJUE que se queda muy lejos de lo que se pretende conseguir. En primer lugar, porque no es más que un mero formulario, sin hacer referencia al derecho de oposición o cancelación, en el que los afectados envían sus solicitudes, sin saber si van a ser borrados dichos enlaces, en caso de que se borren cuándo se va a hacer y en el caso de que sean denegados, qué criterios han seguido. Por último, el criterio para eliminar los enlaces consiste en la explicación que den los usuarios sobre por qué le pueden perjudicar

³⁰ Solicitud de retirada de resultados de búsqueda en virtud de la normativa de protección de datos europea. Disponible en: https://support.google.com/legal/contact/lr_eudpa?product=websearch.

³¹ Datos disponibles en: <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=es>.

dichos enlaces, algo muy subjetivo y que, quizá, debería ser refrendado por algún documento.

1.3. EL TJUE RECHAZA EL DERECHO AL OLVIDO DE LOS DATOS DEL REGISTRO MERCANTIL

Tras la sentencia C-131/12, de 13 de mayo de 2014, caso *Google Spain, S.L. y Google Inc. v. AEPD y Mario Costeja González*, el TJUE se ha vuelto a pronunciar sobre el derecho al olvido en la sentencia C-398/15, de 9 de marzo de 2017, caso *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*³². En esta ocasión, el TJUE considera que “no existe derecho al olvido en relación con los datos personales recogidos en el registro de sociedades”.

El Tribunal de Lecce dictó sentencia³³ y ordenó a la Cámara de Comercio de Lecce que hiciera anónimos los datos que vinculaban al Sr. Manni con el procedimiento concursal de la primera sociedad y la condenó a indemnizar el perjuicio causado. El Tribunal de Casación italiano, tras conocer el recurso interpuesto contra esta sentencia y ante las dudas sobre la interpretación de Derecho de la Unión Europea planteó al Tribunal de Justicia de la Unión Europea varias cuestiones prejudiciales, deseando saber si la Directiva relativa a la protección de los datos de las personas físicas y la Directiva sobre la publicidad de los actos de las sociedades se oponen a que cualquier persona pueda

³² En 2007, Salvatore Manni, administrador único de una sociedad a la que se adjudicó un contrato para la construcción de un complejo turístico en Italia, interpuso una demanda contra la Cámara de Comercio de Lecce. A su juicio, los inmuebles de dicho complejo no se vendían porque en el registro de sociedades constaba que había sido administrador de otra sociedad, declarada en concurso de acreedores en 1992 y liquidada en 2005.

³³ En este caso, el Tribunal de Lecce estimó que “los asientos que vinculan el nombre de una persona física a una fase crítica de la vida de la empresa (como el concurso de acreedores) no pueden ser indefinidos, a falta de un interés general específico en su conservación y divulgación”. Además, como el Código Civil no prevé la duración máxima de la inscripción, consideró que “tras un período de tiempo adecuado después de la finalización del concurso de acreedores de la empresa de que se trata y de la cancelación de sus asientos en el registro de sociedades, la necesidad y la utilidad, en el sentido del Decreto Legislativo nº196, de la indicación del nombre del antiguo administrador único de esta sociedad en el momento de su liquidación desaparece, dado que el interés público de una «memoria histórica» de la existencia de la sociedad y de las dificultades por las que pasó [puede] satisfacerse en gran medida también a través de datos anónimos”.

acceder, sin límite en el tiempo, a los datos relativos a las personas físicas que figuran en el registro de sociedades.

El Abogado General, Yves Bot, en sus conclusiones, expuso que “las cuestiones planteadas por el órgano jurisdiccional remitente están dirigidas a conciliar dos principios, a saber, por un lado, el principio de publicidad de los registros de sociedades, consagrado en la Directiva 68/151, y, por otro, el principio de conservación de los datos personales por un período no superior al necesario para la consecución de los objetivos para los cuales son tratados tales datos, establecido en la Directiva 95/46”. Con el objeto de conciliar ambos principios, “el órgano jurisdiccional remitente examina la posibilidad de limitar el principio de publicidad de los registros de sociedades permitiendo el acceso a los datos personales inscritos en los mismos únicamente durante un período limitado y/o en beneficio de un grupo restringido de personas”³⁴.

El TJUE considera que esta injerencia entre el derecho a la vida privada y el derecho a la protección de datos no es desproporcionada, ya que, por un lado, “imponen la publicidad únicamente de un número limitado de datos personales, a saber, los relativos a la identidad y las funciones respectivas de las personas que tienen poder para vincular a la sociedad de que se trate respecto de terceros y representarla en juicio o que participan en la gestión, el seguimiento o el control de esta sociedad, o han sido nombrados liquidadores”, mientras que, por otro lado, “las sociedades anónimas y las sociedades de responsabilidad limitada solo ofrecen como garantía respecto de terceros su patrimonio social, lo que implica un riesgo económico acrecentado para éstos. Habida cuenta de ello, parece justificado que las personas físicas que deciden participar en los intercambios económicos mediante una sociedad de este tipo estén obligadas a hacer públicos los datos relativos a su identidad y a sus funciones dentro de aquélla, más aún cuando son conscientes de esta obligación en el momento en que deciden involucrarse en tal actividad”³⁵.

³⁴ Apartados 35 y 36 de las conclusiones del Abogado General, de 8 de septiembre de 2016.

³⁵ Apartados 58 y 59 de las conclusiones del Abogado General, de 8 de septiembre de 2016.

Por último, la sentencia declara que, “en la ponderación que debe llevarse a cabo en el marco de esta disposición prevalece, en principio, la necesidad de proteger los intereses de terceros en relación con las sociedades anónimas y las sociedades de responsabilidad limitada y de garantizar la seguridad jurídica, la lealtad de las transacciones comerciales y, de este modo, el buen funcionamiento del mercado interior, sin embargo no es posible excluir que puedan existir situaciones particulares en las que razones preponderantes y legítimas propias de la situación concreta del interesado justifiquen excepcionalmente que el acceso a los datos personales que les conciernen, inscritos en el registro, se limite, al expirar un plazo suficientemente largo tras la liquidación de la sociedad de que se trate, a los terceros que justifiquen un interés específico en su consulta”. Además, remarca que “incumbe a los Estados miembros determinar si las personas físicas pueden solicitar a la autoridad responsable de la llevanza del registro central, del registro mercantil o del registro de sociedades, respectivamente, que compruebe, sobre la base de una apreciación caso por caso, si está excepcionalmente justificado, por razones preponderantes y legítimas relacionadas con su situación particular, limitar, al expirar un plazo suficientemente largo tras la disolución de la empresa de que se trate, el acceso a los datos personales que les conciernen, inscritos en dicho registro, a los terceros que justifiquen un interés específico en la consulta de dichos datos”³⁶. Aunque en este caso concreto, el TJUE desestimó el derecho al olvido digital y afirma que, por norma general, no existe tal derecho en el ámbito de los

³⁶ Apartados 60 y 64 de las conclusiones del Abogado General, de 8 de septiembre de 2016. Para MARTÍNEZ LÓPEZ-SÁEZ, M. (2017). Los nuevos límites al derecho al olvido en el sistema jurídico de la Unión Europea: la difícil conciliación entre las libertades económicas y la protección de datos personales. *Estudios de Deusto*. Vol. 65, nº 2, págs. 158-159; esta sentencia, a pesar de ser “correcta desde un punto de vista técnico, se puede calificar su conclusión de «lógica», ya que tanto la sentencia del Asunto *Google Spain SL* como las resoluciones de la AEPD sobre el derecho al olvido parecen dejar fuera de la supresión de datos personales (o en otras palabras, el derecho al olvido digital), aquellos relativos al ámbito profesional; aunque, a la vez, esto pueda suponer un riesgo para la dignidad y el libre desarrollo de la personalidad en algunos casos, razón por la cual es comprensible que el TJUE no haya cerrado la posibilidad de limitar otros derechos e intereses a favor del derecho al olvido digital, y no viceversa”. Aunque para la autora, en parte, esta decisión del TJUE adolece de falta de rigor, entre otras razones, por “no abordar los límites de la utilización de los datos que figuran en estos registros, sobre todo, teniendo en cuenta que la información personal, a pesar de figurar en un registro mercantil y ser sucinta, no pierde su calificación de dato de carácter personal, definido en el nuevo RGPD”.

registros de sociedades o mercantiles no cierra la puerta a que se pueda dar el derecho al olvido en algún caso concreto.

1.4. LA AUDIENCIA NACIONAL IDENTIFICA EL DERECHO AL OLVIDO

La Sección Primera de la Sala de lo Contencio-administrativo de la AN ha notificado las primeras sentencias de un tribunal español en las que se aplica la doctrina europea sobre el derecho al olvido establecida por la STJUE, de 13 de mayo de 2014. En total han sido 18 sentencias, “en 14 de las cuales se desestiman los recursos de Google, reconociendo el derecho de los particulares. En las otras cuatro resoluciones, la Audiencia Nacional estima los recursos del buscador frente a las pretensiones de los particulares”. Además de estas sentencias, “la Audiencia Nacional tiene una veintena de recursos pendientes de resolver. En todos los casos se seguirán las pautas establecidas en esta primera resolución”³⁷.

La primera de las sentencias es la que originó la cuestión prejudicial ante el Tribunal de Justicia de la UE en Luxemburgo. Esta resolución reconoce el derecho del demandante (Mario Costeja González) a que se retiren los enlaces a unos anuncios aparecidos en la web del periódico la Vanguardia, sobre unos embargos por deudas a la seguridad Social ejecutados hace 16 años. La AN considera que, en este caso, “estamos ante un tratamiento de datos inicialmente lícito por parte del buscador Google que dado el tiempo transcurrido no son necesarios en relación con los fines para los que se recogieron o trataron. Por otro lado, la libertad de información se encuentra satisfecha por su subsistencia en la fuente, es decir, en el sitio web donde se pública la información por el editor, sin que el hecho de eliminar de la lista de resultados los vínculos a las páginas web objeto de reclamación por el afectado, impida que utilizando otros datos se llegue a las citadas páginas web, pero no a partir de su nombre. En consecuencia, el demandante tiene derecho a que la información ya no esté vinculada a su nombre por una lista de resultados obtenida tras una búsqueda

³⁷ *La Audiencia Nacional establece los criterios para reconocer el “derecho al olvido”* (2015). Disponible en: <http://www.poderjudicial.es/cgpi/es/Poder-Judicial/Noticias-Judiciales/La-Audiencia-Nacional-establece-los-criterios-para-reconocer-el-derecho-al-olvido->. En este sentido, DE MIGUEL ASENSIO, P. (2012). Buscadores de Internet y protección de datos: la cuestión prejudicial de la Audiencia Nacional sobre Google. *Diario La Ley* nº7870.

efectuado a partir de sus datos personales” {SAN 5129/2014, de 29 de diciembre. Sala de lo Contencioso-administrativo (nº de recurso: 725/2010). FJ14}. En definitiva, viene a señalar el poder de disposición del particular sobre las informaciones que se publican en la red acerca de su persona.

Con anterioridad a estas sentencias, la Audiencia Provincial de Barcelona condenó a Google Spain S.L. a pagarle 8.000 euros, por vulneración de su derecho a la protección de datos personales al demandante, que exigía una indemnización por mantener indexado el contenido relativo a un indulto publicado en el año 1999 en la página web del BOE, a pesar de existir una resolución de la AEPD, solicitando a Google que eliminara ese resultado de búsqueda y, a pesar de que el BOE, había utilizado el fichero robots.txt para evitar la indexación de esa disposición de indulto por parte de los buscadores.

La sentencia establece que el “demandante no desempeña ningún papel en la vida pública que justifique una injerencia en sus derechos fundamentales. La parte demandada no ha afirmado ni acreditado lo contrario. Google Spain ha fundamentado el interés público de la publicación en la materia sobre que versa: la concesión del indulto, alegando que los artículos 2.2 y 8.1 de la LO 1/1982 excluyen expresamente la consideración de intromisión ilegítima de la publicación de información cuando dicha publicación venga impuesta por Ley del indulto {STS 6147/2010, de 17 de noviembre. Sala de lo Contencioso-administrativo (nº de recurso: 1513/2009)}³⁸. Tiene toda la razón la demandada cuando subraya la necesidad de transparencia de los indultos, teniendo en cuenta que se trata de una medida excepcional que implica una renuncia al ejercicio del poder punitivo del Estado y alcanza interés público. De ahí, la

³⁸ FJ4: “La publicación del Real Decreto de indulto por parte de la Administración en el BOE es una imposición legal de obligado cumplimiento, y que debe llevarse a cabo para hacer público el ejercicio de la gracia de indulto que concede el Gobierno, con la publicidad necesaria y la suficiente identificación de las personas a quienes se beneficia con ella. En ocasiones esa publicidad pueda llevar a la consecuencia desgraciada de que una o varias personas coincidan en nombres y apellidos con el reo indultado, y que esa circunstancia pueda trascender al conocimiento público de un modo más o menos intenso por la publicación en el BOE del Real Decreto de indulto, y por el hecho de que esos Reales Decreto aparezcan en buscadores de internet que les incluyan entre sus contenidos, y por ello resulten de fácil acceso a un importante número de personas que lo puedan conocer de ese modo ocasionalmente, constituye un daño antijurídico que el perjudicado por ese hecho está obligado a soportar”.

obligada publicación en el BOE. Ahora bien, el deber de publicación del indulto en el BOE y el acceso a la edición electrónica del BOE deben diferenciarse del acceso a la base de datos del BOE, a que se refiere el artículo 17 del Real Decreto 181/2008, de 8 de febrero³⁹. Así lo distinguió el BOE, al exponer que: la página electrónica del BOE reproducía fielmente la edición en papel, por lo que cualquier modificación sobre la página significaría una manipulación sustancial del contenido que alteraría de forma grave una fuente de acceso público; y que había adoptado las medidas a su alcance necesarias para evitar la automatización de los datos y había eliminado el nombre del actor del buscador del BOE, de manera que ya no era posible acceder a la disposición citada por el demandante, mediante su nombre, en ninguno de los buscadores de la web del BOE. Añadía que, siguiendo indicaciones de la AEPD, los documentos en que aparecía el nombre del actor habían sido incluidos en una lista de exclusión (robots.txt), para notificar a las empresas con buscadores en Internet que no debían utilizar esos datos, los cuales, en unos días, debían desaparecer de los buscadores de Internet” {SAP Barcelona 8246/2014, de 17 de julio. Sección 16 (nº de recurso: 99/2012). FJ18}.

1.5. EL TRIBUNAL SUPREMO RECONOCE LA RESPONSABILIDAD DEL EDITOR DE UNA PÁGINA WEB

El TS fija su doctrina sobre el derecho al olvido digital en su sentencia 4132/2015, de 15 de octubre, en la que establece que, “el editor de una página web en la que se incluyen datos personales realiza un tratamiento de datos personales y como tal es responsable de que dicho tratamiento de datos respete las exigencias de la normativa que lo regula, en concreto las derivadas del principio de calidad de los datos. Aunque la STJUE del caso Google analizó la responsabilidad de los gestores de motores de búsqueda en Internet (tales como Google, Yahoo, Bing...) por el tratamiento de datos personales en informaciones contenidas en páginas web cuyos vínculos aparecían en la

³⁹ Real Decreto 181/2008, de 8 de febrero, de ordenación del diario oficial Boletín Oficial del Estado. Artículo 17: “La Agencia Estatal Boletín Oficial del Estado ofrecerá en su sede electrónica, con carácter diferenciado a la edición electrónica del «Boletín Oficial del Estado», una base de datos gratuita que permita la búsqueda, recuperación e impresión de las disposiciones, actos y anuncios publicados en el «Boletín Oficial del Estado», con sujeción a lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal”.

lista de resultados de tales buscadores cuando los datos personales (en concreto el nombre y apellidos) eran utilizados como palabras clave para la búsqueda, ello no significa que los editores de las páginas web no tengan la condición de responsables del tratamiento de esos datos personales, con los consiguientes deberes de respetar el principio de calidad de datos y atender el ejercicio de los derechos que la normativa de protección de datos otorga a los afectados, y la responsabilidad derivada de no respetar estas exigencias legales. Los editores de páginas web tienen la posibilidad de indicar a los motores de búsqueda en Internet que desean que una información determinada, publicada en su sitio, sea excluida total o parcialmente de los índices automáticos de los motores, mediante el uso de protocolos de exclusión como robot.txt , o de códigos como noindex o noarchive” {STS 4132/2015, de 15 de octubre. Sala de lo Civil (nº recurso: 2772/2013). FJ5} ⁴⁰.

Al igual que se pronunció el TJUE, la sentencia reconoce que “los sucesos delictivos son noticiables por su propia naturaleza, con independencia de la condición de sujeto privado de la persona o personas afectadas por la noticia (...), pero una vez publicada en los medios de prensa por el interés que supone su carácter actual, el tratamiento automatizado de los datos personales de los implicados en ella, vinculado a la información de manera que una consulta a través de los motores de búsqueda de Internet en la que se utilice como palabras clave esos datos personales (particularmente el nombre y apellidos) arroje como resultados destacados los vínculos a las páginas de la hemeroteca digital en las que aparezca tal información, va perdiendo su justificación a medida que transcurre el tiempo si las personas concernidas carecen de relevancia pública y los hechos, vinculados a esas personas, carecen de interés histórico”. La sentencia dictaminó que El País tenía que adoptar medidas tecnológicas para que “la página web de su hemeroteca digital en la que

⁴⁰ Los hechos se remontan a los años ochenta, cuando dos personas estuvieron implicadas en el tráfico y consumo de drogas. Tras cumplir condena por estos hechos rehicieron su vida personal, familiar y profesional, pero la noticia sobre su detención, ingreso en prisión y padecimiento del síndrome de abstinencia, aparecía, utilizando como palabras clave sus nombres y apellidos, en los primeros lugares de los buscadores de Internet, pues las hemerotecas ya se encontraban digitalizadas. La empresa editora del diario (El País) y responsable de la hemeroteca no atendió la petición de los procesados de adoptar las medidas necesarias para evitar la difusión actual y permanente de la información publicada cuando sucedieron los hechos y, en consecuencia, interpusieron una demanda en protección de su honor, su intimidad y su derecho a la protección de los datos personales.

aparecía la información sobre las personas demandantes que las relacionaba con el tráfico de drogas y su dependencia de tales drogas, no pueda ser indexada por los proveedores de servicios de Internet. Tal medida es correcta puesto que supone dar satisfacción al derecho de cancelación que la normativa de protección de datos da a los afectados por un tratamiento de datos personales que no reúna los requisitos de calidad establecidos en dicha normativa, y no afecta desproporcionadamente a la libertad de información que ampara las hemerotecas digitales⁴¹ en Internet”. (FJ6 y FJ7).

Por tanto, la sentencia reconoce el derecho de protección de datos para que los responsables de las hemerotecas digitales adopten medidas para impedir que en sus páginas la información obsoleta y perjudicial pueda ser indexada por los buscadores de Internet. Lo que no establece es la eliminación de los nombres y apellidos de la información recogida en la hemeroteca, o que los datos personales contenidos en la información no puedan ser indexados por el motor de búsqueda interno de la hemeroteca. La sentencia del TS también obligará a que Google no muestre las noticias relacionadas con una determinada persona, con solo introducir su nombre y apellidos en la búsqueda, salvo por razones justificadas de relevancia pública, ya que no tiene sentido la permanencia ilimitada de la identidad de las personas afectadas y vinculadas a informaciones incorrectas y dañinas para su reputación de datos veraces pero obsoletos o ya irrelevantes.

⁴¹ COTINO HUESO, L. (2010). *Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público (Art. 3 de la LOPD)*, pág. 299; en TRONCOSO REIJADA, A., (dir.). *Comentario a la Ley Orgánica de Protección de Datos Personales*. Thomson-Civitas. Para el autor, “la hemeroteca no es un medio de comunicación en sí, sino un tratamiento a partir de tales datos que son fuentes accesibles. Por ello, la solución pasa por el ejercicio del derecho de oposición frente a quien realiza el tratamiento perjudicial al afectado, ya sea el buscador que indexa, ya sea la hemeroteca virtual. En este punto, el paso del tiempo y la situación particular del afectado podrá llevar a considerar que no se justifica el tratamiento que opera la hemeroteca, por lo que aún existiendo históricamente la noticia, ésta no tendrá porqué permanecer fácilmente accesible en su formato virtual o quedar indexada por Google, por ejemplo. Esta posición es compatible con soluciones que pasan por el principio de proporcionalidad preventivo tanto por los periodistas como por los gestores de las hemerotecas virtuales y los buscadores. Primero la valoración de la necesidad de incluir datos personales por el medio de comunicación. Segundo, la elección de sistemas que reduzcan la visibilidad de la información y su indexación más allá de lo necesario. Tercero. Mecanismos automáticos de anonimización, especialmente sobre la base del paso del tiempo”.

El magistrado no duda en afirmar que el riesgo para los derechos de la personalidad de las personas afectadas por la información guardada en la hemeroteca digital “no radica tanto en que la información sea accesible a través del motor de búsqueda interno del sitio web en que se encuentra alojada, pues se trata de una búsqueda comparable a la que efectuaban quienes acudían a las viejas hemerotecas en papel, como en la multiplicación de la publicidad que generan los motores de búsqueda de Internet, y en la posibilidad de que mediante una simple consulta utilizando los datos personales, cualquier internauta pueda obtener un perfil completo de la persona afectada en el que aparezcan informaciones obsoletas sobre hechos ya remotos en la trayectoria vital del afectado, con un grave potencial dañoso para su honor y su intimidad, que tengan un efecto distorsionador de la percepción que de esta persona tengan los demás conciudadanos y le estigmaticen. Es por eso que esa información debe resultar invisible para la audiencia general de los usuarios de los motores de búsqueda, pero no para la audiencia más activa en la búsqueda de información, que debe tener la posibilidad de acceder a las noticias en su integridad a través del sitio web de la hemeroteca digital”. Dicho esto, según la sentencia, “las hemerotecas digitales gozan de la protección de la libertad de información, al satisfacer un interés público en el acceso a la información. Por ello, las noticias pasadas no pueden ser objeto de cancelación o alteración”.

Lo novedoso de esta sentencia, es que el TS reconoce que el derecho al olvido encuentra su límite en la libertad de información⁴², “no amparando que cada uno construya un pasado a su medida, obligando a los editores de páginas web o a los gestores de los motores de búsqueda a eliminar el tratamiento de sus datos personales cuando se asocian a hechos que no se consideran positivos”. Por otro lado, “tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículum a su gusto, controlando el discurso sobre sí mismos, eliminando de Internet las

⁴² Para PAZOS CASTRO, R. (2016). El derecho al olvido frente a los editores... *ob. cit.*, pág. 16, aunque “el responsable de la hemeroteca digital sí está en disposición de borrar la página fuente al completo o una parte de la misma, así como de modificar algunos de los datos que figuren allí. Sin embargo, obligar a modificar la versión digitalizada de una información legítimamente publicada sería un gran ataque a la libertad de información, como ha declarado el Tribunal Supremo haciendo referencia al Tribunal Europeo de Derechos Humanos”. Véase también ABERASTURI GORRIÑO, U. (2016). Derecho a ser olvidado en Internet y medios de comunicación digitales. A propósito de la Sentencia del Tribunal Supremo de 15 de octubre de 2015. *Revista Española de Derecho Administrativo* n°175.

informaciones negativas, posicionando a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones”. Por tanto, el derecho al olvido digital “no puede suponer una censura retrospectiva de las informaciones correctamente publicadas en su día”.

De ahí que en el fallo se declaró “sin valor ni efecto alguno en los pronunciamientos relativos a la supresión de los datos personales de las personas demandantes en el código fuente de la página web que contenía la información y de su nombre, apellidos o incluso iniciales, y a la prohibición de indexar los datos personales para su uso por el motor de búsqueda interno de la hemeroteca digital gestionada por la demandada, pronunciamientos que dejamos sin efecto, manteniendo el resto de los pronunciamientos de la sentencia recurrida” (Sentencia AP de Barcelona 486/2013⁴³, de 11 de octubre, sección 14).

Cada vez son más los que defienden el derecho al olvido como opción para exigir a los buscadores que borren cualquier dato que pudiera identificarles en un futuro, sea negativo o no. Por dicho motivo, Salvador Coderch, no cree que “censurar retrospectivamente las hemerotecas de este país para ocultar mis yerros y gazapos sea una buena idea. No lo es, desde luego, si la información era veraz, no invadía mi privacidad y se publicó lícitamente en un diario, en un boletín oficial o en un medio de comunicación, pues todos ellos son fuentes accesibles al público, incluso según la legislación española de protección de datos personales”. Dicha censura retroactiva es “la cara oscura del pretendido derecho al olvido. Su consagración legal produciría efectos perversos e imprevistos por muchos de sus proponentes. Realimentaría nuestros prejuicios, perpetuándolos, en lugar de permitirnos encararlos y superarlos con humanidad”. Además, vincula el derecho al olvido con el derecho a la memoria histórica, afirmando que la combinación de ambos, “pondría en las manos de cada generación un arma ideológica devastadora, pues los dos derechos juntos propician

⁴³ En ella se condenó a Ediciones El País a “cesar en el uso de los datos personales en el código fuente de la página web que contenía la noticia, sin que puedan constar ni sus nombres ni apellidos ni sus iniciales, y a no mencionar los datos identificativos de las personas demandantes ni sus nombres y apellidos, ni sus iniciales, en la noticia que pudiera publicar sobre el proceso”.

olvidar al secuaz y a sus desaguisados al tiempo que fuerzan el recuerdo imperecedero del enemigo histórico y los suyos”⁴⁴.

1.5.1. Google Spain, ¿es o no responsable del derecho al olvido?

El Tribunal Supremo ha anulado, aceptando el recurso de casación que Google Spain interpuso contra la sentencia de la AN 5129/2014, de 29 de diciembre, las resoluciones de la AEPD que declaraban que Google Spain debía proceder a “adoptar las medidas necesarias para retirar los datos de su índice e imposibilitar el acceso futuro a los mismos, respecto de los siguientes enlaces” (R/02054/2014, de 22 de septiembre), dando la razón al buscador al que exonera de la corresponsabilidad en el tratamiento de datos personales sobre el derecho al olvido y obligando a los usuarios españoles a dirigir sus reclamaciones directamente a Google Inc. en Estados Unidos.

La sentencia afirma que “no cabe duda alguna de que Google Inc., que gestiona el motor de búsqueda Google Search, es responsable del tratamiento de datos, al determinar los fines, las condiciones y los medios del tratamiento de datos personales, existiendo”. Por eso, “hablar de corresponsabilidad supone un examen de la situación fáctica y comprobar que la entidad en cuestión tiene una participación concreta e identificada en la determinación de los fines y medios del tratamiento de que se trate, tratamiento que en este caso y según se declara por el TJUE al dar respuesta a la cuestión prejudicial planteada por la Sala de instancia, «consiste en hallar información publicada o puesta en Internet por terceros, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia determinado». En este caso no se identifica por la Sala de instancia ninguna actividad de Google Spain que suponga la participación en esa actividad del motor de búsqueda, además de no estar probado que realice en España una actividad directamente vinculada a la indexación o almacenamiento de información o de datos contenidos en los sitios de Internet de terceros” {STS 964/2016, de 14 de marzo. Sala de lo Contencioso-administrativo (nº recurso: 1380/2015). FJ7}.

El TS establece que “el cumplimiento de las obligaciones han de imponerse al responsable del tratamiento, que es Google Inc. y no Google Spain, a pesar de lo cual, la AEPD concluye declarando que la actuación de Google Spain, S.L. no resulta acorde a

⁴⁴ SALVADOR CODERCH, P. (2011). *Entre recordar y olvidar*. El País, pág. 29.

la normativa aplicable y que debió proceder a la exclusión de las informaciones relativas al recurrente e impedir su captación por el buscador, efectuando así un pronunciamiento respecto de una entidad que carecía de legitimación pasiva en el procedimiento y frente a la cual no tenía habilitación legal para ejercitar las facultades de control ni, en consecuencia, seguir procedimiento eficaz al respecto, lo que determina la nulidad de pleno derecho de la resolución impugnada. La apreciación de este vicio de la resolución impugnada no puede eludirse por la simple referencia a la condición de Google Spain, S.L. de representante de la compañía estadounidense, pues, en primer lugar, no se acredita en forma alguna la realidad de la misma, ni con carácter general ni específica para este procedimiento, habiéndose negado tal condición por la recurrente, y, en segundo lugar y fundamental, la intervención de un representante no altera la titularidad del derecho o condición de obligado ni traslada la responsabilidad del representado al representante” (FJ11).

Por todo ello, la sentencia decidió también estimar el recurso contencioso administrativo interpuesto por la entidad mercantil Google Spain, S.L. contra la resolución de 13 de diciembre de 2011 dictada por el Director de la Agencia Española de Protección de Datos, que se declara nula de pleno derecho por ser contraria al ordenamiento jurídico en los términos que se contienen y razonan en la sentencia del Supremo y en la que “se estimaba la reclamación del demandante contra Google Spain, S.L., instando a esta entidad, como representante en España de la compañía estadounidense del sitio web <http://www.blogspot.com>, para que adopte y realice las gestiones necesarias en orden a la exclusión de los datos personales del interesado contenidos en los blogs objeto de la presente tutela de derechos” (R/02816/2011, de 13 de diciembre. Fallo).

En conclusión, esta sentencia del Tribunal Supremo establece que las reclamaciones ya no han de hacerse a Google Spain, sino que han de dirigirse al responsable del tratamiento, en este caso Google Inc., cuya sede central se encuentra en Estados Unidos. Además, pone en entredicho las diferentes sentencias dictadas por la AN, en las que las cuales se reconocía el derecho de los particulares a que la información de la lista de resultados ya no estuviese vinculada a su nombre, obligando a Google Spain a retirarla, al establecer que “no cabe hablar de corresponsabilidad de Google Spain en el tratamiento de datos en cuestión, por cuanto no concurren en la misma los requisitos

que determinan la condición de responsable, y tampoco constituye título para ello la unidad de negocio que conforma con Google Inc. a que se refiere la sentencia de instancia. Quiere decirse con ello y en relación con el litigio que nos ocupa, que en todo caso el planteamiento de la Sala de instancia resulta injustificado, pues, de una parte, aprecia una corresponsabilidad de carácter genérico, sin precisar o identificar los concretos fines o medios del tratamiento que determina Google Spain ni cuál es el alcance de su responsabilidad y menos que forme parte de ella la obligación cuyo cumplimiento se exige por el interesado y que la AEPD declara. Muy al contrario, la propia sentencia reconoce, como hemos señalado antes, que no cabe duda alguna de que Google Inc., que gestiona el motor de búsqueda Google Search, es responsable del tratamiento de datos, al determinar los fines, las condiciones y los medios de dicho tratamiento, sin que identifique actividad concreta al efecto de Google Spain. Y por otra parte, aun apreciada por la Sala de instancia tal corresponsabilidad, en todo caso y no siendo de carácter solidaria, la obligación a que se refiere la resolución impugnada de la AEPD era exigible a Google Inc., en cuanto es el único responsable del concreto tratamiento cuestionado que se identifica por la misma, y por lo tanto necesariamente el procedimiento debía seguirse contra el mismo sin que Google Spain aparezca legitimado en tal aspecto” (FJ8 y FJ9).

Si bien la anterior sentencia daba la razón a Google Spain y no le consideraba responsable. El TS, un par de semanas después, en su sentencia 1280/2016, de 5 de abril. Sala de lo Civil (nº recurso: 3269/2014)⁴⁵, estableció que Google Spain sí es responsable, en el marco de un proceso civil de protección de derechos fundamentales,

⁴⁵ FJ1: “El BOE, de 18 de septiembre de 1999, publicó el RD de 27 de agosto de 1999 por el que se indultó al demandante la pena privativa de libertad pendiente de cumplimiento, a la que había sido condenado en sentencia de la Sala Segunda del TS, de 18 de enero de 1990. Esta sentencia resolvía el recurso de casación interpuesto contra otra de la Sección Quinta de la Audiencia Provincial de Madrid, de 26 de junio de 1986, que le condenaba como autor de un delito contra la salud pública, por hechos cometidos en el año 1981. El 8 de enero de 2009, el demandante, que se dedica profesionalmente al sector de las telecomunicaciones, informática y multimedia, se dirigió al BOE, mediante un breve mensaje de correo electrónico en el que, tras identificarse, afirmaba que desde hacía años, a través de la búsqueda en Google por su nombre y apellidos, salía una página del BOE que informaba sobre su indulto, de 1999, por un delito ocurrido en 1981. Pedía que retiraran sus datos porque habían hundido su vida y le gustaría rehacerla”.

del tratamiento de los datos personales que indexa el buscador a raíz de no retirar del buscador los datos personales sobre un antiguo indulto del demandante.

El TS fundamenta su sentencia al entender que “cobra pleno sentido que Google Inc. haya designado a Google Spain como responsable del tratamiento en España de dos ficheros inscritos por Google Inc. ante la AEPD; que cuando la AEPD ha requerido a Google Spain para que cancele el tratamiento de datos de una determinada persona, dicho tratamiento haya resultado cancelado, aunque haya sido con algunos meses de retraso; o que Google Spain haya aceptado su legitimación pasiva en anteriores litigios seguidos en relación con los efectos en España del funcionamiento del motor de búsqueda Google, porque dicho tratamiento de datos se realiza en el ámbito de actividad conjunta de la matriz y la filial española”. La sentencia señala que si bien “es cierto que Google Inc., en tanto que gestor del motor de búsqueda Google Search, es responsable del tratamiento de datos, también lo es que Google Spain puede ser considerada, en un sentido amplio, como responsable del tratamiento de datos que realiza el buscador Google Search en su versión española (www.google.es), conjuntamente con su matriz Google Inc., y, por tanto, está legitimada pasivamente para ser parte demandada en los litigios seguidos en España en que los afectados ejerciten en un proceso civil sus derechos de acceso, rectificación, cancelación y oposición, y exijan responsabilidad por la ilicitud del tratamiento de datos personales realizado por el buscador Google en su versión española” (FJ3).

La sentencia establece que “el derecho al olvido digital es una concreción de los derechos que para los afectados se derivan del principio a la calidad de los datos en la normativa sobre protección de datos de carácter personal” y añade que “la actividad de los tribunales, incluido el TJUE, es diferente a la actividad del legislador, y que sus resoluciones tienen una naturaleza distinta a la de las normas legales o reglamentarias. A diferencia del legislador, cuando un tribunal dicta una sentencia, no se plantea qué cuestiones quiere tratar para, de este modo, establecer una regulación general de las mismas que proyecte sus efectos hacia el futuro, y cuya eficacia retroactiva requiere no solo una previsión expresa sino que además está sujeta a ciertas condiciones. Los jueces y tribunales integrantes del poder judicial conocen los litigios que se les plantean, sobre hechos o situaciones ya existentes, aplican el ordenamiento jurídico vigente cuando

sucedieron los hechos relevantes, y adoptan una resolución que ha de tener eficacia respecto de esa situación preexistente” (FJ7).

El TJUE, en la sentencia del caso Google, resolvió, como apunta la STS “una cuestión prejudicial en la que un tribunal español, que debía resolver un litigio en el que aplicaba la normativa ya existente sobre protección de datos, le planteaba dudas sobre la interpretación que debía darse a la Directiva comunitaria que regulaba la materia, conforme a lo previsto en el art.267 del TFUE. El TJUE, en esta sentencia, no estableció una regulación general aplicable a partir del momento en que la dictó, sino que interpretó el Derecho de la Unión Europea que era aplicable cuando sucedieron los hechos, esto es, en un momento pasado. El derecho al olvido digital no fue, por tanto, una creación del TJUE, ni lo fueron las normas en las que este se sustenta. El TJUE declaró qué interpretación debía darse a unas normas preexistentes, y más concretamente, a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales. El derecho al olvido digital es, pues, una concreción en el ámbito de Internet de los derechos derivados de los requisitos de calidad del tratamiento de datos personales, y más concretamente de los arts. 2 , 6 , 7 , 9 , 12 y 14 de la Directiva, así como el art. 8 del CEDH y de las Libertades Fundamentales, que establece el derecho al respeto de la vida privada y familiar, convenio cuya trascendencia en el Derecho de la Unión resulta de los arts. 52 y 53 de la Carta de Derechos Fundamentales de la Unión Europea, que se encontraban en vigor cuando sucedieron los hechos que han motivado el pronunciamiento condenatorio de Google Spain que aquí se recurre” (FJ7).

En esta ocasión, el TS da la razón a la AP en lo que respecta a que Google Spain “está legitimada pasivamente para soportar la acción ejercitada por una persona afectada por el tratamiento de esos datos personales realizado por el buscador Google en defensa de sus derechos de la personalidad y de su derecho a la protección de datos personales” (FJ3). No tiene mucho sentido que el TS se pronuncie en menos de un mes de una manera tan distinta en sus sentencias. Creemos que es más correcta la segunda interpretación de considerar responsable tanto a Google Inc. como a su filial en España, Google Spain, ya que en el territorio español las búsquedas que se realizan se hacen a través de www.google.es, por lo que la responsabilidad de los resultados

encontrados en las listas de búsqueda están estrechamente relaciones con Google Spain y es más fácil que, dirigiéndose a ellos, puedan retirarse las informaciones. El único problema que podría llegar a suscitar esto es que sólo se retirasen los enlaces del dominio español y no en todo el mundo. Al respecto ya se pronunció el *Tribunal de Grande Instance* de París, en su sentencia 16 de septiembre de 2014 en la que estableció que “una filial de Google Inc. en un Estado miembro de la Comunidad Europea es su representante en el Estado del que se trate y que las actividades del operador del motor de búsqueda y las de su filial en el Estado miembro de que se trate están estrechamente vinculadas”.

1.6. LOS NOMBRES PROPIOS COMO CRITERIO DE BÚSQUEDA EN UNA HEMEROTECA DIGITAL VULNERAN EL DERECHO AL OLVIDO

El TC en su sentencia 58/2018, de 4 de junio de 2018, estimó el recurso de amparo 1086/2018⁴⁶ en el que se consideraba vulnerado sus derechos al honor, a la intimidad y a la protección de datos al aparecer sus nombres en el buscador de la hemeroteca digital del diario El País. De tal forma, consideraban también que se estaba vulnerando su derecho al olvido, recogido en el artículo 17 del Reglamento de Protección de Datos de la Unión Europea. Esta sentencia viene a ser un paso más en la lucha a favor del derecho al olvido⁴⁷, extendiendo su ámbito a las hemerotecas digitales, al prohibirse “la indexación de los datos personales de las demandantes de amparo, en lo que se refiere al

⁴⁶ El TS en su sentencia 4132/2015, de 15 de octubre, reconoció el derecho al olvido digital de las personas procesadas por implicación en un caso de tráfico y consumo de drogas en los años ochenta, pero rechazó la eliminación de los nombres y apellidos de la información recogida en la hemeroteca y que no pudiesen ser indexados por el motor de búsqueda interno de la hemeroteca al considerar que dichas medidas suponían una restricción excesiva de la libertad de información.

⁴⁷ Como señala PIÑAR MAÑAS, J. L. (2018). *El derecho al olvido y las hemerotecas digitales*. Consejo General de la Abogacía Española. Disponible en: <https://www.abogacia.es/2018/07/23/el-derecho-al-olvido-y-las-hemerotecas-digitales/>; esta sentencia plantea “una muy destacada cuestión que es la de la consideración del alcance del derecho al olvido no frente al buscador, sino frente al editor y más en particular frente a un medio de comunicación, en este caso frente a la edición digitalizada... A este respecto debe tenerse en cuenta que los motores de búsqueda internos de los sitios web cumplen la función de permitir el hallazgo y la divulgación de la noticia, y que esa función queda garantizada aunque se suprima la posibilidad de efectuar la búsqueda acudiendo al nombre y apellidos de las personas en cuestión, que no tienen relevancia pública alguna.

nombre y apellidos de las recurrentes, para su uso por el motor de búsqueda interno de la hemeroteca digital gestionada por Ediciones El País”, ya que los nombres y apellidos de las personas recurrentes “para su uso por el motor de búsqueda interno, debe ser limitado, idóneo, necesario y proporcionado al fin de evitar una difusión de la noticia lesiva de los derechos invocados”.

El TC entendió que “el derecho al olvido –recogido exactamente bajo esta denominación, sólo en el art. 17 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016⁴⁸, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de protección de datos), norma europea que entró en vigor el 25 de mayo de 2018– es una vertiente del derecho a la protección de datos personales frente al uso de la informática (art. 18.4 CE), y es también un mecanismo de garantía para la preservación de los derechos a la intimidad y al honor, con los que está íntimamente relacionado, aunque se trate de un derecho autónomo” (FJ 5).

Por tanto, como expone la sentencia, si las libertades informáticas “pueden definirse como derecho fundamental, también lo es, porque se integra entre ellas, el derecho al olvido. Esta conclusión puede extraerse sin dificultad de la configuración que hace nuestra jurisprudencia del art. 18.4 CE, al definirlo como un conjunto de derechos que el ciudadano puede ejercer «frente a quienes sean titulares, públicos o privados, de ficheros de datos personales» (STC 290/2000, FJ 7), y establecer que tales derechos son, entendidos como haz de facultades de su titular, el derecho a consentir la recogida y el uso de sus datos personales y a conocer los mismos, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, y el derecho a oponerse a esa posesión y

⁴⁸ El Reglamento, según recoge la sentencia del TC en su FJ5, viene a “legislar de forma más clara el derecho a la supresión de los datos personales de una determinada base que los contuviera. Eso, y no otra cosa, es el derecho al olvido. Un derecho a la supresión de los datos personales, existente ya por obra de la Directiva 95/46/CE, estrechamente vinculado con la salvaguardia del derecho fundamental a la protección de datos personales frente al uso de la informática (art. 18.4 CE), y con la protección del art. 8 de la Carta de los derechos fundamentales de la Unión Europea y del Convenio núm. 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal”.

uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos, esto es el derecho de supresión (en este sentido, STC 290/2000, FJ 7)”.

El TC considera que “la libertad de información⁴⁹ constituye no sólo un derecho fundamental de cada persona sino también una garantía de la formación y existencia de una opinión pública libre y plural, capaz de adoptar decisiones políticas a través del ejercicio de los derechos de participación”. Para dirimir la colisión entre el derecho a la información y los derechos de la personalidad, el TC entiende que deben ser añadidas dos variables determinantes: “el valor del paso del tiempo a la hora de calibrar el impacto de la difusión de una noticia sobre el derecho a la intimidad del titular de dicho derecho, y la importancia de la digitalización de los documentos informativos, para facilitar la democratización del acceso a la información de todos los usuarios de internet”⁵⁰ (FJ 7). Además, el TC continúa con su exposición, señalando en el mismo FJ

⁴⁹ Al respecto, en el FJ 7 se expone que “la libertad de información puede llegar a ser considerada prevalente sobre los derechos de la personalidad garantizados por el art. 18.1 CE, no con carácter absoluto sino caso por caso, en tanto la información se estime veraz y relevante para la formación de la opinión pública, sobre asuntos de interés general, y mientras su contenido se desenvuelva en el marco del interés general del asunto al que se refiere. Del mismo modo, y por la conexión que existe entre los apartados 1 y 4 del art. 18 CE, se puede decir que también el derecho a la autodeterminación de datos personales, el derecho a la supresión de esos datos de una base informatizada gestionada por un medio de comunicación, el derecho al olvido respecto de las hemerotecas en suma, puede ceder frente a la libertad de información en determinados supuestos”. En este sentido, PIÑAR MAÑAS, J. L. (2018). *El derecho al olvido... ob. citada*, señala “el derecho a la libertad de información puede convertirse con el paso del tiempo en una cuestión de formación de la cultura o actividad investigadora. Además, si se digitaliza la información, como ocurre con las hemerotecas digitales, el impacto al derecho a la intimidad y al derecho a la autodeterminación informativa es sin duda más relevante”.

⁵⁰ En primer término, según se recoge en el FJ 7, “la información transmitida debe ser veraz. El requisito de veracidad, cuya ponderación reviste especial interés cuando la libertad de información colisiona con el derecho al honor, no insta a que los hechos sean rigurosamente verdaderos, sino que se entiende cumplido en los casos en los que el informador haya realizado, con carácter previo a la difusión de la noticia, una labor de averiguación de aquéllos con la diligencia exigible a un profesional de la información (por todas, STC 129/2009, de 1 de junio, FJ 2). Así, queda protegida por el derecho fundamental incluso la noticia errónea, siempre que haya precedido dicha indagación y que el error no afecte a la esencia de lo informado. Cuando la libertad de información colisiona con el derecho a la intimidad, la veracidad «no es paliativo, sino presupuesto, en todo caso, de la lesión» (SSTC 185/2002, de 14 de octubre, FJ 4; y 127/2003, de 30 de junio, FJ 8). Ello significa que, en términos generales, si la información carece de interés público prevalente, no cabrá excluir la vulneración del derecho a la

que es “preciso reconocer que la prensa, al poner a disposición del gran público sus bases de datos de noticias, desarrolla una doble función. Por un lado, la de garante de la pluralidad informativa que sustenta la construcción de sociedades democráticas, y, por otro, la de crear archivos a partir de informaciones publicadas previamente, que resulta sumamente útil para la investigación histórica”, concluyendo que “si bien ambas desempeñan una función notable en la formación de la opinión pública libre, no merecen un nivel de protección equivalente al amparo de la protección de las libertades informativas, por cuanto una de las funciones es principal y la otra secundaria. Y estas consideraciones deben tener un efecto inmediato en el razonamiento que nos lleve a buscar el equilibrio entre los derechos reconocidos en el art. 20 d) CE y en el apartado 4 del art. 18 CE”.

El fallo concluye que “la prohibición de indexar los datos personales, en concreto los nombres y los apellidos de las personas recurrentes, para su uso por el motor de búsqueda interno de El País debe ser considerada una medida limitativa de la libertad de información idónea, necesaria y proporcionada al fin de evitar una difusión de la noticia lesiva de los derechos invocados. La medida requerida es necesaria porque su adopción, y solo ella, limitará la búsqueda y localización de la noticia en la hemeroteca digital sobre la base de datos personales inequívocamente identificativos de las personas recurrentes. A este respecto debe tenerse en cuenta que los motores de búsqueda internos de los sitios web cumplen la función de permitir el hallazgo y la divulgación de la noticia, y que esa función queda garantizada aunque se suprima la posibilidad de efectuar la búsqueda acudiendo al nombre y apellidos de las personas en cuestión, que no tienen relevancia pública alguna. Siempre será posible, si existe una finalidad investigadora en la búsqueda de información alejada del mero interés periodístico en la persona «investigada», localizar la noticia mediante una búsqueda temática, temporal, geográfica o de cualquier otro tipo” (FJ 8). En definitiva, el nombre y apellidos de los solicitantes no agregan nada de interés a la noticia y han de ser suprimidos o sustituidos por sus iniciales.

intimidad porque los hechos íntimos desvelados sean ciertos”. Por otro lado, junto a la veracidad, “la protección constitucional de la libertad de información, y su eventual prevalencia sobre los derechos de la personalidad, exige que la información se refiera a hechos con relevancia pública, en el sentido de que sean noticiables”.

1.7. LA IMPORTANCIA DE LA AEPD EN LA EVOLUCIÓN DEL DERECHO AL OLVIDO

Los ciudadanos españoles, como señala la AEPD, “han sido pioneros⁵¹ en ejercitar el denominado derecho al olvido (derechos de cancelación y oposición) para evitar la difusión universal, permanente e indiscriminada de sus datos personales en internet. En este sentido, debe subrayarse la indudable trascendencia de la sentencia del TJUE de 13 de mayo de 2014 que reconoce, como ya venía aplicando la Agencia en sus resoluciones, que los buscadores de internet realizan un tratamiento de datos del que son responsables y que las personas tienen derecho a solicitarles, con las condiciones establecidas en la Directiva de protección de datos, que los enlaces a sus datos personales no figuren en los resultados de una búsqueda en internet realizada por su nombre”⁵².

La primera vez que la AEPD se pronunció al respecto fue en 2007 y falló en contra del interesado, desestimando la reclamación contra Google España y Prisacom, S.A., al considerar que “la solicitud formulada por el reclamante ante el Diario El País, relacionada con sus datos personales recogidos en una noticia publicada en la edición digital de dicho diario, no constituye una solicitud de cancelación de sus datos personales sometidos a tratamiento en el sentido expresado y, por tanto, queda fuera del ámbito objetivo de la LOPD” (R/00692/2007, de 9 de julio. FJ8). Además, los buscadores “realizan la localización de información en Internet, en base a unos criterios que le son señalados por el usuario, buscando ocurrencias en textos o documentos publicados en la red y ofreciendo enlaces a los mismos. La información no se encuentra ubicada en los servidores o máquinas de los prestadores de los servicios de búsqueda, sino en las máquinas hacia las cuales apuntan los enlaces que ofrecen los buscadores, por lo que, la cancelación de los datos, si procede, deberá ejercitarse ante los

⁵¹ Ya en el año 2009, en su memoria anual, la AEPD recogía la preocupación de los ciudadanos en relación con el derecho al olvido, debido “al aumento de las solicitudes de cancelación de los datos o de oposición al tratamiento de los mismos por los buscadores de Internet, incrementándose en un 200%. Lo que revela que cada vez es mayor el interés mostrado por los ciudadanos para que no aparezcan sus datos personales en los índices que ofrecen los servicios de búsqueda en Internet a partir de los datos identificativos de una persona”. Memoria AEPD 2009, pág. 11.

⁵² Memoria AEPD 2014, pág. 40.

responsables de las máquinas que contienen la información. En este sentido, los prestadores de estos servicios facilitan los denominados servicios de intermediación de la Sociedad de la Información, no siendo responsables por la información a la que dirijan a los destinatarios de sus servicio” (R/00692/2007, de 9 de julio. FJ9).

Ese mismo año, la AEPD también resolvió a favor del reclamante, en este caso, obligó a Google a “adoptar las medidas necesarias para retirar los datos de su índice e imposibilitar el acceso futuro a los mismos” (R/01046/2007, de 20 de noviembre). La resolución basa su decisión en la Directiva 95/46/CE, considerando que “cuando se pudiera efectuar lícitamente un tratamiento de datos por razones de interés público o del ejercicio de la autoridad pública, o en interés legítimo de una persona física, cualquier persona deberá, sin embargo tener derecho a oponerse a que los datos que le conciernan sean objeto de un tratamiento, en virtud de motivos fundados y legítimos relativos a su situación concreta; que los Estados miembros tienen, no obstante, la posibilidad de establecer disposiciones nacionales contrarias”⁵³.

Como podemos ver, en esa primera resolución lo que la AEPD da a entender es que Google o los diferentes motores de búsqueda no son más que meros índices que dirigen a los usuarios a diferentes direcciones web en las que se recogen las informaciones. La neutralidad del servicio de búsqueda, constituye, como expone Rallo, “uno de los principales asideros sobre los que Google argumenta su falta de responsabilidad sobre el tratamiento de datos que implica la actividad del buscador. Por el contrario, la capacidad del webmaster de decidir sobre la indexación de los contenidos de su web le convertiría en responsable directo y, en consecuencia, debería garantizar el cumplimiento de la normativa de protección de datos”⁵⁴. Sin embargo, esa idea ha ido

⁵³ Directiva 95/46/CE. Considerando 45.

⁵⁴ RALLO LOMBARTE. A. (2014). *El derecho al olvido en Internet... ob. cit.*, pág. 140. En este sentido, ÁLVAREZ CARO, M. (2015). *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la red digital*. Editorial Reus, pág. 132; afirma que “la clave del éxito del nuevo derecho al olvido estará, sin duda, en el establecimiento en la práctica de unos límites y excepciones adecuados... Por tanto, los matices, las restricciones, excepciones y limitaciones son necesarias a la hora de contemplar el derecho al olvido digital, puesto que no podemos olvidarnos del gran motor que para la economía suponen las empresas digitales y sería inviable reconocer un derecho que comprometa la supervivencia de este sector económico de gran auge”.

evolucionando con el paso del tiempo hasta ser ratificada por la STJUE de mayo de 2014.

La AEPD ha basado sus decisiones en el derecho del ciudadano a ejercer el derecho de cancelación de los datos que se conservan en Internet y el derecho de oposición contra los buscadores por el tratamiento que efectúan de los datos personales. Según Simón, para “entender las razones que han llevado a la AEPD a reconocer estos dos manifestaciones concretas del derecho al olvido en Internet, resulta necesario el estudio de dos principios del tratamiento legítimo de los datos personales: consentimiento y finalidad”. El principio de consentimiento, recogido en la LOPD, puede aplicarse, a efectos del derecho al olvido, “cuando alguien presta el consentimiento o es él mismo quién publica información que contiene datos personales en la red”. En este caso, el ciudadano puede “revocar su consentimiento y exigir que aquello que antes permitió desaparezca”. También puede aplicarse cuando “el ciudadano decide oponerse a la información que contenga datos personales que hayan sido publicados por terceros sin su consentimiento, eso sí, con la excepción que tal divulgación de información se realice dentro del ejercicio de las libertades informativas”. En cuanto al principio de finalidad, “el derecho al olvido digital actuaría como un instrumento que persigue el efectivo cumplimiento de este principio, exigiendo que los datos personales sólo puedan utilizarse para la finalidad concreta para la que fueron registrados, y una vez ya no son necesarios a tal efecto se produciría su cancelación. No obstante, no en todos los casos la cancelación es posible, especialmente si los datos personales están contenidos en fuentes que tiene la consideración de accesibles al público”⁵⁵.

No sólo los buscadores han sido motivo de conflicto, los usuarios también han ejercido su derecho de reclamación frente a las redes sociales. La principal diferencia radica en que en las redes sociales son los propios usuarios los que comparten sus datos personales. En este sentido, como explica Orza y Ruíz, “nos encontramos con un principio de consentimiento otorgado expresa o tácitamente por la misma persona a la que se refieren sus datos personales”. El problema surge a la hora de la difusión de esos datos, ya que la idea original del usuario era que “sólo fueran accesibles a un círculo

⁵⁵ SIMÓN CASTELLANO, P. (2012). *El derecho al olvido en el universo 2.0*. Textos universitaris de biblioteconomia i documentació nº28. Universitat de Barcelona.

reducido de sus conocidos, han sido finalmente accesibles a todo el mundo sin restricciones, con consecuencias diversas para sus propietarios, bien por propia torpeza del usuario a la hora de configurar la privacidad de sus datos, o bien por dificultades inherente a la dinámica de la propia página de internet utilizada”⁵⁶. Lo que se pretende es una mayor agilidad por parte de las redes sociales a la hora de facilitar a los usuarios la posibilidad de borrar los datos o imágenes publicadas o, incluso, cancelar su cuenta, para que los motores de búsquedas no puedan acceder a los datos personales publicados.

Es un hecho que “los tratamientos de información personal constituyen el elemento nuclear de las redes sociales. Y ello es así tanto desde la perspectiva de los proveedores de servicios, cuyo negocio se basa precisamente en los beneficios que produce la explotación de esta información, como desde la de los usuarios, que exponen su información y se exponen con ella personal y profesionalmente”. Por ello, tanto Rallo como Martínez, consideran que “el derecho por excelencia en este contexto no podría ser otro que el derecho a la protección de datos”⁵⁷.

Al respecto, la AEPD resolvió en una de sus últimas resoluciones a favor del reclamante, obligando a “Facebook Spain para que, en el plazo de los diez días hábiles siguientes a la notificación de la presente resolución, remita al reclamante certificación en la que haga constar que ha atendido el derecho de cancelación ejercido por éste o deniegue motivadamente la cancelación solicitada, pudiendo incurrir en su defecto en una de las infracciones previstas en el artículo 44 de la LOPD. Las actuaciones realizadas como consecuencia de la presente Resolución deberán ser comunicadas a esta Agencia en idéntico plazo”. El motivo es que los datos del interesado aparecen “en un comentario publicado por una tercera persona en el muro público de la red social Facebook. En dicho comentario se utilizan los datos personales del interesado sin su consentimiento, lesionando su dignidad y honorabilidad personal y profesional” (R/03392/2015, de 15 de enero de 2016).

⁵⁶ ORZA LINARES, R. M. y RUÍZ TARRÍAS, S (2011). *El derecho al olvido en Internet*, pág. 379.; en CERRILLO-I-MARTÍNEZ, A., PEGUERA, M., PEÑA-LÓPEZ, I., y VILASAU SOLANA, M (2011). *Neutralidad de la red y otros retos para el futuro de Internet*. Huygens. Barcelona.

⁵⁷ RALLO LOMBARTE, A. y MARTÍNEZ MARTÍNEZ, R. (2011). Protección de datos personales y redes sociales: obligaciones para los medios de comunicación. *Quaderns del CAC*, volumen XIV (2), diciembre, pág. 42.

CAPÍTULO 2. EL DERECHO AL OLVIDO, UNA REALIDAD SOCIAL

¿Por qué si las acciones prescriben, no lo hacen las informaciones? Con la llegada de las nuevas tecnologías a nuestras vidas, el olvidar nuestro pasado se ha convertido en una ardua tarea, ya que siempre habrá un buscador o una red social que nos recuerde cualquier episodio de nuestra existencia. Su presencia en la sociedad actual abre una etapa en la que habrá que acometer la adaptación necesaria para dar seguridad jurídica a todo el flujo informativo que circula, sobre todo, por Internet. Pero, para llevar a cabo esta adaptación, nos encontramos con el problema de que afecta a todas las ramas del Derecho, ya que se trata de una transversalidad fáctica con repercusión legal, igualmente transversal.

La nueva Sociedad de la Información, con Internet a la cabeza, ha creado un nuevo horizonte en la concepción de la comunicación. La instantaneidad y universalidad de acceso a la información plantea otra realidad. Una realidad en la que el derecho a la información libre y la transparencia informativa están muy presentes, al menos, como aspiraciones legítimas. En otro tiempo “sólo los medios de comunicación tradicional tenían la capacidad de llegar a una gran cantidad de destinatarios y ser así generadores de opinión, en la actualidad cualquier sujeto puede hacer llegar su mensaje a millones de usuarios de Internet. Desde servicios como Blogger, Wordpress o Live Journal, hasta redes sociales masivas o plataformas colaborativas de Internet, las tecnologías de la información y la comunicación hacen que nuestra voz sea escuchada en cualquier rincón del planeta. Esto genera innumerables ventajas, pero también enormes riesgos desde el punto de vista jurídico”⁵⁸.

Contra lo que pudiese parecer, a medida que aumenta la libertad de expresión (foros, blogs), la transparencia informativa torticeramente interpretada, aunque ha adquirido un gran protagonismo teórico y doctrinal con la llegada de las nuevas tecnologías, provoca, en la práctica, que cada vez sean más los casos en los que no se respetan los derechos de las personas, ya sea desde las redes sociales u otros ámbitos, o bien desde las propias

⁵⁸ TOURIÑO, A. (2014). *El derecho al olvido... ob. cit.*, pág. 67. Ver también PLATERO ALCÓN, A. (2016). El derecho al olvido en Internet. El fenómeno de los motores de búsqueda. *Revista Opinión Jurídica*. Vol. 15, nº 29, págs. 243-260; y ÁLVAREZ CARO, M. (2015). *Derecho al olvido en Internet: el nuevo paradigma... ob. cit.*

Administraciones. Las intromisiones en la privacidad y la protección de datos hablan de los efectos más injustos de una transparencia descontrolada.

En la época de los medios de comunicación tradicionales convivíamos con un pluralismo informativo que nos permitía crearnos una idea global de la sociedad, pero la llegada de la era digital ha estrechado este pluralismo y creado una segmentación que permite a los usuarios filtrar las fuentes de información, quedándose sólo con aquellas que les interesan, reafirmando sus convicciones y provocando la pérdida del pluralismo informativo, creando el concepto de autismo informacional. Con esto, lo que se generan son situaciones de radicalización, promovidas por la red digital. Así lo corrobora Sunstein al afirmar que “la tecnología ha aumentado en gran medida la capacidad de la gente para filtrar lo que quieren leer, ver y escuchar. Periódicos y revistas de interés general son en gran parte una cosa del pasado. Con la ayuda de la televisión y de Internet, los ciudadanos son capaces de ver exactamente lo que quieren ver, ni más ni menos”. El mercado se encuentra dominado por “innumerables versiones del “*Daily Me*” (periódico a la carta) que haría reducir, y no aumentar, la libertad de elección de los individuos. Se crearía un alto grado de fragmentación social. Sin embargo, la fragmentación y la polarización del grupo, son riesgos significativos incluso si sólo una pequeña proporción decide escuchar y hablar sólo con aquellos que tienen su misma ideología. Una sociedad libre crea dominios públicos que contienen una amplia variedad de personas y posiciones”⁵⁹.

⁵⁹ SUNSTEIN, C. (2001). *Republic.com*. Princeton University Press, págs. 192-193. En McLuhan, M. (1962). *The Gutenberg Galaxy: The Making of Typographic Man*. University of Toronto Press, pág. 51; el autor señala que si “se introduce una tecnología, sea desde dentro o desde fuera, en una cultura, y da nueva importancia o ascendencia a uno u otro de nuestros sentidos, el equilibrio o proporción entre todos ellos queda alterado. Ya no sentimos del mismo modo. La interacción entre nuestros sentidos es perpetua, salvo en condiciones de anestesia... Es más sencillo decir que si una nueva tecnología extiende uno o más de nuestros sentidos fuera de nosotros en un mundo social, aparecen en esa cultura particular nuevas proporciones entre todos nuestros sentidos. Y cuando las proporciones de los sentidos cambian, en cualquier cultura, lo que ha aparecido diáfano antes puede hacerse opaco de súbito, y lo que ha sido vago u opaco, hacerse transluciente”. Una idea ya expresada por WÖLFFLIN, H. (1915). *Kunstgeschichtliche Grundbegriffe*. Traducido al español por Espasa-Calpe (2007): *Conceptos fundamentales de la Historia del Arte*, pág. 62; donde señala que lo que “importa es el efecto, no los hechos sensorios”.

Lamentablemente, en la actualidad, no existe dicho pluralismo, ya que, como señala Fiss, “los ciudadanos dependen de los medios de comunicación, incluidas las televisiones, para que les informen acerca de las posibilidades de los diversos candidatos a ocupar los cargos públicos, y para que analicen y evalúen las políticas y prácticas del gobierno. Para poder cumplir estas responsabilidades democráticas, necesitaría un cierto grado de autonomía respecto del Estado, y esta autonomía, en primer lugar, ha de ser de índole económica”. Además, añade que “la autonomía jurídica de la prensa refuerza su autonomía económica. Ambas mantienen al Estado a distancia y se nutren de las ideologías dominantes”⁶⁰.

Mientras la sociedad reclama una mayor transparencia que facilite el ejercicio de la democracia, es cierto que un volumen excesivo de información puede conseguir el efecto contrario y una saturación de datos lo que conlleva es a una opacidad que resulta contraproducente y pone en riesgo, a su vez, el derecho de las personas y su intimidad, nos encontramos ante una situación de *infoxicación*⁶¹. Una idea que ya había lanzado

⁶⁰ FISS, O. (1999). *La ironía de la libertad de expresión*. Gedisa Editorial. Barcelona, págs. 71-72. Véase también YANES MESA, R. (2007). La comunicación política y los nuevos medios de comunicación personalizada. *Revista Internacional de Comunicación* nº16, págs. 355-365; LÓPEZ GARCÍA, X. (2000). Los medios tradicionales en los nuevos escenarios de la comunicación. *Revista Latina de Comunicación Social* nº32.

⁶¹ En la obra de BORGES, J. L. (1994). *La Biblioteca de Babel, Obras completas (1923-1949)*. Emece Editores. Buenos Aires, págs. 467-468; el autor fantasea con la posibilidad de que esta biblioteca albergue todos los libros escritos en todas las lenguas, contiene, por tanto, toda la información, justificando la existencia del universo, ya que no existiría ningún secreto, todo estaría en los libros, aunque para poder leerlos todos, el lector tendría que tender a la eternidad. Lo curioso del caso llega a la hora de abarcar tal cantidad de información, es imposible acceder a ella porque uno no sabe por dónde empezar. Borges, un adelantado a su tiempo, estaba anticipándose a un fenómeno que, actualmente es ya una realidad, la infoxicación. Partiremos de la base de que con Internet, la información perdura y es de fácil acceso, por lo que cada vez hay un flujo mayor de contenidos. Por tanto, para GUTIÉRREZ MARÍN, D. (2014). *Los efectos del analfabetismo tecnológico: consecuencias en la formación universitaria*. Libro de actas Primer Congreso Internacional “Infoxicación: mercado de la información y psique”. Ladecom. Sevilla, pág. 17; “infoxicar es intoxicar mediante exceso de información, a través de un atracón de datos, fechas, números, nombres y hechos, dispuestos de una manera inconexa, que produce procesos erráticos ante la sobrecarga de estímulos y un deterioro de la capacidad individual en la toma de decisiones”. Sin embargo, para el autor “infoxicar también es reducir hasta el extremo el contacto con la realidad: si el profesor usa la tecnología para resumir los contenidos en una serie de puntos básicos a conocer, por ejemplo, está alejando al alumno de la complejidad del asunto que está tratando. Se produce un proceso de infoxicación

Bush, ya que la publicación continua de información “se ha extendido mucho más allá de nuestra capacidad actual para hacer uso de él. La suma de la experiencia humana se está expandiendo a un ritmo prodigioso y los medios que utilizamos para guiarnos a través del consiguiente laberinto hasta dar con lo momentáneamente importante son los mismos a que se recurría en los albores de la navegación a vela”⁶².

No hay que olvidar que las redes informáticas, como explica Carr, “al reducir drásticamente el costo de crear, almacenar y compartir información, han puesto a nuestro alcance mucha más información de la que jamás nos fue accesible. Y las potentes herramientas para descubrir, filtrar y distribuir información desarrolladas por empresas como Google nos garantizan que estemos siempre inundados de información de interés inmediato para nosotros, en cantidades muy por encima de lo que nuestro cerebro puede manejar... Se nos presenta mucho más de lo que resulta de interés para nosotros. La única manera de hacerle frente es aumentar nuestra capacidad de exploración y criba, confiar aún más en esas máquinas tan maravillosamente potentes que son la fuente del problema”.

Las nuevas formas de comunicación han cambiado también el paradigma clásico de la comunicación formulado por Marshall McLuhan en el que afirmaba que “el medio es el

por no estimulación, alejándolo de la realidad que le compete y basando, en adelante, sus conocimientos en una realidad contada”. Por su parte, para BREY, A. (2009). *La sociedad de la ignorancia y otros ensayos*. Infonomia. Barcelona, pág. 26; la infoxicación es “una intoxicación por exceso de información, que se traduce en una dificultad creciente para discriminar lo importante de lo superfluo y para seleccionar fuentes fiables de información. Así pues, ante la acumulación exponencial de información nos inunda progresivamente la certeza de que cada vez es más difícil disponer de una visión equilibrada del conjunto, ni que sea de baja resolución. Como reacción está surgiendo una actitud de renuncia al conocimiento por desmotivación, por rendición, y una tendencia a aceptar de forma tácita la comodidad que nos proporcionan las visiones tópicas prefabricadas”

⁶² CARR, N. (2008). *Superficiales, ¿Qué está haciendo Internet con nuestras mentes?* Editorial Taurus, pág. 208. El autor afirma que “desde la perspectiva de Google, la información es una especie de mercancía, un recurso utilitario que puede y debe ser extraído y procesado con eficiencia industrial, ya que cuanto más información se vuelva accesible y más rápidamente podamos destilar su esencia, más productivos nos volveremos como pensadores. Cualquier cosa que se interponga en el camino de la recogida rápida de datos, su disección y su transmisión es una amenaza para la nueva utopía de eficiencia cognoscitiva que Google pretende construir en Internet”.

mensaje”⁶³, ya que, como apunta Brey, “el nuevo medio, en lugar de abrirnos a un conocimiento más amplio del mundo, resulta que nos impulsa a residir en otros creados a la medida de nuestras necesidades y temores. El espacio digital formado por los ordenadores y las redes de telecomunicación se presenta ante nosotros como una atractiva experiencia sensible en la cual residimos cada vez más tiempo. Su combinación con los nuevos tipos de relaciones personales por medios telemáticos está configurando un ambiente capaz de seducir a muchas personas, especialmente a las más jóvenes, que ante el desmantelamiento de los mecanismos y los protocolos de relación tradicionales optan por instalarse en este nuevo mundo donde es posible encontrar las emociones que la realidad, mucho más mediocre, no les proporciona”⁶⁴.

⁶³ McLuhan, M. (1964). *Understanding Media: The Extensions of Man*. McGraw-Hill. New York, pág. 9; señala que “en una cultura como la nuestra, acostumbrada durante mucho tiempo a dividir y dividir todas las cosas como un medio de control, a veces es un poco chocante recordar que, en realidad, el medio es el mensaje. Esto es simplemente para decir que las consecuencias personales y sociales de cualquier medio, es decir, de cualquier extensión de nosotros mismos, resultan de la nueva escala que se introduce en nuestros asuntos por cada extensión de nosotros mismos o por cualquier nueva tecnología...La luz eléctrica es pura información. Es un medio sin mensaje, por así decirlo, a menos que se use para deletrear algún nombre. Este hecho, característico de todos los medios, significa que el contenido de cualquier medio es siempre otro medio. El contenido de la escritura es el habla, al igual que la palabra escrita es el contenido de la impresión, y la impresión es el contenido del telégrafo”. Al respecto, STRATE, L. (2012). El medio y el mensaje de McLuhan: La tecnología, extensión y amputación del ser humano. *Infoamérica: Iberoamerican Communication Review* n°7, págs. 62-67; señala que dicha afirmación “casi se podría clasificar como el primer axioma de la ecología de medios de McLuhan, si no fuera porque no constituye un postulado de lógica, sino que es fruto de la sensibilidad literaria del autor. Como tal, constituye una metáfora en la que ‘mensaje’ representa a ‘medio’, llevándonos a plantear cada medio en particular, cuál es el mensaje que transmite y qué efecto produce. También constituye un oxímoron, ya que el medio y el mensaje se suelen considerar dos elementos muy diferentes del proceso de comunicación y, en cierto sentido, antónimos (haciendo paralelas las polaridades del emisor y el receptor)”. Además, al decir que el medio es el mensaje, McLuhan “estaba resaltando que tenemos la tendencia de prestar atención al contenido y a ignorar el medio, pero es el medio el que juega un papel más significativo, el que tiene un efecto mayor”.

⁶⁴ BREY, A. (2009). *La sociedad de la ignorancia... ob. cit.*, pág. 29. BAGDIKIAN, B. (2004). *The new media monopoly*. Beacon Press Books. USA, pág. 27; reconoce que “los nuevos medios electrónicos permanecen en un equilibrio aún incierto. Hoy en día, las manifestaciones masivas que protestan contra una política del gobierno se han reunido únicamente por la organización de simpatizantes por Internet. Al mismo tiempo, la revolución digital ha hecho ambigua la privacidad dentro de la propia casa porque un funcionario del gobierno, o cualquier otra persona con suficiente habilidad, puede ingresar a la

Ante estos cambios, Orihuela, ha sistematizado en siete paradigmas los cambios que caracterizan el nuevo paisaje mediático que ha ocasionado Internet. En primer lugar, la interactividad, ya que se genera “un modelo bilateral frente a la unilateralidad de la prensa, radio y televisión, que provoca sistemas de feedback más dinámicos, inmediatos y globales”. También menciona la personalización como consecuencia de “la desmasificación de la comunicación pública mediante la personalización de los servicios de información, generando una información a la carta”; y la multimedialidad, generada por “la integración de todos los formatos de información en un mismo soporte”. En cuanto a la hipertextualidad, este nuevo paradigma discursivo “tiene la virtualidad de dotar a la escritura y a la lectura de un modelo estructural muy próximo al del pensamiento, que funciona por procesos asociativos y no de modo lineal”. Orihuela señala también la actualización, caracterizada por “la velocidad y la obsesión de inmediatez, que hace saltar por los aires los mecanismos de control, verificación y contraste de fuentes, sacrificados con aras de llegar los primeros”. Estrechamente relacionados están la abundancia, ya que “no hay límites a la cantidad de medios que pueden existir en la red ni tampoco sobre el volumen de información que cada uno de ellos puede ofrecer al usuario”, y la mediación, que permite el “acceso directo del público a las fuentes de información sin la mediación de los comunicadores profesionales; y por otra parte permite el acceso universal a un sistema mundial de publicación que funciona, igualmente, al margen de los editores de los medios tradicionales. El paradigma de la nueva mediación multiplica el número de voces, pero a la vez diluye su autoridad al haber fracturado el sistema de control editorial previo a la difusión pública de información”⁶⁵.

En el nuevo mundo, como apunta Castells, de la “autocomunicación de masas y de audiencias muy segmentadas hay pocos ejemplos de mensajes de los medios que sean de forma simultánea, sí que está extendida la cultura de compartir los mensajes procedentes de múltiples emisores-receptores. Precisamente porque el nuevo sistema de comunicación es tan versátil, diversificado y abierto, puede integrar mensajes y códigos

computadora del ciudadano desde una ubicación remota y, por lo tanto, terminar con el supuesto histórico de que «mi casa es mi castillo».

⁶⁵ ORIHUELA, J. L. (2002). Internet: nuevos paradigmas de la comunicación. *Chasqui: Revista Latinoamericana de Comunicación* n°77, págs. 10-13.

de cualquier origen, abarcando la mayor parte de la comunicación socializada en sus redes multimodales y multicanales. Por tanto, si las relaciones de poder se construyen en gran medida en la mente humana, y si la construcción de significado en la mente humana depende principalmente de los flujos de información e imágenes procesados en las redes de comunicación, parecería lógico concluir que el poder reside en las redes de comunicación y en las empresas propietarias. Esta conclusión puede ser lógica, pero es empíricamente errónea, porque si bien las redes de comunicación son los mensajeros, no son el mensaje. El medio no es el mensaje, aunque sí condiciona el formato y la distribución del mensaje. El mensaje es el mensaje, y el emisor del mensaje está en el origen de la construcción de significado. De hecho, es una de las condiciones para su construcción. La otra es la mente del receptor, ya sea individual o colectiva. Por mente colectiva entiendo el contexto cultural en el que se recibe el mensaje”⁶⁶.

Por su parte, William Mitchell expuso cómo la transformación de la tecnología inalámbrica y la creación de un mundo interconectado están cambiando nuestro entorno y nuestras vidas, ya que la comercialización de las informaciones no están ya limitadas ni geográfica ni especialmente⁶⁷. Por tanto, en la era de la información, los patrones de producción han cambiado drásticamente y “las fronteras entre la vida humana y la vida

⁶⁶ CASTELLS, M. (2009). *Comunicación y poder*. Madrid. Alianza Editorial, pág. 537. Para dicho autor, el concepto de comunicación ha cambiado, pasando de “una comunicación meramente unidireccional en la comunicación tradicional, en la que sí es verdad que se podía interactuar con los medios mediante cartas o llamadas telefónicas. Con la llegada de Internet surge una nueva forma de comunicación interactiva, caracterizada por la capacidad para enviar mensajes de muchos a muchos, en tiempo real o en un momento concreto, y con la posibilidad de usar la comunicación punto-a-punto, estando el alcance de su difusión en función de las características de la práctica comunicativa perseguida”. Esta nueva forma la denomina “autocomunicación de masas”, ya que es comunicación porque “potencialmente puede llegar a una audiencia global y, al mismo tiempo, es autocomunicación porque uno mismo genera el mensaje, define los posibles receptores y selecciona los mensajes concretos o los contenidos”.

⁶⁷ MITCHELL, W. (2003). *Me++: The Cyborg Self and the Networked City*. Cambridge. The MIT Press. La evolución tecnológica, como señala, NEUMAN, W. R. (1991). *The future of the Mass Audience*. Cambridge University Press, pág. 114; ha provocado un cambio en la audiencia que es “pasiva y activa al mismo tiempo. La mente actúa de tal forma que las informaciones, ideas e impresiones nuevas se toman, evalúan e interpretan a la luz del esquema cognitivo y de la información acumulada de la experiencia anterior... La investigación acumulada durante las últimas décadas confirma que la audiencia media presta relativamente poca atención, solo recuerda una pequeña fracción y no se siente sobrecargada en absoluto por el flujo de información o las opciones disponibles en los medios y mensajes”.

artificial se han difuminado, de modo que las redes extienden su interacción desde nuestro interior hasta todo el ámbito de la actividad humana, trascendiendo las barreras del tiempo y el espacio”⁶⁸.

Por otro lado, las nuevas tecnologías han provocado también una mayor vulnerabilidad del derecho al honor, intimidad y propia imagen. Los usuarios reproducen imágenes de terceros en las redes sociales sin su consentimiento, incurriendo en un delito o intromisión ilícita civilmente. Además, las opiniones vertidas en foros o blogs, en muchos casos, resultan ofensivas, produciéndose una violación de sus derechos. Los autores huyen de una dinámica reguladora creciente de sus derechos desde hace dos siglos⁶⁹.

2.1. CONCEPTO Y CONTEXTUALIZACIÓN DEL DERECHO AL OLVIDO

El derecho al olvido se ha convertido en un asunto de actualidad del que trataremos de dar las claves, desde un punto de vista jurídico y analizando los proyectos de ley que se están tratando de llevar a cabo para conseguir que, de una vez por todas, se regule. El primer paso ya está dado y el Parlamento Europeo, a través Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, lo ha reconocido como tal. Resultaba necesario un cambio en las normativas jurídicas, debido a que la universalidad de Internet había cambiado el concepto de libertad de expresión⁷⁰,

⁶⁸ CASTELLS, M. (2009). *Comunicación y poder ob. cit...* pág. 50.

⁶⁹ SÁNCHEZ GARCÍA, R. (2002). La propiedad intelectual en la España contemporánea, 1847-1936. *Revista Hispania LXII*, nº212, págs. 1003-1010. La primera Ley española que reconoció los derechos del autor fue la publicada el 10 de junio de 1847, Ley de Propiedad Intelectual, aunque con anterioridad, en tiempos de Carlos III, se produjo el primer reconocimiento de los derechos del autor, decretándose el carácter vitalicio de los derechos de autor y la potestad de éste de traspasar tales derechos a sus herederos. Esta Ley, que sería sustituida por la ley de 10 de enero de 1879, recogía en su artículo 1, el objeto de protección: “Se entiende por propiedad literaria para los efectos de esta ley el derecho exclusivo que compete a los autores de escritos originales para reproducirlos o autorizar su reproducción por medio de copias manuscritas, impresas, litografiadas, o por cualquiera otro semejante”.

⁷⁰ Artículo 10 CEDH. “Libertad de expresión: 1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas, sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de

haciendo desaparecer las fronteras y facilitando que los comentarios circulen libremente por cualquier rincón del mundo. La Comisión Europea había dado, en 2010, una primera definición de derecho al olvido: “el derecho de las personas a que sus datos no se traten y se supriman cuando dejan de ser necesarios con fines legítimos. Se trata, por ejemplo, del caso en que la persona retira su consentimiento al tratamiento de datos, o del caso en que haya expirado el plazo de conservación de los datos”⁷¹.

Para iniciar nuestra andadura e introducirnos en el derecho al olvido, habrá que empezar por definirlo. Lo haremos desde varias vertientes. La Real Academia Española de la Lengua recoge tres acepciones, definiéndolo como: cesación de la memoria que se tenía; cesación del afecto que se tenía; y descuido de algo que se debía tener presente. Desde la perspectiva médica, el olvido está estrechamente relacionado con la enfermedad de Alzheimer “desorden degenerativo cerebral, familiar y/o esporádico, caracterizados por el declinar progresivo de los instrumentos cognitivos, inicialmente de la memoria episódica y orientación”⁷².

Frente al envejecimiento de una sociedad que tiende a ir olvidándose de las cosas, ha surgido Internet, capaz de con un solo clic recuperar la memoria y los acontecimientos que parecían olvidados. La pregunta es evidente, ¿por qué no podemos tener una protección legal sobre aquellos datos que no se consideran de interés y que circulan sin restricciones por Internet? La velocidad vertiginosa a la que se mueven las nuevas tecnologías ha hecho que la cobertura legal, siempre por detrás, se haya quedado anclada en el pasado, obligando a buscar nuevas vías y medidas para combatir este

televisión a un régimen de autorización previa. 2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial”.

⁷¹ *Un enfoque global de la protección de los datos personales en la Unión Europea*. Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Noviembre de 2010, pág. 8.

⁷² GOBERNADO SERRANO, J. M. (2012). *Demencias*. Unidad de Demencias del Servicio de Neurología del Hospital Ramón y Cajal. Madrid, pág. 13.

nuevo problema social. En las sociedades tradicionales, antes de la existencia de Internet, los errores humanos no se registraban y los límites de la memoria de las personas aseguraban que dichos errores se olvidasen con el tiempo, pero ahora todo se registra y resulta imposible, en la mayoría de los casos, escapar de ellos.

Esta vinculación entre el derecho a la vida privada y el avance de la tecnología se puso ya de manifiesto en el artículo de los juristas norteamericanos Samuel Warren y Louis Brandeis, *The right to privacy*, en el que ya se exponía que “la vigente ley reconoce un principio para proteger la privacidad del individuo de la invasión por la prensa, los fotógrafos o los poseedores de cualquier otro dispositivo moderno para la redacción o reproducción de escenas o sonidos. Para la protección otorgada no se limita por las autoridades a los casos en que se ha adoptado cualquier medio o forma de expresión particular, sino que se amplía también a las emociones y sensaciones expresadas en una composición musical o composición literaria. Las decisiones indican un derecho general a la privacidad para los pensamientos, emociones y sensaciones, éstas deben recibir la misma protección, ya sea expresada por escrito u oralmente”⁷³. Se proponía un nuevo derecho fundado para proteger la dignidad personal como respuesta a la aparición de nuevas tecnologías, en aquella ocasión la fotografía.

Partiendo de la premisa imprescindible de conocer cuál es su definición, vamos a centrarnos ahora en el derecho al olvido. Hay autores como Rouvroy que señalan que este derecho puede “concebirse en un doble sentido: un derecho a olvidar y otro, a ser

⁷³ WARREN, S. y BRANDEIS, L. (1890). *The right to privacy*. *Harvard Law Review*. Boston. Traducido al español por Civitas (1995): *El derecho a la intimidad*. Por su parte, WESTIN, A. (1967). *Privacy and freedom*. Atheneum. New York, pág. 7; aportó una definición de la privacidad muy vinculada con el derecho al olvido actual al afirmar que “es el reclamo de individuos, grupos o instituciones para determinar por sí mismos cuándo, cómo y en qué medida la información sobre ellos se comunica a otros”. En el caso de MILLER, A. R. (1971). *The Assault on Privacy: Computers, Data Banks, and Dossiers*. University of Michigan Press, pág. 25; dicho autor señaló que “el concepto de privacidad es difícil de definir porque es exageradamente vago y evanescente, lo que a menudo significa cosas muy diferentes para diferentes personas. En parte, esto se debe a que la privacidad es una noción que es emocional en su atractivo y abarca una multitud de derechos diferentes, algunos de los cuales están interrelacionados, otros a menudo no parecen estar relacionados o son inconsistentes”.

olvidado”⁷⁴. Por su parte, Koops reconoce que “el derecho a ser olvidado utiliza la perspectiva de terceros (que deben olvidarse de su pasado), el derecho a olvidar utiliza la perspectiva en primera persona, lo que implica que es importante que sea capaz de olvidar su propio pasado. Por lo tanto, aunque puede ser concebido como un derecho legal, también puede ser visto como un valor o interés digno de protección que debe alcanzarse, ya sea por ley o por otros mecanismos de regulación”⁷⁵. En cambio, Artemi Rallo, quien fuera director de la AEPD, se muestra tajante y reconoce que “el derecho al olvido no existe, porque ninguna norma reconoce y regula el hipotético y específico derecho. Es más, no puede existir porque ni siquiera nos hallamos ante un concepto jurídico pacíficamente delimitado. Mal se puede regular, reconocer o amparar por el ordenamiento jurídico algo que no goza en la realidad social de perfiles delimitadores básicos”⁷⁶.

Podemos establecer el nacimiento del derecho al olvido como tal en el caso *Melvin v. Reid*, en Estados Unidos en el año 1919. Una prostituta es acusada de asesinato, pero, finalmente, es absuelta. Decide rehacer su vida, casándose y formando una familia, manteniendo oculto su pasado en su nueva vida. Todo cambia cuando en 1925, el

⁷⁴ ROUVROY, A. (2008). *Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?* University of Namur, Bélgica, pág. 26. También en DE BAETS, A. (2016). A historian's view on the right to be forgotten. *International Review of Law, Computers & Technology*. Vol. 30 (1-2), págs. 57-66; COOK, L. (2015). The Right to Be Forgotten: A Step in the Right Direction for Cyberspace Law and Policy. *Journal of Law, Technology & The Internet*. Vol. 6; y BROCK, G. (2016). *The Right to be Forgotten: Privacy and the Media in the Digital Age*. I.B.Tauris. London.

⁷⁵ KOOPS, B. (2008). *Forgetting Footprints, Shunning Shadows. A Critical Analysis of the “Right To Be Forgotten” in Big Data Practice*. Tilburg Law School. Países Bajos, pág. 3. Si bien es cierto que, como señala AYALA PÉREZ, T. (2016). *Memoria versus olvido: La paradoja de Internet*. UNIVERSUM. Vol. 31, n°1, pág. 43; “la memoria es parte fundamental de la esencia del hombre y base de la cultura, el olvido es importante para la vida en sociedad. Así como la memoria se cultiva y los recuerdos se preservan, también se ha fijado en el inconsciente colectivo que *forgive is forget* –olvidar es perdonar–, expresiones que demuestran que en muchos casos el olvido es una recompensa. Por este motivo, el derecho a ser olvidado se convierte, en la actualidad, en uno de los derechos más importantes, pero a la vez el más esquivo, puesto que hasta el momento no hay conciencia que la publicación de contenidos sin el consentimiento de las personas deben ser considerados como atentado a los derechos humanos. Por este motivo, si bien es cierto que es importante celebrar la memoria, en la actualidad también debiéramos celebrar el olvido”.

⁷⁶ RALLO LOMBARTE, A. (2014). *El derecho al olvido en Internet...ob. cit.*, pág. 23.

director de cine Walter Lang, decide plasmar en la película “El kimono rojo”, la historia real de Gabrielle Darley, relatando los detalles de su vida como prostituta y el juicio en el que fue absuelta. La interesada demandó a la productora y la Corte de Apelación de California, en sentencia dictada el 28 de febrero de 1931, estimó la demanda interpuesta, basándose en “el derecho a su privacidad y en el derecho a buscar y obtener la felicidad que la Constitución de California garantiza y en función del cual, entiende el Tribunal, toda persona que vive una vida de rectitud, con independencia de su pasado, tiene ese derecho a una protección frente a ataques innecesarios o agresiones injustificadas contra su libertad, su propiedad, su posición social y su reputación”⁷⁷. Según Salvador Coderch, la demandante había logrado el derecho al olvido, “lo cual no es otra cosa sino el derecho a la intimidad, que se ha visto lesionado por aquella película, ya que no afecta al derecho al honor, al ser cierto los hechos”⁷⁸.

El derecho al olvido es “la última manifestación de la necesidad de preservar la privacidad de las personas frente a las amenazas que entraña el progreso tecnológico. Los riesgos que pueden surgir de una sociedad tecnológicamente avanzada están en el origen, como reconoció tempranamente el Tribunal Constitucional, del reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio pueden realizarse sobre los espacios o ámbitos en los que las personas desarrollan su esfera personal (STC 110/1984, de 26 de noviembre)”⁷⁹. Por

⁷⁷ BENITO MARTÍN, R. (2014). *Consideraciones en torno al derecho al olvido*. Observatorio Iberoamericano de Protección de Datos. Véase también CHÉLIZ INGLÉS, M. C. (2016). El “derecho al olvido digital”. Una exigencia de las nuevas tecnologías, recogida en el futuro reglamento general de protección de datos. *Actualidad jurídica iberoamericana* nº5, págs. 255-271; CASINO RUBIO, M. (2012). El periódico de ayer, el derecho al olvido en Internet y otras noticias. *Revista española de Derecho Administrativo* nº156. Civitas, págs. 201-216, y MINERO ALEJANDRE, G. (2014). A vueltas con el “derecho al olvido”... ob. cit.

⁷⁸ SALVADOR CODERCH, P. (1987). *¿Qué es difamar? Libelo contra la Ley del Libelo*. Civitas, Madrid, pág. 97.

⁷⁹ MIERES MIERES, L. J. (2014). *El derecho al olvido... ob. cit.*, pág. 6. El autor recordaba esta sentencia que dice en su FJ3: “la exigencia de aportar las certificaciones relativas a las operaciones activas y pasivas de las cuentas abiertas en determinados establecimientos de crédito constituye una vulneración del derecho a la intimidad personal y familiar reconocido en el art. 18.1 de la Constitución. El reconocimiento explícito en un texto constitucional del derecho a la intimidad es muy reciente y se encuentra en muy pocas Constituciones, entre ellas la española (...). El avance de la tecnología actual y el desarrollo de los medios de comunicación de masas ha obligado a extender esa protección más allá del

otro lado, Esther Mitjans, quien fuera Directora de la Autoritat Catalana de Protecció de Dades, lo definió como “el derecho a que el pasado no se convierta en presente continuo”, resaltando “no sólo el valor jurídico del concepto sino también el aspecto vital de la necesidad de olvidar el pasado, si bien ello no implica la necesidad de cambiar la historia. El derecho al olvido es una cuestión global y, por tanto, se necesitan unos principios globales, dudándose todavía en su construcción doctrinal de si se trata de un derecho nuevo del usuario y de un deber de los proveedores de los contenidos a no tener nuestros datos por siempre”⁸⁰.

La AEPD fundamenta la existencia del derecho al olvido, basándose en algunos preceptos de la Directiva 95/64/CE, estableciendo que: “los Estados miembros dispondrán que los datos personales sean adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente”⁸¹ y que dichos Estados sólo “dispondrán que el tratamiento de datos personales sólo pueda efectuarse si el interesado ha dado su consentimiento de forma inequívoca”⁸². El

aseguramiento del domicilio como espacio físico en que normalmente se desenvuelve la intimidad y del respeto a la correspondencia, que es o puede ser medio de conocimiento de aspectos de la vida privada. De aquí el reconocimiento global de un derecho a la intimidad o a la vida privada que abarque las intromisiones que por cualquier medio puedan realizarse en ese ámbito reservado de vida. No siempre es fácil, sin embargo, acotar con nitidez el contenido de la intimidad. El primer problema que se plantea en el presente caso es determinar en qué medida entran dentro de la intimidad constitucionalmente protegida los datos relativos a la situación económica de una persona y a sus vicisitudes. (...). La simple existencia del sistema tributario y de la actividad inspectora y comprobatoria que requiere su efectividad lo demuestra. Es claro también que este derecho tiene un firme apoyo constitucional en el art. 31.1 de la Norma fundamental, según el cual «todos contribuirán al sostenimiento de los gastos públicos de acuerdo con su capacidad económica mediante un sistema tributario justo inspirado en los principios de igualdad y progresividad que en ningún caso tendrá carácter confiscatorio» (...). De ahí la necesidad de una actividad inspectora especialmente vigilante y eficaz aunque pueda resultar a veces incómoda y molesta y la imposición del deber jurídico de colaborar con la Administración en este aspecto fundamental del bien público, deber que recae no sólo sobre los contribuyentes directamente afectados, sino que también puede extenderse, como hace la LRF, a quienes puedan prestar una ayuda relevante en esa tarea de alcanzar la equidad fiscal, como son los Bancos y demás Entidades de crédito”.

⁸⁰ DE LA CUEVA GONZÁLEZ-COTERA, J. (2012). Relato del VII Congreso Internacional sobre Internet, Derecho y Política: Neutralidad de la red y derecho al olvido. *Revista de Internet, Derecho y Política* nº13, febrero, pág. 88.

⁸¹ Directiva 95/46/CE. Artículo 6.1.c).

⁸² Directiva 95/46/CE. Artículo 7.a).

interesado podrá solicitar el derecho de oposición a los Estados miembros en los casos: “a) contemplados en las letras e) y f) del artículo 7⁸³, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos. b) Oponerse, previa petición y sin gastos, al tratamiento de los datos de carácter personal que le conciernan respecto de los cuales el responsable prevea un tratamiento destinado a la prospección; o ser informado antes de que los datos se comuniquen por primera vez a terceros o se usen en nombre de éstos a efectos de prospección, y a que se le ofrezca expresamente, el derecho de oponerse, sin gastos, a dicha comunicación o utilización”⁸⁴. La LOPD 15/1999 también reconoce el derecho de oposición al usuario: “en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, este podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una situación concreta. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado”⁸⁵.

2.2. EL DERECHO A LA MUERTE DIGITAL

Francia se ha convertido en pionera al aprobar la Ley para una República Digital⁸⁶. La ley garantiza a los usuarios el derecho a la muerte digital estableciendo que “toda persona puede definir sus condiciones relativas a la conservación y a la comunicación de sus datos de carácter personal tras su muerte. Estas condiciones pueden ser generales o particulares. Las condiciones generales se refieren al conjunto de datos de carácter

⁸³ “El tratamiento de datos personales sólo pueda efectuarse si: e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos; f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva”.

⁸⁴ Directiva 95/46/CE. Artículo 14.

⁸⁵ LOPD 15/1999. Artículo 6.4.

⁸⁶ Aprobada en el Parlamento francés, el 26 de enero de 2016, con 365 votos a favor, uno en contra y 187 abstenciones. Como novedad, esta ley estuvo en línea durante tres semanas para que los ciudadanos pudieran hacer sus aportaciones y comentarios, siendo sometida a un proceso participativo.

personal de sus autores y pueden ser gestionadas por un tercero de confianza. En cuanto a las condiciones particulares se refieren al tratamiento de datos que los fallecidos designen”. Las condiciones establecidas definen la manera en la que la persona fallecida entiende que se ejerzan los derechos que poseen tras su muerte. Dichas condiciones, que pueden ser modificadas o revocadas en cualquier momento, cuando prevén la comunicación de datos de carácter personal relativos a terceros han de efectuarse respetando la nueva ley. Cada usuario podrá designar a la “persona encargada para su ejecución de sus datos cuando la persona haya fallecido, para tener conocimiento de las directivas y solicitar la aplicación a los responsables del tratamiento de los datos. Si no se ha designado a nadie, se seguirá el siguiente orden: descendientes, el cónyuge contra el que no exista un juicio de separación con sentencia firme o que no haya contraído un nuevo matrimonio, herederos que no sean descendientes que reúnan una parte o totalidad de la herencia y los herederos universales o donatarios del total de los bienes adquiridos”⁸⁷. Por tanto, esta ley lo que permite es que los usuarios puedan dejar en su testamento lo que quieren que se hagan con sus cuentas en las redes sociales, claves de acceso y bibliotecas digitales (música, películas y libros adquiridas por el usuario en formato digital), designando un albacea o bien a través de sus sucesores.

Las redes sociales ya ofrecen a sus usuarios, la posibilidad de que, tras su fallecimiento, un familiar pueda, aportando el certificado de defunción, darle de baja. Es el caso de Google que, como señalan desde Bórrame.es, ha puesto a disposición de los usuarios “la posibilidad de redactar nuestro testamento digital, a través de su administrador de cuentas, pudiendo decidir el destino de nuestras fotos, correos electrónicos, documentos o dato que se encuentran en los distintos servicios de Google”⁸⁸. Facebook, por su parte,

⁸⁷ Ley para una República Digital. Artículo 28.

⁸⁸ *Google activa la opción de hacer nuestro testamento digital*. Disponible en: <http://www.borrardeinternet.com/google-activa-la-opcion-de-hacer-nuestro-testamento-digital/>. Son muchos los autores que a raíz de la aparición de las nuevas tecnologías y como consecuencia de ellas, la muerte digital han abordado el tema como GOTVED, S. (2014). Research Review: Death Online - Alive and Kicking! *Thanatos*. Vol. 3; CHRISTENSEN, D. R. y SANDVIK, K. (2014). *Mediating and Remediating Death*. Ashgate; BRUBAKER, J. R., HAYES, G. R. Y DOURISH, P. (2013). Beyond the Grave: Facebook as a Site for the Expansion of Death and Mourning. *The Information Society*. Vol. 29, nº3, págs. 152-163; PENNINGTON, N. (2013). You don't De-friend the Dead: An Analysis of Grief Communication by College Students Through Facebook Profiles. *Death Studies*. Vol. 37, nº7, págs. 617-635; FORMAN, A. E., KERN, R. y GIL-EGUI, G. (2012). Death and Mourning as Sources of

va un paso más allá y permite, además de eliminar la cuenta de una persona fallecida, crear una cuenta conmemorativa, proporcionando un lugar para que amigos y familiares se reúnan y compartan recuerdos de un ser querido fallecido.

La ley francesa también regula el derecho al olvido para los menores de edad en Internet, reconociendo que: “a petición de la persona interesada, el responsable del tratamiento deberá borrar en el menor tiempo posible los datos de carácter personal que ha sido recogidos en el marco de la oferta de servicios de la sociedad de la información cuando la persona interesada fuese menor en el momento de la recogida de dicha información. En caso de no ejecución del borrado de los datos personales o de ausencia de respuesta del responsable de tratamiento en un plazo de un mes tras la petición, la persona interesada puede solicitar que la CNIL se pronuncie en un plazo de 15 días a contar desde la fecha de recepción de la reclamación”. Las disposiciones anteriores no se aplicarán cuando el tratamiento de datos de carácter personal sea necesario: “para ejercer el derecho a la libertad de expresión y de información; cumplir una obligación legal que requiera el tratamiento de los datos o ejercer una misión de interés público o relevante en el ejercicio del poder público que se le ha conferido al responsable del tratamiento; por motivos de interés público en el ámbito de la Sanidad Pública; con la finalidad de almacenaje para el interés público o con fines científicos estadísticos e históricos; y en el ejercicio o defensa de los derechos legales”⁸⁹. Con este artículo, lo que se pretende es que los menores de edad, que no son conscientes a esas edades de los riesgos que suponen las redes sociales, puedan enmendar los errores del pasado y borrar aquellas fotos o informaciones que puedan suponer un riesgo a la hora de afrontar su futuro personal o laboral.

Por otro lado, aunque la muerte del sujeto de derecho extingue los derechos de la personalidad (art. 32 CC), hay que tener en cuenta que “el ejercicio de las acciones de protección civil del honor, la intimidad o la imagen de una persona fallecida corresponde a quien ésta haya designado a tal efecto en su testamento. La designación puede recaer en una persona jurídica” (art. 4.1 LO 1/1982, de 5 de mayo). En el caso de

Community Participation in Online Social Networks: R.I.P. Pages in Facebook. *First Monday*. Vol. 17, nº9; y STOKES, P. (2011). Ghosts in the Machine: Do the Dead Live on in Facebook? *Philosophy & Technology*. Vol. 25, nº3, págs. 363-379.

⁸⁹ Ley para una República Digital. Artículo 27.

que no existiese designación, “se encontrarán legitimados para el ejercicio de estas acciones, el cónyuge, los descendientes, ascendientes y hermanos de la persona afectada que viviesen al tiempo de su fallecimiento” (art. 4.2). A falta de todos ellos, “el ejercicio de las acciones de protección corresponderá al Ministerio Fiscal, que podrá actuar de oficio o a instancia de la persona interesada, siempre que no hayan transcurrido más de ochenta años desde el fallecimiento del afectado. El mismo plazo se observará cuando el ejercicio de las acciones mencionadas corresponda a una persona jurídica designada en testamento” (art. 4.3).

El TC entendió en su sentencia 231/1988, de 2 de diciembre⁹⁰, que “no puede pronunciarse sobre aquellas cuestiones que, por el fallecimiento del afectado, carecen ya de dimensión constitucional; concretamente, y en el presente caso, sobre la explotación comercial de la imagen de don Francisco Rivera en el ejercicio de su actividad profesional. En este aspecto, el derecho a la imagen» que se invoca es, en realidad, el derecho a disponer de la imagen de una persona desaparecida y de su eventual explotación económica, protegible, según la Ley 1/1982 en vías civiles, y susceptible de poseer un contenido patrimonial, pero derecho que no puede ser objeto de tutela en vía de amparo, ya que, una vez fallecido el titular de ese bien de la personalidad, no existe ya un ámbito vital que proteger en cuanto verdadero objeto del derecho fundamental aun cuando pudieran pervivir sus efectos patrimoniales” (FJ3). Aun así, el TC reconoce que “debe estimarse el derecho a la intimidad personal y familiar se extiende, no sólo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar; aspectos que, por la relación o vínculo existente con ellas, inciden en la propia esfera de la personalidad del individuo que los derechos del art. 18 de la C.E. protegen. Sin duda, será necesario, en cada caso,

⁹⁰ Isabel Pantoja Martín interpuso una demanda de protección civil del derecho a la intimidad y a la propia imagen (al amparo de lo prevenido en la Ley Orgánica 1/1982 que desarrolla el art. 18.1 de la CE) ante el Juzgado de Primera Instancia núm. 14 de los de Madrid y contra la entidad mercantil Prographic, S.A., que había realizado y, posteriormente comercializado, sin autorización alguna, unas cintas de vídeo en las que se mostraban imágenes de la vida privada y profesional de su difunto marido, D. Francisco Rivera Pérez, de profesión torero y conocido públicamente como “Paquirri”, y muy especialmente, imágenes de la mortal cogida que sufrió en la plaza de toros de Pozoblanco y de su posterior tratamiento médico en la enfermería de la citada plaza.

examinar de qué acontecimientos se trata, y cuál es el vínculo que une a las personas en cuestión; pero al menos, no cabe dudar que ciertos eventos que puedan ocurrir a padres, cónyuges o hijos tienen, normalmente, y dentro de las pautas culturales de nuestra sociedad, tal trascendencia para el individuo, que su indebida publicidad o difusión incide directamente en la propia esfera de su personalidad. Por lo que existe al respecto un derecho a la intimidad, constitucionalmente protegible” (FJ4).

El TC falló a favor de la demandante reconociéndole el derecho a su intimidad personal y familiar. Los magistrados Fernando García-Mon y González-Regueral y Carlos de la Vega Benayas dictaron un voto particular a la STC 231/1988 consideran que “la información del suceso tal y como fue difundida por TVE, primero como noticia en los telediarios y, días después, en el programa Informe Semanal, no entraña infracción alguna del art. 18.1 de la CE, ni de la protección que a ese derecho otorga el art. 20.4. CE. La profesión de la víctima, el riesgo inherente a su ejercicio y el carácter público del espectáculo, legitiman dicha información”. Además, añaden que “no cabe olvidar que si la primera información visual de la noticia y su posterior difusión en un reportaje emitido por televisión, no mereció de la actual recurrente reacción alguna en defensa de sus derechos, sin duda por entender que la importancia de la noticia trascendía de su propia intimidad, no parece coherente que ahora, con su recurso, pueda valorar los mismos hechos ya divulgados como una intromisión ilegítima en su derecho constitucional a la intimidad. No queremos decir con ello que su reclamación sobre la comercialización del vídeo realizada sin su consentimiento por la sociedad demandada en el proceso del que trae causa este recurso, fuera improcedente, sino que sobre ese derecho de naturaleza privada y de contenido patrimonial, por no tener la dimensión constitucional con que ahora se plantea, no puede pronunciarse este Tribunal” (Voto particular).

El TS también se pronunció al respecto en su sentencia 1588/1988⁹¹, de 7 de marzo. Sala de lo Civil, señalando que las informaciones publicadas por El País y Diario 16,

⁹¹ Los periódicos El País y Diario 16 publicaron información sobre un accidente aéreo ocurrido el 19 de febrero de 1985 en las proximidades del aeropuerto de Sondica (Bilbao), que ocasionó el fallecimiento de 148 personas y, entre ellas, el del comandante de vuelo del avión siniestrado, don José Luis Patiño Arróspide. Dichas informaciones motivaron la interposición, por los hijos del piloto, de una demanda

“inmediatamente después de producirse la catástrofe aérea y estando abiertas unas diligencias penales y una investigación técnica para determinar sus causas, conducen subliminalmente a los lectores del periódico, mediante una especie de juicio paralelo, a la conclusión de que el accidente se debió a una patente irresponsabilidad del comandante del avión siniestrado, que pilotaba la aeronave en condiciones anímicas y profesionales incompatibles con la delicadeza de la función correspondiente, lo que configura por sí solo una intromisión ilegítima en el ámbito del honor y de la intimidad personal de dicho piloto, titular del derecho lesionado y cuya memoria constituye una prolongación de su personalidad” (FJ2). Posteriormente, el TC en su sentencia 172/1990, de 12 de noviembre, denegó el amparo solicitado por los medios de comunicación.

2.3. NUEVO REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

El Parlamento Europeo aprobó el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos⁹². La reforma pretende devolver a los ciudadanos el control de sus datos personales y garantizar en toda la UE unos estándares de protección elevados y adaptados al entorno digital. Dicha aprobación reforma la directiva 95/64/CE, aplicándose ya desde abril de 2018.

Viendo la relevancia social del derecho al olvido, el Reglamento lo recoge en su artículo 17: *Derecho al olvido y a la supresión*⁹³. El objetivo es que cualquier persona pueda

civil de protección de los derechos al honor, a la intimidad personal y la propia imagen de su padre dirigidas, una, contra el Director y Editor de El País, y otra, contra el Director y Editores de Diario 16.

⁹² El Reglamento había sido propuesto por la Comisión Europea en enero de 2012 y aprobado, inicialmente, por la Eurocámara el 12 de marzo de 2014 por 621 votos a favor, 10 en contra y 22 abstenciones.

⁹³ Artículo 17: 1.El interesado tendrá derecho a que el responsable del tratamiento suprima los datos personales que le conciernen y se abstenga de darles más difusión, especialmente en lo que respecta a los datos personales proporcionados por el interesado siendo niño, cuando concurra alguna de las circunstancias siguientes: a) los datos ya no son necesarios en relación con los fines para los que fueron recogidos o tratados; b) el interesado retira el consentimiento en que se basa el tratamiento de conformidad con lo dispuesto en el artículo 6, apartado 1, letra a), o ha expirado el plazo de conservación

solicitar que se borren sus datos si no se cumplen las normas de la UE, los datos ya no

autorizado y no existe otro fundamento jurídico para el tratamiento de los datos; c) el interesado se opone al tratamiento de datos personales con arreglo a lo dispuesto en el artículo 19; d) el tratamiento de datos no es conforme con el presente Reglamento por otros motivos. 2. Cuando el responsable del tratamiento contemplado en el apartado 1 haya hecho públicos los datos personales, adoptará todas las medidas razonables, incluidas medidas técnicas, en lo que respecta a los datos de cuya publicación sea responsable, con miras a informar a los terceros que estén tratando dichos datos de que un interesado les solicita que supriman cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos. Cuando el responsable del tratamiento haya autorizado a un tercero a publicar datos personales, será considerado responsable de esa publicación. 3. El responsable del tratamiento procederá a la supresión sin demora, salvo en la medida en que la conservación de los datos personales sea necesaria: a) para el ejercicio del derecho a la libertad de expresión de conformidad con lo dispuesto en el artículo 80; b) por motivos de interés público en el ámbito de la salud pública de conformidad con lo dispuesto en el artículo 81; c) con fines de investigación histórica, estadística y científica de conformidad con lo dispuesto en el artículo 83; d) para el cumplimiento de una obligación legal de conservar los datos personales impuesta por el Derecho de la Unión o por la legislación de un Estado miembro a la que esté sujeto el responsable del tratamiento; las legislaciones de los Estados miembros deberán perseguir un objetivo de interés público, respetar la esencia del derecho a la protección de datos personales y ser proporcionales a la finalidad legítima perseguida; e) en los casos contemplados en el apartado 4. 4. En lugar de proceder a la supresión, el responsable del tratamiento limitará el tratamiento de datos personales cuando: a) el interesado impugne su exactitud, durante un plazo que permita al responsable del tratamiento verificar la exactitud de los datos; b) el responsable del tratamiento ya no necesite los datos personales para la realización de su misión, pero estos deban conservarse a efectos probatorios; c) el tratamiento sea ilícito y el interesado se oponga a su supresión y solicite en su lugar la limitación de su uso; d) el interesado solicite la transmisión de los datos personales a otro sistema de tratamiento automatizado de conformidad con lo dispuesto en el artículo 18, apartado 2. 5. Con excepción de su conservación, los datos personales contemplados en el apartado 4 solo podrán ser objeto de tratamiento a efectos probatorios, o con el consentimiento del interesado, o con miras a la protección de los derechos de otra persona física o jurídica o en pos de un objetivo de interés público. 6. Cuando el tratamiento de datos personales esté limitado de conformidad con lo dispuesto en el apartado 4, el responsable del tratamiento informará al interesado antes de levantar la limitación al tratamiento. 7. El responsable del tratamiento implementará mecanismos para garantizar que se respetan los plazos fijados para la supresión de datos personales y/o para el examen periódico de la necesidad de conservar los datos. 8. Cuando se hayan suprimido datos, el responsable del tratamiento no someterá dichos datos personales a ninguna otra forma de tratamiento. 9. La Comisión estará facultada para adoptar actos delegados, de conformidad con lo dispuesto en el artículo 86, a fin de especificar: a) los criterios y requisitos relativos a la aplicación del apartado 1 en sectores y situaciones específicos de tratamiento de datos; b) las condiciones para la supresión de enlaces, copias o réplicas de datos personales procedentes de servicios de comunicación accesibles al público a que se refiere el apartado 2; c) los criterios y condiciones para limitar el tratamiento de datos personales contemplados en el apartado 4.

son necesarios, o la persona no da su consentimiento o lo retira para el almacenamiento de esa información. Se trataría, por tanto, de un derecho a la supresión más que un derecho al olvido como tal, que quedará limitada cuando dichos datos, como establece el artículo 17.3, se hayan recabado con fines estadísticos, para la investigación histórica o científica, por motivos de salud pública, o para ejercer la libertad de expresión.

Lo que ha conseguido Internet, además de la globalización de los contenidos, es crear un mundo paralelo en el que existen un sinnúmero de entresijos que dificultan acceder al origen de algunos servidores, que tienen su ubicación en países con una legislación muy laxa, lo que generara un criterio interpretativo diferente del que se pudiese producir ante la misma circunstancia en otra ubicación. Es el problema con el que se encuentra la legislación europea al tratar de aplicar el derecho al olvido en buscadores como Google, que tienen su sede en Estados Unidos, y que se niegan a adoptar las medidas a todos sus dominios, sólo lo hacen en aquellos en los que el país tiene una legislación al respecto (España, Francia, Italia...). Por tanto, se trata de crear una legislación global transfronteriza, más rígida y ágil, que permita controlar este tipo de situaciones. Y sí, hablamos de rapidez, ya que una de las ventajas de Internet es que los datos se desplazan a gran velocidad, por lo tanto, si el perjudicado se dilata en procesos largos, la repercusión de la información, aunque luego pueda ser, finalmente, retirada, puede dejar secuelas en la vida privada de la persona afectada y dañar su honor y su imagen. Este es un panorama difícil de crear, debido al diferente enfoque que, como señalaba, aplica cada circunscripción.

Al respecto, Rallo reconoce que “uno de los retos actuales es dotar a los ciudadanos de mecanismos reales y efectivos para garantizar el olvido, entendiendo que ningún ciudadano que no sea objeto de un hecho noticiable de relevancia pública tiene que resignarse a que sus datos se difundan en Internet sin poder reaccionar ni corregir su inclusión”⁹⁴. Lo importante sería hacerlo en un tiempo razonable que minimice el daño

⁹⁴ RALLO LOMBARTE, A. (2010). El Derecho al olvido y su protección. *Revista TELOS* (Cuadernos de Comunicación e Innovación) nº 85, octubre-diciembre. Fundación Telefónica. Madrid, pág. 108. Véase también PIÑAR MAÑAS, J. L. (dir.) (2017). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*. Editorial Reus; FERNÁNDEZ VILLAZÓN, L. A., (2016). El nuevo reglamento europeo de protección de datos. *Revista Foro. Nueva Época*. Vol. 19, nº1; GIL GONZÁLEZ, E. (2016). *Big data, privacidad y protección de datos*. Agencia Española de Protección de

y no haga inútil el olvido. Lo que se pretende al hablar de derecho al olvido, como señala Pere Simón, es “encontrar el equilibrio entre todo lo que forma parte de la vida privada de las personas –intimidad, honor, propia imagen y datos personales– y lo que es público –contenido de las resoluciones judiciales y artículos de prensa–”. De esta manera, se configuraría como un derecho subjetivo de titularidad individual, ya que “a pesar de que no esté recogido explícitamente en la CE, no supondría un problema si se pretende establecer su titularidad individual, ya que el art. 10.1 de la CE reconoce la dignidad de la persona y el libre desarrollo de la personalidad como un espacio propio y reservado, de autonomía y libertad de actuar, del que es titular cada persona, vinculado necesariamente a la dignidad humana, con lo que las personas jurídicas no serían titulares del derecho al olvido digital”⁹⁵.

Parece, por tanto, que una vez que un usuario se da de alta en ciertas redes sociales, no puede luego borrar su rastro y desaparecer como si no hubiese estado allí. Es lo que se viene a conocer como “olvido digital” y que empieza a ser reclamado por quienes han usado las redes sociales y quieren desaparecer del ciberespacio. Internet se ha convertido en una herramienta de comunicación rápida y de fácil accesibilidad que se vuelve compleja a la hora de optar por borrar los datos de carácter personal. Se ha insistido mucho en la importancia de ser cuidadosos con las informaciones que se ofrecen en la red, con el objetivo de proteger al máximo la privacidad de esos datos y de evitar su utilización con fines para los que no han sido autorizados. En este sentido, “la acumulación de noticias que el motor de un buscador genera a través de millones de páginas web esparcidas en la red digital puede llegar a resultar, según los casos, una hipoteca para el honor y la intimidad”⁹⁶.

2.4. LA PROBLEMÁTICA DE LOS BUSCADORES Y LAS REDES SOCIALES

Los principales buscadores (*Google, Yahoo, Msn*) gestionan la mayor parte de la información que aparece en la red y es necesario su consentimiento para poder borrar

Datos; y YOUM, K. y PARK, A. (2016). The right to be forgotten in european union law: data protection balanced with free speech? *Journalism and Mass Communication Quarterly*. Vol. 93 (2), págs. 273- 295.

⁹⁵ SIMÓN CASTELLANO, P. (2011). *El Régimen Constitucional del derecho... ob. cit.*, págs. 100-125.

⁹⁶ CARRILLO LÓPEZ, M. (2009). *El derecho al olvido en Internet*. Disponible en línea en: https://elpais.com/diario/2009/10/23/opinion/1256248805_850215.html

una imagen o eliminar un dato personal. Por este motivo, el gobierno francés se ha planteado ya en varias ocasiones que el conocido como olvido digital se convierta en un derecho. Sin ir más lejos, el *Tribunal de Grande Instance* de París no dudó en afirmar que “toda persona que ha estado mezclada en acontecimientos públicos puede, con el paso del tiempo, reivindicar el derecho al olvido; que el recuerdo de esos acontecimientos y del papel que ha podido desempeñar en ellos es ilegítimo si no está fundado en las necesidades de la historia o si su naturaleza es tal que puede herir su sensibilidad. Visto que el derecho al olvido que se impone a todos, incluyendo a los periodistas, debe beneficiar a todos, incluyendo a los condenados que han pagado su deuda con la sociedad y que intentan reintegrarse en ella”. Además, dicha sentencia estableció dos condiciones que permiten exceptuar el derecho al olvido: “que se trate de la primera divulgación de hechos que dieron lugar a un procedimiento penal, y que los hechos expuestos presenten un interés contemporáneo y presente, es decir, actual en el momento de la divulgación”⁹⁷. Si se dan ambos condicionantes, no hay derecho al olvido.

El objetivo sería facilitar al máximo la supresión de la información de una persona sobre noticias pasadas que no están basadas en criterios de actualidad, incluidos los delitos de aquellas personas que ya hubiesen cumplido condena. Esto afectaría, sobre todo, a los motores de búsqueda, redes sociales y blogs. Este no es el primer paso que el país galo da en su interés por reconocer el carácter fundamental de dicho derecho, ya que, de manera pionera, en 1999, la *Comission nationale de l’informatique et les libertés* estableció la existencia del derecho al olvido, atendiendo al principio de finalidad del tratamiento de los datos. Por otra parte, el *Tribunal de Grande Instance* de París dictó la primera sentencia en la que se ordenaba a Google aplicar de manera correcta el derecho al olvido, exigiéndole que extendiese el borrado de ciertos enlaces a todos los dominios y no, como pretendía Google, hacerlo sólo en su filial francesa (Google.fr). El motivo es que “desde el territorio francés se puede conectar con otras *sites* del motor de búsqueda, lo que permite acceder a la información asociada a los apellidos de los demandantes”⁹⁸. Al respecto, también se ha posicionado la CNIL que considera que para que se cumpla

⁹⁷ Sentencia del *Tribunal de Grande Instance* de París, de 20 de abril de 1983. *Caso Mme. M. c. Filipacchi et Cogedipresse*.

⁹⁸ Sentencia del *Tribunal de Grande Instance* de París, de 16 de septiembre de 2014. *Caso M. et Mme X et M. Y / Google France*,

la sentencia del TJUE, de 13 de mayo, y la norma sea realmente efectiva, la eliminación de los enlaces en las páginas de resultados debe hacerse en todos los dominios y no sólo en el del país correspondiente.

Durante los últimos años, se han sucedido los casos de personas que se han visto perjudicadas por imágenes que colgaron tiempo atrás en la red. Las empresas, en procesos de selección para ocupar un determinado puesto, pueden, en muchos casos, a través de esas redes sociales, conocer datos personales de los candidatos, algunos, incluso íntimos, como aficiones o tendencias políticas. Esto es un hecho, ya que como recoge Rossen, en una encuesta realizada en 2010 por Microsoft, “el 75% de los reclutadores de los Estados Unidos y los profesionales de recursos humanos informan que sus empresas les obligan a hacer investigación en línea acerca de los candidatos, y muchos utilizan una variedad de sitios al examinar los candidatos, incluyendo motores de búsqueda, redes sociales, sitios web personales y blogs, Twitter y sitios de juego en línea”. Además, no dudan en reconocer (el 70%) que “rechazan a los candidatos debido a la información que encuentran en línea, como fotografías, conversaciones y pertenencia a grupos controvertidos”⁹⁹.

También las redes sociales sirven a las empresas para “espíar” a sus empleados y llegar a despedirlos. Un caso muy conocido es el Stacey Snyder¹⁰⁰. La Universidad Millersville en Pennsylvania le negó su título días antes de la graduación por una foto publicada, un año antes, en MySpace en la que aparecía disfrazada de pirata y con una copa en la mano con el texto “Pirata borracha”. Tras descubrir la página, el supervisor de la escuela dijo que la foto era poco profesional y, desde la Facultad de Educación, se la acusó de “promover la bebida entre los jóvenes”. Pero ese motivo no fue el único que llevó a la Universidad a tomar su decisión, ya que Snyder también publicó en la misma

⁹⁹ ROSEN, J. (2010). *The Web Means the End of Forgetting*. New York Times. Disponible en línea en: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?_r=1. Véase también VVAA (2016). Procesos de reclutamiento y las redes sociales. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo*. Vol. 6, nº12; y FLORES VIVAR, J. M. (2009). Nuevos modelos de comunicación, perfiles y tendencias en las redes sociales. *Comunicar. Revista Científica de Educomunicación*. Vol. 17, nº33, págs. 73-81.

¹⁰⁰ KREBS, B. (2008). *Court Rules Against Teacher in MySpace 'Drunken Pirate' Case*. Blog Security Fix. Washington Post. Disponible en línea en: http://voices.washingtonpost.com/securityfix/2008/12/court_rules_against_teacher_in.html.

red un comentario negativo contra su supervisor en la escuela secundaria, haciendo caso omiso a la recomendación de la Facultad que había advertido, con anterioridad, a los alumnos que no publicasen ningún comentario sobre el personal de la escuela en sus páginas web, ni agregar a sus estudiantes a páginas web personales. La implicada demandó a la Universidad entendiendo que se había violado sus derechos de la Primera Enmienda, pero un juez federal rechazó la demanda y falló a favor de la Universidad al considerar que “esa foto no estaba amparada por la libertad de expresión que protege la Primera Enmienda de la Constitución de los Estados Unidos, ya que se trata de un empleado público” (Caso *Snyder v. Millersville University*, de 3 de diciembre de 2008, Corte del Distrito Este de Pennsylvania).

En Alemania, las empresas hacían uso de las redes sociales para informarse de la vida privada de sus empleados o candidatos. Una práctica con la que ha acabado el Gobierno Federal Alemán al aprobar, el 25 de agosto de 2010, el Proyecto de Ley que modifica la legislación de protección de datos alemana. La conocida como “Ley Facebook”, que recoge que “para los datos guardados en las redes sociales, que sirven a la comunicación, prevalece el interés del usuario, digno de ser protegido”, prohibirá a las empresas hacer uso de datos personales de los empleados o candidatos contenidos en redes sociales de uso particular, con la que sólo se permitiría buscar a las empresas información sobre los candidatos en perfiles de redes sociales profesionales (*Xing*, *LinkedIn*) y no en otras como *Facebook* o *Twitter*.

El principal problema que plantea esta modificación es “la forma de probar cuándo una empresa ha consultado y tenido en cuenta los datos de una red social. Es decir, una empresa podría consultar los datos de un candidato a un puesto de trabajo y rechazar su candidatura alegando motivos que nada tuvieran que ver con la consulta de datos acerca de su vida privada. La misma dificultad se presentaría a la hora de poder probar que un despido se ha producido debido a que una empresa ha consultado la información contenida en redes sociales de uso privado”¹⁰¹.

¹⁰¹ BAÑOS, J. M. (2010). *Ley Facebook: Modificaciones en la legislación de protección de datos alemana*. Legal Today. Disponible en línea en: http://www.legaltoday.com/practica-juridica/publico/proteccion_de_datos/ley-facebook-modificaciones-en-la-legislacion-de-proteccion-de-datos-alemana. Véase también HORNUNG, G. y SCHNABEL C., (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law &*

Si trasladamos el caso a España, como apunta José Miguel Maestro, “es sabido que en el proceso de contratación laboral en España confluyen de forma contrapuesta el derecho a la libertad empresarial de contratación, de un lado (art. 38 de la CE), y el derecho fundamental a la intimidad del candidato en su búsqueda de empleo, por el otro (artículo 18.4 de la CE). Ambos intereses no gozarán de la misma protección, siendo éste último (y sus múltiples derivaciones) sobre el cual debiera gravitar una mayor atención por parte del legislador. Precisamente, la fase previa a la contratación ha sido uno de los ámbitos tradicionalmente criticados por la doctrina científica al no disponerse de una regulación específica”¹⁰².

2.5. MECANISMOS PARA HACER MÁS EFICAZ EL DERECHO AL OLVIDO

La pregunta que surge es cuándo y por qué puede solicitarse el derecho al olvido. Koops considera que existen dos razones para exigirlo. En primer lugar, “cuando el almacenamiento de los datos es potencialmente perjudicial para el individuo (un riesgo aquí y ahora) y, en segundo lugar, porque el almacenamiento de los datos ya no es necesaria y su retención podría llegar a ser perjudicial para el individuo en algún momento (un riesgo en el futuro)”¹⁰³.

Para que dicho riesgo no exista en un futuro, debería existir un buen sistema que asegurase que los responsables del tratamiento de los datos, los eliminen inmediatamente después de que cumplan su propósito y dejen de ser relevantes. Al respecto, Mayer-Schönberger propone “que los usuarios configuren de forma sistemática fechas de expiración de los datos. A través de esta eliminación automática de los datos después de su fecha de caducidad, se aseguraría que los usuarios puedan ejercer su derecho al olvido a priori: antes de generar, almacenar o compartir datos, sin

Security Report. Vol. 25 (1), págs. 84-88; y de los mismos autores (2009). Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention. *Computer Law & Security Report*. Vol. 25 (2), págs. 115-122.

¹⁰² MESTRE VÁZQUEZ, J. M. (2010). La protección de potenciales trabajadores en los procesos de selección: Incidencia de las redes sociales. *Capital Humano* n°248, noviembre, pág. 42.

¹⁰³ KOOPS, B. (2008). *Forgetting Footprints... ob. cit.*, pág. 12.

tener que preocuparse acerca de cuánto tiempo los datos se almacenarían sin su conocimiento”¹⁰⁴.

2.5.1. Aplicaciones tecnológicas para no dejar rastro y borrar el pasado

Esto es ya una realidad y ya hay aplicaciones que ofrecen a los usuarios proteger su privacidad y que puedan borrar sus datos. Dos estudiantes de la Universidad de Washington crearon en 2009 un programa, Vanish (Desaparecer), que permite borrar el pasado de un usuario en internet gracias a la autodestrucción de los textos de correos electrónicos, mensajes en foros, blogs, etc... en una fecha programada por dicho usuario. La forma de actuar es “cifrar el contenido de este texto con una llave que ni siquiera el propio usuario del programa conocerá. Una vez cifrado el texto con Vanish y elegida la fecha de autodestrucción, el texto será legible (usando Vanish para descifrarlo), pero al llegar la fecha fijada, el texto desaparecerá, ya que Vanish romperá la llave de cifrado repartiendo infinidad de trozos de esta por la red usando la tecnología P2P. Por cada ordenador que tenga una parte de la llave y que se desconecte se irá borrando parte del texto haciendo esta al final completamente ilegible”¹⁰⁵.

Una de las primeras aplicaciones que salió al mercado fue, en febrero de 2010, TigerText, que “permitía a los usuarios proteger la privacidad de los mensajes SMS que se mandaban de un móvil a otro. Ambos móviles han de tener descargada la aplicación y tanto los mensajes, como fotos y vídeos se autodestruyen cuando son leídos por el destinatario. Desaparecen, además, de los datos de la compañía telefónica, con lo que resultan irrecuperables. El período de tiempo en el que quieran que sus contenidos se eliminen es programado por los usuarios y pueden variar entre un minuto y treinta días”¹⁰⁶. Poner límite al transcurso del tiempo es un concepto que no es ajeno al derecho. Las instituciones de la caducidad y la prescripción tratan de poner límites

¹⁰⁴ MAYER-SCHÖNBERGER, V. (2009). *Delete: The virtue of forgetting in the digital Age*. Princeton University Press, pág. 171.

¹⁰⁵ GÓMEZ, H. (2009). *Borra tu pasado en internet en un fecha determinada con Vanish*. Disponible en línea en: <http://www.softzone.es/2009/07/26/dos-estudiantes-americanos-crean-un-programa-que-puede-borrar-textos-publicados-en-internet-en-una-fecha-determinada-en-softzone-lo-probamos-y-creamos-un-manual-de-vanish>

¹⁰⁶ *TigerText, una aplicación que protege la intimidad autodestruyendo los SMS* (2011). Disponible en línea en: <https://actualidad.rt.com/ciencias/view/23256-TigerText,-una-aplicaci%C3%B3n-que-protege-intimidad-autodestruyendo-SMS>

temporales a hechos o posibilidades jurídicas en atención a la seguridad jurídica y así aparece recogido cuando hablamos de acciones civiles¹⁰⁷ o penales¹⁰⁸.

Por lo tanto, como reconoce Jeffrey Rosen, “Facebook podría implementar fechas de vencimiento de su propia plataforma, por lo que nuestros datos desaparecerían después de, digamos, tres días o tres meses a menos que un usuario especificase que quería guardarlos para siempre, permitiendo a los usuarios que están preocupados por la privacidad de hacer desaparecer sus datos, sin imponerles el valor de guardarlos por defecto para todos los usuarios de Facebook”. Al contrario de lo que pudiese parecer, Facebook en lugar de “apostar por la privacidad, lo hace por la transparencia”¹⁰⁹.

2.5.2. Derechos reconocidos: rectificación, cancelación, oposición y supresión

Es muy frecuente que en momento puntual, cualquier usuario realice un comentario en sus redes sociales sin pensar en las consecuencias que podría tener. Aunque a continuación lo borre, ese mensaje ya ha circulado y puede aparecer en el perfil de otros usuarios, que lo hayan compartido o retuiteado¹¹⁰. Los medios de comunicación tradicionales utilizan las redes sociales de los famosos para cubrir sus informaciones, pasando de un periodismo de investigación a un periodismo virtual de caracteres.

El escribir en el anonimato o bajo un seudónimo permite a los usuarios desinhibirse y realizar cualquier tipo de comentario, que puede dañar la imagen o el honor de las personas. La directiva 2000/31/CE establece, en su artículo 16, que los prestadores de servicios de alojamiento de datos en la web, no serán responsables por la “información almacenada a petición del destinatario, siempre que no tengan conocimiento efectivo de que la actividad o información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o si es que lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos”. La Ley 34/2002, LSSICE,

¹⁰⁷ El Código Civil recoge entre los artículos 1.962 y 1.968 el período que ha de transcurrir para que prescriban las acciones civiles.

¹⁰⁸ El artículo 131 del Código Penal recoge la prescripción de los delitos, las faltas y los delitos de lesa humanidad, genocidio y terrorismo.

¹⁰⁹ ROSEN, J. (2010). *The Web Means the End... ob. cit.*, pág. 5.

¹¹⁰ Debido a la cotidianidad en el uso de las redes sociales, la RAE recogió el verbo tuitear, haciendo referencia a la red social Twitter, definiéndolo como “comunicarse por medio de tuits”.

ratifica dicha argumentación, excusando a los prestadores de servicio de hosting o alojamiento web si no tienen conocimiento de los comentarios que allí se publican.

Podemos decir que el derecho ya contempla mecanismos para regular, de algún modo el derecho al olvido, como son el derecho de rectificación y cancelación¹¹¹. Este artículo viene a completar la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación en la que se reconoce que “toda persona natural o jurídica, tiene derecho a rectificar la información difundida, por cualquier medio de comunicación social, de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicio”¹¹². Pero no ha sido hasta la entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, cuando se ha reconocido el derecho al olvido como un derecho de supresión.

¹¹¹ Artículo 16 LOPD: “1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días. 2. Serán rectificadas o canceladas, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos. 3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión. 4. Si los datos rectificadas o canceladas hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación. 5. Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado”. El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, recoge en su artículo 16 el derecho de rectificación, en el que señala que “el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional”.

¹¹² Ley Orgánica 2/1984. Artículo 1.

No hay que olvidar que en el ámbito del derecho fundamental a la protección de datos, los ciudadanos poseen el derecho a exigir la cancelación¹¹³ de la información que contiene datos personales cuando “el tratamiento de los datos de carácter personal requiera el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa”¹¹⁴. En este sentido, el siguiente apartado del artículo 6 recoge las excepciones en las que no son precisas que el usuario dé su consentimiento: “cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6¹¹⁵, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado”.

¹¹³ El Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, aprobado por el Real Decreto 1720/2007, de 21 de diciembre, define en su artículo 5.1.b) la cancelación como: “procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos”.

¹¹⁴ LOPD. Artículo 6.1.

¹¹⁵ “Podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 -datos que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros- y 3 -datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual-de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto”.

Entre la rectificación de los medios de comunicación y aquella que tiene lugar en la protección de datos, existe “una diferencia sustantiva: el derecho no implica la sustitución de lo publicado, sino una aclaración e indicación del error cometido. En otros términos, rectificar forma parte del reconocimiento del error, del deber de entregar información veraz que, aunque no haya sido la correcta, aclara su verdadero contenido”¹¹⁶. Por otra parte, sabemos que el derecho a rectificación en materia periodística significa más allá de la exactitud de la información publicada, la divulgación de otra versión de los hechos, tal como lo ha dicho el Tribunal Constitucional español en la STC 168/1986, de 22 de diciembre¹¹⁷.

El derecho de oposición se aplicaría, por tanto, como señala Mario Hernández “para evitar la indexación de datos personales por los motores de búsqueda valorando siempre, en cada caso concreto, la incidencia que pueda tener en los derechos del ciudadano, atendiendo a sus circunstancias específicas”. Aunque reconoce que “ningún derecho fundamental es absoluto ni ilimitado y el derecho al olvido no escapa a esta categórica afirmación, pues la pretensión del ejercicio de cancelación u oposición puede chocar con los derechos, por ejemplo, de libertad de información o expresión de otras personas”¹¹⁸.

¹¹⁶ ZÁRATE ROJAS, S. (2013). La problemática entre el derecho al olvido y la libertad de prensa. *Revista Derecom* nº13, pág. 4.

¹¹⁷ FJ5: “El ejercicio del derecho de rectificación tampoco limita el derecho de la colectividad y de los individuos que la componen a recibir libremente información veraz, pues no comporta una ocultación o deformación de la que, ofrecida con anterioridad, lo sea o pueda serlo. Aún más, como ya se ha dicho, la inserción de la rectificación interesada en la publicación o medio de difusión no implica la exactitud de su contenido, pues ni siquiera la decisión judicial que ordene dicha inserción puede acreditar, por la propia naturaleza del derecho ejercitado y los límites procesales en que se desenvuelve la acción de rectificación, la veracidad de aquélla. A todo ello cabe añadir que la divulgación de dos versiones diferentes de unos mismos hechos, cuya respectiva exactitud no ha sido declarada por ningún pronunciamiento firme de los órganos judiciales competentes, no restringe tampoco el derecho a recibir la información que sea veraz, es decir, a conocer cuál de aquellas dos versiones se adecúa a la realidad de lo acontecido, ya que debemos insistir en ello la investigación de la verdad y la declaración de los hechos ciertos siempre puede instarse y determinarse a posteriori mediante las acciones y procedimientos plenarios que el ordenamiento arbitra al efecto”.

¹¹⁸ HERNÁNDEZ RAMOS, M. (2013). El derecho al olvido digital en la web 2.0. *Revista Cátedra Telefónica-Universidad de Salamanca* nº11, mayo, págs. 30-32. ”. El derecho de oposición también aparece recogido en el artículo 21 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo,

La actividad de los buscadores se centra, principalmente, en asociar los términos de búsqueda a los sitios web en los que consta información al respecto. Por lo que “el ejercicio de los derechos de cancelación u oposición debería estar asociado a un ejercicio correlativo de tales derechos frente a los responsables de estos sitios web, que son quienes, en origen, permiten el acceso a la información personal”. Sin embargo, el conflicto surge cuando la página web que aloja la información no puede borrar los datos “por existir un amparo legal o un conflicto con otro derecho fundamental, y su indexación por parte de buscadores provoca una difusión masiva de la información personal. Es aquí cuando puede alcanzar su plena virtualidad el derecho del ciudadano a oponerse al tratamiento, si concurre un motivo legítimo y fundado referido a su concreta situación personal”¹¹⁹.

de 27 de abril de 2016, en el que se señala que: “**1.** El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. **2.** Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia. **3.** Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines. **4.** A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información. **5.** En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas. **6.** Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público”.

¹¹⁹ RALLO LOMBARTE, A. (2010). El Derecho al olvido... *ob. cit.*, págs. 109-110. El problema como señala MIERES, L. J., *El derecho al olvido... ob. cit.*, pág. 25; es que el derecho al olvido “supusiese hacer posible borrar o reescribir la historia. Implicaría otorgar a las personas la facultad de alterar la objetividad de lo ocurrido, modificando su contenido o imposibilitando a los demás el acceso a esa información”. Además, hay que matizar como hace la AEPD, que “la cancelación de datos no debe

La AEPD ha delimitado, a través de sus resoluciones, criterios para tutelar la procedencia del derecho de cancelación y oposición en servicios de búsqueda. En estos casos, las resoluciones dictadas “reconocen el derecho de los solicitantes, instando a Google para que adopte las medidas necesarias para retirar los datos de su índice e imposibilite el acceso futuro a los mismos”¹²⁰. La fundamentación jurídica sobre la que se asientan dichas resoluciones parte, “de un lado, del sometimiento de los prestadores de estos servicios a la legislación nacional (aun encontrándose el responsable de tratamiento situado fuera del Espacio Económico Europeo, la legislación comunitaria se aplica cuando cuenta con un establecimiento en un Estado miembro o cuando acude a medios situados en éste), y de la ausencia de precepto legal o amparo constitucional a la permanencia de la información en los índices de búsqueda, ni en las páginas que buscadores conservan temporalmente en memoria caché”¹²¹.

Además, según el artículo 33 del RLOPD: “1. La cancelación no procederá cuando los datos de carácter personal deban ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado que justificaron el tratamiento de los datos. 2. Podrá también denegarse los derechos de rectificación o cancelación en los supuestos en que así lo prevea una ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso. 3. En todo caso, el responsable del fichero informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre”.

confundirse con la solicitud de baja de un servicio previamente contratado; o con la devolución de copias de documentos o contratos; o con la supresión de comentarios en foros, que no es materia de protección de datos”.

¹²⁰ R/00155/2009, de 4 de febrero y R/01795/2009, de 5 de octubre.

¹²¹ RALLO LOMBARTE, A., El Derecho al olvido... *ob. cit.*, pág. 110.

No sólo la LOPD establece los periodos de rectificación o cancelación de los datos de carácter personal, sino que, conforme a la legislación vigente, los principales periodos de prescripción de dichos datos son¹²²:

- “15 años para los datos de clientes y proveedores que fueran persona física, salvo que sea aplicable un plazo inferior de conservación¹²³. Este plazo se corresponde con el general establecido para la prescripción de las acciones personales en la legislación civil.

- 6 años para los datos de proveedores y suministradores, en lo que se refiere al cumplimiento de la obligación de conservar libros, correspondencia, documentación y demás justificantes concernientes a su negocio¹²⁴.

- 5 años para los datos de clientes y proveedores, en lo que se refiere al cumplimiento de obligaciones de pago que deban hacerse por años o plazos más breves¹²⁵.

- 5 años para los datos relativos al cumplimiento de obligaciones en materia de Prevención de Riesgos Laborales¹²⁶.

- 4 años para los datos relativos al cumplimiento de la obligación de pago de las cuotas de la Seguridad Social de los trabajadores¹²⁷.

- 1 año para las restantes categorías de datos de los trabajadores. Los datos relativos a la relación laboral deberán conservarse, al menos, hasta que transcurra un año desde la expiración del contrato, como regla general.

- 30 días para los datos recabados en los registros de visitas de acceso a edificios, a contar desde el día en que fueron recabados¹²⁸.

- 1 mes para los datos recabados mediante sistemas de videovigilancia que incluyan grabación de las imágenes captadas, a contar desde el día de la captación”¹²⁹.

¹²² VV.AA. (2010). *Factbook: Protección de Datos Personales*. Aranzadi. Madrid, pág. 85.

¹²³ Código Civil. Artículo 1964.

¹²⁴ Código de Comercio. Artículo 30.

¹²⁵ Código Civil. Artículo 1966.

¹²⁶ Infracciones y Sanciones en el Orden Social. Artículo 4.

¹²⁷ Ley General de la Seguridad Social. Artículo 21.

¹²⁸ Norma 5ª de la Instrucción 1/1996, de 1 de marzo, de la Agencia Española de Protección de Datos sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.

¹²⁹ Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras y videocámaras. Artículo 6.

- El tiempo adecuado a cada caso o, como mínimo 5 años para la conservación de la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original¹³⁰.

- La documentación clínica también se conservará cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas¹³¹.

A pesar de poder utilizar estos derechos, citados anteriormente, y ya reconocidos para la protección de datos, sin embargo, en la actualidad, como reconoce Ramón Orza, “la confluencia, por un lado, de una demanda creciente de datos personales reales en internet, la continua fuente de datos personales que las publicaciones oficiales se vuelcan en la red y el creciente volumen de información que suministran también a internet los medios de comunicación, hacen que los intentos de los ciudadanos por preservar su vida privada al margen de internet, utilizando estos recursos, resultan infructuosos. Por ello habría que introducir en la legislación otros instrumentos legales, al margen de la reinterpretación de los derechos de acceso, rectificación, cancelación y oposición, que refuerzan la posición del ciudadano que desea preservar su anonimato, incluso en internet. Quizá sea la STC 144/1999, de 22 de julio¹³² la que ofrezca un nuevo punto de apoyo para la creación de instrumentos legales que refuerzan el control

¹³⁰Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Artículo 17.1.

¹³¹ Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. Artículo 17.2.

¹³² FJ8: “Todas estas precauciones derivadas del contenido constitucional del derecho a la intimidad y, en particular, del deber positivo de protección de este derecho, que pesa sobre los poderes públicos, son, justamente, la razón que justifica las medidas legales restrictivas del acceso a esa información sensible, constituyendo una ilegítima intromisión en la intimidad individual, lesiva del art. 18.1 C.E. la infracción de las normas sobre acceso a la información relativa a una persona o su familia, con independencia de que esa información sea objetivamente considerada de las íntimas o de que su conocimiento o divulgación pueda ser pernicioso para la integridad moral o la reputación de aquel o de aquellos a quienes se refiere. Pues, de no ser así, atribuiríamos a los poderes públicos el poder de determinar qué es íntimo y qué no lo es, cuando lo que el art. 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio”.

sobre nuestra propia vida y garanticen también en estos ámbitos, en definitiva, nuestra libertad”¹³³. El derecho, como señala la sentencia, a ser desconocido y a que los demás no sepan qué somos y qué hacemos está ampliamente relacionado con el derecho al olvido, ya que si no queremos que los demás sepan lo que hacemos, con más razón podremos tratar de borrar aquellas informaciones del pasado que sean irrelevantes o atemporales.

Bien es cierto que las nuevas tecnologías habían dejado obsoletos algunos principios y derechos contemplados en la Directiva 95/46/CE, principalmente los relacionados con la privacidad y la protección de datos al encontrarse más expuestos y en un marco completamente desconocido hasta entonces , que, ahora, parecen subsanarse con el artículo 17 del nuevo Reglamento Europeo, ya citado. Además, la UE aprobó la Directiva 2009/136/CE por la que se modificaban la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas; y 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. El objeto de esta Directiva es “garantizar la existencia de servicios de comunicaciones electrónicas disponibles al público, de buena calidad, en toda la Comunidad a través de una competencia y una libertad de elección reales, y tratar las circunstancias en que las necesidades de los usuarios finales no se vean atendidas de manera satisfactoria por el mercado”¹³⁴. Además, establece “los derechos de los usuarios finales y las correspondientes obligaciones de las empresas que proporcionan redes y servicios de comunicaciones electrónicas disponibles al público. Con vistas a garantizar que se preste un servicio universal dentro de un entorno de mercado abierto y competitivo, definiendo el conjunto mínimo de servicios de calidad especificada al que todos los usuarios finales tienen acceso habida cuenta de condiciones nacionales específicas, a un precio asequible, sin distorsión de la competencia”¹³⁵.

¹³³ ORZA LINARES, R. M. (2012). Derechos Fundamentales e Internet: Nuevos problemas, nuevos retos. *Revista de Derecho Constitucional Europeo* nº18, julio-diciembre, pág. 335.

¹³⁴ Directiva 2009/136/CE. Artículo 1.1.

¹³⁵ Directiva 2009/136/CE. Artículo 1.2.

El artículo 5 de dicha Directiva¹³⁶ es el encargado de desarrollar y concretar la adopción de aquellas medidas, técnicas o de gestión, precisas para garantizar un nivel de seguridad adecuado, además, de un deber de informar a abonados y usuarios. La confidencialidad, tanto de los contenidos transmitidos como de cualquier dato relacionado con la persona ha encontrado su máxima garantía en la tipificación de los delitos de descubrimiento y revelación de secretos de los artículos 197 a 201 del Código Penal.

¹³⁶ Directiva 2009/136/CE. Artículo 5: “1. Los Estados miembros garantizarán, a través de la legislación nacional, la confidencialidad de las comunicaciones, y de los datos de tráfico asociados a ellas, realizadas a través de las redes públicas de comunicaciones y de los servicios de comunicaciones electrónicas disponibles al público. En particular, prohibirán la escucha, la grabación, el almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los usuarios, sin el consentimiento de los usuarios interesados, salvo cuando dichas personas estén autorizadas legalmente a hacerlo de conformidad con el apartado 1 del artículo 15. El presente apartado no impedirá el almacenamiento técnico necesario para la conducción de una comunicación, sin perjuicio del principio de confidencialidad. 2. Las guías mencionadas en el apartado 1 incluirán, a reserva de lo dispuesto en el artículo 12 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas a todos los abonados a servicios telefónicos disponibles al público. 3. Los Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento. La presente disposición no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado”.

CAPÍTULO 3. EL DERECHO A LA INTIMIDAD ELECTRÓNICA

Con la aparición de Internet y las nuevas tecnologías se ha producido un aumento de las conductas lesivas a través de ataques a la información patrimonial y de acceso a datos reservados, realizado con el objetivo de conseguir información personal o profesional. En este sentido, hay que señalar que ambas conductas podían ocurrir simultáneamente y que el mero acceso no autorizado a un sistema informático ajeno no constituía por sí solo delito hasta la reforma del Código Penal¹³⁷. Desde el punto de vista penal, este tipo de delitos estaría encuadrado dentro de los “delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio”¹³⁸ cuando el bien atacado sea la intimidad personal o el secreto de las comunicaciones de carácter personal.

En relación a los correos electrónicos, hay quién señala a efectos penales, que éstos deben entenderse como “una modalidad de comunicación, por lo general de carácter personal, que incorpora texto, voz, sonido o imagen y que se sirve de las redes telemáticas como tecnología de transmisión y de los sistemas informáticos como instrumentos de remisión y de recepción entre dos o más comunicantes, y de almacenamiento de los mensajes”¹³⁹. Por eso, se amplía el abanico no sólo a los correos electrónicos como tales, sino también a los programas de mensajería instantánea, a los mensajes privados de foros o cualquier otra comunicación mediante texto, imagen, audio o vídeo.

3.1. EL DERECHO A LA VIDA PRIVADA EN LAS REDES

Las redes sociales (*Facebook, Tuenti, Twitter, Instagram*) cada vez están más presentes en el día a día. Actualmente en España, más de 25 millones de personas interactúan

¹³⁷ La Ley Orgánica 5/2010 de Reforma de Código Penal, de 22 de junio, en su artículo 197.3 señala que: “El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años”.

¹³⁸ Capítulo Primero del Título X de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

¹³⁹ ROMEO CASABONA, C. M. (2005). *Los delitos de descubrimiento y revelación de secretos*. Tirant lo Blanch. Valencia, pág. 80.

habitualmente a través de este medio¹⁴⁰, manteniéndose estable con respecto a los últimos años. Un fenómeno que lleva consigo una serie de riesgos en lo que a privacidad se refiere, porque, como apunta Celaya, “las redes sociales son lugares en Internet donde las personas publican y comparten todo tipo de información, personal y profesional, con terceras personas, conocidos y absolutos desconocidos”¹⁴¹.

Lo que está claro es que las actividades en línea dejan huellas electrónicas. Los proveedores de Internet pueden determinar qué tipo de buscadores se utilizan, qué páginas web se han visitado. Los administradores de los sitios pueden monitorear las actividades colocando *cookies* en la computadora del internauta, pudiendo obtener más información e, incluso, transmitirla a otros sitios. Existen herramientas de protección de la privacidad, que evitan dejar rastro y, en este sentido, en efecto, nos protegen. En 2009, la Unión Europea preocupada por la privacidad de los usuarios aprobó la Directiva 2009/136/CE, de 25 de noviembre, que más tarde, concretamente en marzo de

¹⁴⁰ Datos recogidos del Estudio Anual de Redes Sociales 2019, elaborado por IAB Spain. Por primera vez, el estudio señala que la red social con más usuarios es Whatsapp, superando a Facebook. Por su parte, Instagram, se coloca en cuarta posición, siendo la red que más sube en usuarios con un 49%.

¹⁴¹ CELAYA, J. (2008). *La Empresa en la WEB 2.0*. Editorial Grupo Planeta. Con anterioridad BOYD, D. y ELLISON, N. (2007). Social Network Sites: Definition, history and scholarship. *Journal of Computer-Mediated Communication* nº13 (1); las definieron como “servicios dentro de las webs que permiten al usuario construir un perfil público o semi-público dentro de un sistema limitado, articular una lista de otros usuarios con los que comparte una conexión, y visualizar y rastrear su lista de contactos y las elaboradas por otros usuarios dentro del sistema. La naturaleza y nomenclatura de estas conexiones suele variar de una red social a otra”. Por su parte, RIZO GARCÍA, M. (2003). *Redes. Una aproximación al concepto*. Consejo Nacional para la Cultura y las Artes (Conaculta), las define como “formas de interacción social, que se definen fundamentalmente por los intercambios dinámicos entre los sujetos que las forman. Las redes son sistemas abiertos y horizontales y aglutinan a conjuntos de personas que se identifican con las mismas necesidades y problemáticas. Las redes, por tanto, se erigen como una forma de organización social que permite a un grupo de personas potenciar sus recursos y contribuir a la resolución de problemas”. Por último, el *Estudio sobre la privacidad de los datos y la seguridad de la información en las redes sociales online* (2009). Observatorio de la Seguridad de la Información. Madrid; las califica como “los servicios prestados a través de Internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al perfil publicado”.

2012, se incorporaría al ordenamiento jurídico español, modificando el apartado 2 del artículo 22¹⁴² de la LSSICE 34/2002, de 11 de julio.

Los proveedores de Internet presentan su política de privacidad en sus sitios electrónicos o en otros documentos. Sellos de aprobación como *TRUSTe*¹⁴³ o *BBBOnline*¹⁴⁴ respaldan la privacidad. La revisión de las *cookies* llevará a aceptar, rechazar o seleccionar a las de aquellas páginas en las que se esté interesado a acceder. No toda comunicación en Internet es privada, a menos que se utilicen programas decodificadores especiales.

3.1.1. Usurpación de la identidad y fraudes online

Los usuarios facilitan una serie de datos de carácter personal al inscribirse en estos portales que deben ser convenientemente protegidos conforme a la legislación. La propia naturaleza de estos sitios web implica que los usuarios incluyan amplia información sobre sus preferencias, que también ha de ser protegida, especialmente en el caso de los menores¹⁴⁵. El hecho de que las redes sociales pongan a disposición pública tal cantidad de información provoca, tanto de forma directa como indirecta, la aparición de casos jurídicos novedosos como la usurpación de identidad o los fraudes online. En este sentido, “no es que los nuevos medios electrónicos hayan modificado el

¹⁴² Tras la modificación, dicho artículo quedaría así: “Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

¹⁴³ *TRUSTe*: Empresa, con sede en San Francisco, encargada de certificar la privacidad y protección de datos de los sitios web, a través de sellos de privacidad en línea.

¹⁴⁴ *BBBOnline*: Empresa encargada de tramitar con rapidez y facilidad las denuncias en línea, principalmente las reclamaciones relativas a transacciones del mercado y publicidad.

¹⁴⁵ *Estudio sobre la privacidad de los datos personales... ob. cit.* (2009), pág. 27.

concepto de privacidad, pero sí que han cambiado las formas en que éste puede ser protegido o puesto en peligro”¹⁴⁶.

Como la información de carácter personal que se introduce en la red puede ser captada y tratada en cualquier parte del mundo, resulta más necesario crear disposiciones que se aparten de la casuística y sienten líneas de solución. Desde un punto de vista procedimental aparece con más fuerza la necesidad de disponer de normas válidas y asumibles a nivel internacional y no aplicables por poderes judiciales soberanos sino por otros órganos no jurisdiccionales¹⁴⁷.

Cada vez es más frecuente la utilización de Internet como medio de comunicación interpersonal para acceder a informaciones reservadas, atentando contra aspectos de la intimidad. Este delito que viene tipificado en el primer apartado del artículo 197 del CP está castigado con penas de prisión de entre uno y cuatro años.

El mecanismo más frecuente de usurpación o suplantación de identidad en cuentas de correo electrónicas, que supone el vínculo electrónico entre la imagen y la intimidad, es la obtención de las claves de acceso por diversos procedimientos. La sentencia 140/2008, de 20 de julio, del Juzgado de lo Penal número 11 de Barcelona¹⁴⁸ señala que “el moderno sistema de comunicación y transmisión de datos e información que

¹⁴⁶ CAMPUZANO TOMÉ, H. (2000). *Vida privada y datos personales: su protección jurídica frente a la sociedad de la información*. Tecnos. Madrid, pág. 69. Ver también AGUSTINA, J. R. (2014). *Cibercriminalidad y perspectiva victimológica: Un enfoque explicativo de la cibervictimización*. *Cuadernos de Política Criminal* nº114, págs. 143-178; MIRÓ LLINARES, F. (2011). *La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen*. *Revista Electrónica de Ciencia Penal y Criminología* nº 13-07; DE LA CUESTA ARZAMENDI, J. L. y PÉREZ MACHÍO, A. I. (2010). *Ciberdelincuentes y cibervíctimas*. *Derecho Penal Informático*. Pamplona, págs. 99-120; y ROMEO CASABONA, C. M^º. (2006) (coord.). *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Comares. Granada.

¹⁴⁷ Es el caso de ICANN (Internet Corporation for Assigned Names and Numbers), organización dedicada a preservar la estabilidad operacional de Internet, promover la competencia, lograr una amplia representación de las comunidades mundiales de Internet y desarrollar las normativas adecuadas a su misión por medio de procesos “de abajo hacia arriba” basados en el consenso.

¹⁴⁸ Los hechos ocurrieron cuando la acusada, antigua compañera de clase de la demandante, gracias al conocimiento de diversos datos personales de ésta, logró descifrar la contraseña y acceder a la cuenta de correo, modificando la contraseña e impidiendo a la verdadera titular acceder y controlar dicha cuenta.

conocemos como correo electrónico, hace referencia a una realidad compleja compuesta de al menos, y a los efectos que ahora nos importan, tres elementos diferentes. Primero, cada uno de los concretos mensajes que a través de este procedimiento informático circulan; segundo, los ficheros que incorporan las aplicaciones, donde se guarda el correo entrante, el enviado, incluso aquellos mensajes que están preparados como borrador o ya han sido eliminados, y por último, la libreta de direcciones y el historial de tráfico registrado. Parecidamente a lo que ocurre con otros sistemas actuales como los teléfonos celulares portátiles, el correo electrónico, como sistema informático, contiene una ingente cantidad de datos de carácter personal, en diversa presentación y de diferentes características, que normalmente atañen a la esfera privada de las personas, y que encuentran variadas vías de protección en el art. 197 del Código Penal” (FJ3).

La sentencia concluye en castigar a quien accede a correos electrónicos ajenos, al considerar que “resulta subsumible en el artículo 197.2 del Código Penal la conducta de quien sin estar autorizado, acceda por cualquier medio a datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros informáticos o electrónicos. El sistema de correo electrónico participa de la naturaleza de fichero o soporte de datos en tanto que conserva además de los mensajes concretos, listados de mensajes enviados o recibidos, libreta de direcciones, etc. La entrada no consentida en la aplicación de correo electrónico de otra persona y el recorrido por las diferentes bases de datos que el sistema contiene, incluso sin abrir ningún mensaje, puede ser penalmente típica ya que con ella se está produciendo una intromisión en la intimidad y susceptible de facilitar una toma de conocimiento de datos muy sensibles y reservados”. Además reconoce que “el artículo 197.2 del Código Penal se presenta desprovisto de la necesaria concurrencia de otros elementos subjetivos del injusto adicionales como son el ánimo de descubrir los secretos o vulnerar la intimidad de otro. Por lo tanto, al acceder a estos archivos, se asume como mínimo con dolo eventual o mejor decir por indiferencia, que con su proceder podría vulnerar la legalidad penal, en tanto que el sistema de correo electrónico es un archivo, soporte o fichero que contiene datos, bases de datos e información que pueden ser reservados de carácter personal o familiar de otro”. De ahí que el magistrado considere que “la intervención del derecho penal está justificada por la especial insidiosidad del medio empleado que penetra en los espacios reservados de la persona, de ahí la intensa ofensividad para el bien jurídico tutelado, que

se atenúa cuando se produce en lugares públicos, aún sin consentimiento del titular del derecho, que en línea de principio debe generar una respuesta extrapenal” (FJ3).

Para finalizar, la sentencia concluye señalando que, “por todo lo expuesto poco importa el contenido de los mensajes, debiendo descartar la teoría de la defensa conforme que sólo un 2% afectaba a la intimidad, dado que la intimidad se vulnera por el hecho de acceder al correo electrónico de una persona con independencia de cuál sea el contenido que tenga en el mismo, puesto que sino esto llevaría al absurdo de que si una persona en sus correos electrónicos sólo los dedica a temas laborales, por ejemplo, el acceso no consentido al mismo nunca podría subsumirse en este delito. El delito no lo constituye el resultado de la información que obtengo sino el modo en que se accede a dicha información” (FJ3). Además, el juez no sólo impone una condena penal al demandado como autor de un delito de revelación de secretos, sino que también fija una cantidad por responsabilidad civil del perjuicio, en parte debido a que “toda vulneración de la intimidad de una persona produce un desasosiego e intranquilidad de la que debe resarcirse. Por ello, por el desasosiego e intranquilidad que le causó al demandante que se tuviera conocimiento de dichos correos, fijo la responsabilidad civil en 4.000 euros por los daños morales ocasionados” (FJ8).

El TS se ha pronunciado al respecto de la usurpación y considera que “usurpar el estado civil¹⁴⁹ de otro lleva siempre consigo el uso del nombre y apellidos de ese otro, pero evidentemente requiere algo más, sin que sea bastante la continuidad o la repetición en el tiempo de ese uso indebido para integrar la mencionada usurpación”. Lo que quiere decir es que para usurpar “no basta con usar un nombre y apellidos de otra persona, sino que es necesario hacer algo que solo puede hacer esa persona por las facultades, derechos u obligaciones que a ella solo corresponden; como puede ser el obrar como si uno fuera otro para cobrar un dinero que es de este, o actuar en una reclamación judicial haciéndose pasar por otra persona, o simular ser la viuda de alguien para ejercitar un derecho en tal condición, o por aproximarnos al caso presente, hacerse pasar por un determinado periodista para publicar algún artículo o intervenir en un medio de

¹⁴⁹ Así lo recoge el artículo 401 del CP: “El que usurpare el estado civil de otro será castigado con la pena de prisión de seis meses a tres años”. Entendiendo el concepto civil como identidad o personalidad.

comunicación” {STS 3931/2009, de 15 de junio. Sala de lo Penal (nº de recurso: 1721/2008). FJ2}.

El TS lo ve como “un delito de simple actividad que no exige necesariamente un resultado dañoso y que comporta la arrogación de las cualidades de otra persona, verificando una auténtica implantación de personalidad. El delito, por tanto, se perfecciona con la realización de la actividad usurpadora y cesa cuando concluye la implantación. La conducta del agente exige una cierta permanencia y es inherente al propósito de usurpación plena de la personalidad global del afectado” {STS 6858/2011, de 14 de octubre. Sala de lo Penal (nº de recurso: 10365/2011). FJ7}. Además de vulnerar el artículo 401 del CP, en caso de que se utilizasen fotografías de la persona cuya identidad ha sido usurpada, se podría estar cometiendo un delito contra el derecho a la propia imagen (artículo 18.1 CE). Eso sí, lo que no se consideraría delito es si el usuario crea un perfil falso para participar en una red social, simplemente para ocultar su identidad y no haciéndose pasar por otro.

La usurpación de la identidad puede llevar consigo la comisión de otros delitos como, por ejemplo, la revelación de secretos o el robo de contraseñas o cuentas, que han sido recogidos en el CP en su última modificación, de 30 de marzo de 2015. Así, lo establece el artículo 197 *bis* y *ter* que recogeremos más adelante. Con la reforma del CP y la entrada en vigor de estas modificaciones, España se equipara a Francia que ya en 1988 había aprobado la ley francesa sobre fraude informático, más conocida como Ley Godfrain. Un artículo único que se introduce en el *Code Pénal* y en el que se castiga al que “fraudulentamente acceda en todo o parte a un sistema de tratamiento automatizado de datos; al que intencionadamente obstruya o distorsione el ejercicio de un sistema de tratamiento automatizado de datos; aquel que, intencionadamente, introduzca, borre o altere datos en un sistema de tratamiento automatizado de datos; o el que lleve a cabo la falsificación de documentos informáticos, independientemente de la forma”¹⁵⁰.

En cuanto al fraude online, El TS analizó el caso de una persona acusada que, durante varios meses, con la intención de enriquecerse, publicó en la página web

¹⁵⁰ Artículos 462.2 a 462.5. de la Ley Godfrain, de 5 de enero de 1988, introducidos, posteriormente, en el *Code Pénal* francés.

www.milanuncios.com y otras, anuncios por los que vendía teléfonos móviles Iphone 4 valorados en setecientos cincuenta euros, según precio de mercado, sin ser distribuidor autorizado ni disponer o tener intención de entregar tales móviles a los eventuales compradores, sino con el ánimo de quedarse con el adelanto por ellos recibidos, cosa que ocurrió en tres casos con unos ingresos en cuenta de trescientos, doscientos cincuenta dos y doscientos euros. Quienes ingresaron esas cantidades no recibieron el objeto que creían comprar ni recuperaron el dinero entregado. El TS estimó “el recurso de revisión interpuesto por la representación del demandante, al que se adhirió el Ministerio Fiscal, y se declaró la nulidad de la sentencia del Juzgado de Instrucción nº 2 de Granada, de 15 de octubre de 2012, en el juicio de faltas 239/2012¹⁵¹, en la que fue condenado el ahora recurrente como autor de una falta de estafa” {STS 817/2014, de 26 de noviembre. Sala de lo Penal (nº de recurso: 20811/2013). Fallo}, condenando al autor “por un delito continuado de estafa, a una pena de 8 meses de prisión e inhabilitación especial para el ejercicio del derecho de sufragio pasivo durante el tiempo de la condena, así como al abono de las costas causadas en el presente procedimiento y al pago de 300, 252 y 200 euros, respectivamente a favor de los estafados , en concepto de indemnización civil por los daños y perjuicios causados de naturaleza patrimonial, cantidad sobre la que computarán intereses legales incrementados en dos puntos, desde la fecha de esta resolución hasta su completo pago, por eventual demora procesal” (Sentencia del Juzgado de lo Penal nº 28 de Barcelona 416/2013, de 3 de octubre de 2013. Procedimiento Abreviado 256/13).

3.1.2. Régimen jurídico de la vida privada electrónica

Otro caso bien distinto es que haya sido el propio usuario quien haya “colgado” la información o las imágenes. Facebook, la red social con más seguidores (unos 2.271 millones en todo el mundo¹⁵²), y con sede en California, devenida un fenómeno mundial, para salvaguardar la privacidad de los usuarios cuenta con una licencia de

¹⁵¹ La sentencia condenó al autor por “una falta de estafa, tipificada en el artículo 623.4 del Código Penal a la pena de 40 días multa a razón de una cuota diaria de 6 euros, que deberán hacer efectiva en este Juzgado, con responsabilidad personal subsidiaria, en caso de impago, de un día de privación de libertad por cada dos cuotas diarias no satisfechas. Asimismo y en concepto de responsabilidad civil, deberá indemnizar a la denunciante con la cuantía de 258'45 euros”.

¹⁵² Dato extraído del Informe *Digital In 2019*, elaborado por We Are Social en colaboración con Hootsuite.

certificación del programa *TRUSTe*, que, como señalaba, garantiza que se cumplan las políticas y prácticas de privacidad y seguridad en la red. Lo que no quita para que Facebook, como señala en su política de privacidad, “colaboramos con nuestros socios que nos ayudan a proporcionar y mejorar nuestros productos, o que utilizan las herramientas para empresas de Facebook con el propósito de hacer crecer su negocio. Gracias a ellos, podemos gestionar nuestras empresas y proporcionar servicios gratuitos a personas de todo el mundo. No vendemos tus datos a nadie ni lo haremos en el futuro. Del mismo modo, imponemos estrictas restricciones sobre la manera en que nuestros socios pueden utilizar y divulgar los datos que proporcionamos. Estos son los tipos de socios externos con los que compartimos información”¹⁵³.

El TJUE declaró en su sentencia C-362/14, de 6 de octubre de 2015, caso *Maximillian Schrems v. Data Protection Commissioner*, que Estados Unidos no garantiza un nivel de protección adecuado de los datos personales transferidos por los ciudadanos europeos. El fallo se produjo a raíz de la denuncia de un ciudadano austríaco, Maximilliam Schrems, usuario de Facebook desde 2008. Hay que destacar, como reconoce la sentencia, que “toda persona residente en el territorio de la Unión que desee utilizar Facebook está obligada a concluir en el momento de su inscripción un contrato con Facebook Ireland, filial de Facebook Inc., domiciliada ésta última en Estados Unidos. Los datos personales de los usuarios de Facebook Ireland residentes en el territorio de la Unión se transfieren en todo o en parte a servidores pertenecientes a Facebook Inc, situados en el territorio de Estados Unidos, donde son objeto de tratamiento” (Punto 27). Por dicho motivo, Schrems presentó una reclamación en la que solicitaba que “se prohibiera a Facebook Ireland transferir sus datos personales a Estados Unidos. Alegaba que el Derecho y las prácticas en vigor en este último país no garantizaban una protección suficiente de los datos personales conservados en su territorio contra las

¹⁵³ *Política de Privacidad de Facebook*. Disponible en: <https://www.facebook.com/privacy/explanation>. En la que reconocen que ofrecen a sus anunciantes “informes para indicarles qué tipos de personas ven sus anuncios y qué resultados generan. No obstante, a menos que nos des permiso para hacerlo, no compartimos información que te identifique personalmente, como tu nombre o dirección de correo electrónico; datos que se puedan emplear para ponerse en contacto contigo o que puedan revelar tu identidad. Proporcionamos a los anunciantes datos demográficos generales e información sobre intereses. Estos datos tienen como fin ayudarlos a conocer mejor su público. También confirmamos qué anuncios de Facebook te han llevado a efectuar una compra o realizar una acción con un anunciante”.

actividades de vigilancia practicadas en él por las autoridades públicas, haciendo referencia en ese sentido a las revelaciones del Sr. Edward Snowden sobre las actividades de los servicios de información de Estados Unidos, en particular las de la NSA” (Punto 28).

El TJUE estima que la existencia de una Decisión de la Comisión que “declara que un país tercero garantiza un nivel de protección adecuado de los datos personales transferidos no puede dejar sin efecto ni limitar las facultades de las que disponen las autoridades nacionales de control en virtud del artículo 8.3, de la Carta de Derechos Fundamentales de la Unión Europea y por el artículo 28 de la Directiva 95/46/CE” (Punto 53). Por tanto, “las autoridades nacionales de control, a las que una persona haya presentado una solicitud de protección de sus derechos y libertades frente al tratamiento de datos personales que la conciernen, deben poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencias establecidas por la referida Directiva” (Punto 57).

Por último, sobre la protección del derecho fundamental al respeto de la vida privada al nivel de la Unión, el TJUE “exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario, considerando que lo estrictamente necesario no se limita a una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización” (Puntos 92 y 93).

En cuanto a los menores, Facebook, en el año 2010, subió la edad mínima para registrarse en España de los 13 a los 14 años, como establece la legislación española, ya que, hasta ese momento, la multinacional tenía fijado en 13 años el mínimo de edad, en virtud de la legislación norteamericana. Aunque este aumento de la edad fue un pequeño paso, siguen sin articular mecanismos que garanticen la veracidad del dato proporcionado. La única recomendación que dan a los usuarios es, si son menores de 14

años, no se intenten registrar porque si lo descubren, borrarán la información facilitada. Por lo tanto, en muchos casos hay menores con su perfil navegando por la red, aportando información de carácter personal sin ser conscientes de los problemas y peligros que esto puede desencadenar.

El ciberespacio lo que añade, según apunta Villaverde, es “justamente la inexistencia de espacio físico y de tiempo: la circulación de la información, de datos, la comunicación interpersonal, todo tiene lugar en un espacio inexistente y sin límites temporales. Un lugar donde el *netizen* no es persona en su sentido corpóreo y físico, sino datos e información que circulan de manera irrestricta en el espacio y el tiempo. Esta ausencia de barreras físicas para el ejercicio de los derechos fundamentales es relevante para ciertos derechos donde los límites de espacio y tiempo de su ejercicio constituyen factores que controlan y reducen los riesgos de daño a terceros. El ciberespacio hace incontrolable, incluso para el propio individuo ejerciente de sus derechos, la dimensión espacial y temporal de ese ejercicio y de quienes soportan ese ejercicio, elevando el grado de riesgo de efectos dañosos”¹⁵⁴.

Este ciberespacio ha creado nuevos delitos, el ciberacoso¹⁵⁵ al que cada vez más jóvenes tienen que enfrentarse y que pasa desapercibido por la privacidad que las redes sociales

¹⁵⁴ VILLAVERDE MENÉNDEZ, I. (2007). *Ciberconstitucionalismo. Las TIC... ob. cit.*, pág. 35. Puede verse también en AGUIRRE ROMERO, J. M^a. (2004). Ciberespacio y comunicación. Nuevas formas de vertebración social en el siglo XXI. *Espéculo. Revista de Estudios Literarios* n°27; y ARBELÁEZ-GIRALDO, A. (2017). El ciberespacio y el problema de la realidad virtual. *Revista de Filosofía UIS* n°16 (2).

¹⁵⁵ Este término fue definido por MASON, K. L. (2008). Cyberbullying: A preliminary assessment for school personnel. *Psychology in the School*. Vol. 45, n°4, pág. 323; como “el uso de la información y comunicación a través de la tecnología que un individuo o un grupo utiliza deliberadamente y de manera repetida para el acoso o amenaza hacia otro individuo o grupo mediante el envío o publicación de texto cruel y/o gráficas a través de los medios tecnológicos”. La gran diferencia en comparación con el acoso tradicional está como apuntan SLONJE, R. y SMITH, P. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*. Vol. 49, pág. 148; “a diferencia de las formas tradicionales de acoso escolar, donde una vez que la víctima llega a casa, están lejos del acoso escolar hasta el día siguiente, con el ciberacoso, la víctima puede seguir recibiendo mensajes de texto o correos electrónicos donde sea que estén”. Véase también LI, Q. (2006). Cyberbullying in schools: A research of gender differences. *School Psychology International* n°27, págs. 157-170; e YBARRA, M. L. y

conceden a sus usuarios. El TS ha dado validez como prueba de un delito de abuso sexual a “los datos obtenidos por una madre de la cuenta abierta por su hija menor de edad en Facebook, a la que accedió sin contar con su permiso ante la sospecha de que la niña pudiera estar siendo víctima de un delito” {STS 5809/2015, de 10 de diciembre. Sala de lo Penal (nº de recurso 912/2015)}. El condenado había presentado un recurso de casación ante el TS, que declaró “no haber lugar, contra la Sentencia dictada por la Sección Segunda de la Audiencia Provincial de Tarragona, que le había condenado como autor responsable de un delito de abusos sexuales a un menor de trece años y cinco delitos continuados de exhibicionismo según el artículo 185 del Código Penal”.

Los motivos que alegaba el condenado para que se anularan como prueba los citados mensajes es que no había habido consentimiento de la menor y, por tanto, se había vulnerado el derecho a la intimidad entre los comunicantes, pero la sentencia establece que “no puede considerarse ilícita una prueba cuando la afectación a la intimidad proviene de un particular que está autorizado para acceder a ese ámbito de privacidad”, considerando que la madre está autorizada para acceder a ese ámbito de privacidad que desvela, aunque abuse de la confianza de su hija, afirmando que “no puede el ordenamiento hacer descansar en los padres unas obligaciones de velar por sus hijos menores y al mismo tiempo desposeerles de toda capacidad de control en casos como el presente en que las evidencias apuntaban inequívocamente en esa dirección” (FJ5).

3.1.3. El Registro del usuario de una red social, protección de la vida privada electrónica (y de la intimidad)

Para el registro al usuario en estas redes sociales, se le pide el nombre, el correo electrónico, el sexo y la fecha de nacimiento. Además, también se da la opción de facilitar otros datos, tales como centros educativos, empleo, universidad...; y puede que, a veces, se pida otro tipo de información adicional, bien sea por motivos de seguridad, bien por estar relacionado con la oferta de servicios específicos. Estos datos son sólo para registrarse como usuario. Sin embargo, el usuario puede configurar su perfil para ocultar todo o sólo una parte de los campos de información que ha cubierto, con el fin de que no los vean otros usuarios. En el caso de Facebook, los usuarios emplean su

MITCHELL, K. J. (2004). Online aggressor / targets, aggressors, and targets: a comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry* nº45, págs. 1308-1316.

propio nombre como perfil, para que sean más fáciles de localizar y de buscar a otros usuarios. Lo contrario sucede en Twitter, en donde la gente suele poner pseudónimos.

Una vez completada esta primera fase de datos, se puede seguir añadiendo información relacionada con el lugar de nacimiento, la ciudad de residencia, las aficiones e intereses. Además, también existe la opción de ampliar el contenido personal, ofreciendo la posibilidad de informar sobre las tendencias políticas y religiosas, que también serán abiertas a otros usuarios salvo que se indique lo contrario.

La visibilidad del perfil de usuario de una red social a otra puede variar. En algunas redes se pueden encontrar perfiles haciendo simplemente una búsqueda en Google, como por ejemplo Facebook o Twitter. Sin embargo, esto no es posible en Tuenti, ya que está totalmente cerrada a la gente registrada en la página web. Dependiendo de una red social u otra, los permisos que puede ver la gente por defecto pueden ser públicos o privados. Facebook tiene un enfoque diferente por defecto, los usuarios que forman parte de la misma subred pueden ver los perfiles de los demás, a menos que un perfil haya decidido denegar el permiso a los de su red.

La Comisión Europea ha pedido en varias ocasiones a las redes sociales que mejoren sus políticas de privacidad y seguridad, especialmente respecto a los menores. Así, la Confederación de Autoridades de Protección de datos de la Unión Europea, en concreto el grupo *Article 29 Data Protection Working Party*¹⁵⁶ ha denunciado en multitud de ocasiones las lagunas de Facebook en su política de privacidad. Uno de los aspectos en los que más han insistido estas asociaciones, en sus denuncias, está relacionado con que

¹⁵⁶ Este grupo se creó en virtud del artículo 29 de la directiva 95/46/CE. Se trata de un órgano consultivo independiente integrado por las Autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea y sus cometidos son: a) estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de dicha directiva con vistas a contribuir en su aplicación homogénea; b) emitir un dictamen destinado a la Comisión sobre el nivel de protección existente dentro de la Comunidad Europea y en terceros países; c) asesorar a la Comisión sobre cualquier proyecto de modificación de dicha directiva, cualquier proyecto de medidas adicionales o específicas que deban adoptarse para salvaguardar los derechos y libertades de las personas físicas en lo que respecta al tratamiento de datos personales, así como sobre cualquier otro proyecto de medidas comunitarias que afecte a dichos derechos y libertades; y d) emitir un dictamen sobre los códigos de conducta elaborados a escala comunitaria.

la información del usuario registrado en esta red social “aparezca destacado en los resultados de las búsquedas, si el usuario no lo modifica expresamente, ya que dicho acceso iría más allá de la esfera personal”¹⁵⁷. Por eso, se ha exigido a Facebook que cambie dicha configuración de suerte que no aparezca en los motores de búsqueda la información del registrado a menos que haya dado su consentimiento.

Por otro lado, el 29 de marzo de 2010, Facebook anunció que compartirá información personal de los usuarios con algunas webs asociadas para ofrecer una experiencia más personalizada, cuando “visitas o utilizas sitios web y aplicaciones de terceros que usan nuestros Servicios (por ejemplo, cuando ofrecen nuestro botón "Me gusta" o el inicio de sesión con Facebook, o cuando usan nuestros servicios de medición y publicidad). Dicha información incluye datos acerca de los sitios web y las aplicaciones que visitas, el uso que haces de nuestros Servicios en dichos sitios web y aplicaciones, así como datos que el desarrollador o el editor de la aplicación o del sitio web te proporciona a ti o a nosotros”¹⁵⁸. Esta información se ha ido recabando con los datos recogidos (aficiones, gustos) por la propia red social con el fin de ir acotando el público objetivo y ofrecer al cliente aquello que sea de su agrado. Aquí entrarían marcas comerciales como Adidas, Nike, Nintendo, Sony. Por otro lado, en relación con esto, es frecuente el uso de *cookies* para que la publicidad sea más personalizada. Hasta ahora, era necesaria una aprobación del usuario para conectar estas páginas web asociadas con la información registrada en Facebook. En este sentido, *Article 29 Data Protection Working Party* advierte a la red social de que no existe base legal para que se difundan datos personales a terceras personas o entidades, si no hay consentimiento por parte del usuario.

¹⁵⁷ Dictamen 5/2009, de 12 de junio, relativo a las redes sociales en línea. *Article 29 Data Protection Working Party*. Pág. 6. En dicho Dictamen se destaca también que “el acceso a los datos (perfil, archivos subidos a la red, textos) aportados por un usuario se limita a los contactos seleccionados por él mismo”. Sin embargo, en algunos casos, los usuarios pueden llegar a tener un gran número de personas de contacto, y de hecho puede darse el caso de que no conozca a algunos de ellos, aunque, como se señala, “un alto número de contactos puede ser una indicación para que no se aplique la exclusión a la normativa de protección de datos y se considere al usuario responsable de un fichero”. Véase también GILBERT, F. (2014). *Article 29 Working Party Supports European Court of Justice “Right to Be Forgotten” Rule*. *Computer & Internet Lawyer*. Vol. 31, nº8.

¹⁵⁸ Política de datos de Facebook. Disponible en: <https://www.facebook.com/privacy/explanation>

Del mismo modo, Facebook recopila información cuando se interactúa a través de la red, ya que desde la empresa se realiza un seguimiento de las acciones que se llevan a cabo (crear un álbum de fotos, enviar un regalo, asistir a un evento o conectarte a una aplicación). Pero, no sólo acceden a ese tipo de información, sino que cuando se accede a la red social desde un ordenador o teléfono móvil obtienen el tipo de navegador, la ubicación y dirección IP, así como las páginas que han sido visitadas.

Debido a las constantes quejas recibidas por Facebook, la red social decidió en noviembre de 2014 anunciar a sus usuarios que en enero de 2015 entraría en vigor una nueva política de privacidad, pero no es más que un lavado de imagen, ya que la compañía no modifica en ningún momento las restricciones de privacidad, si no que se encargará de ampliar el radio de actuación de sus aplicaciones y servicios, partiendo del uso de la situación GPS del *Smartphone* del usuario, recomendará los sitios más cercanos a su localización, una forma más de aumentar los ingresos y el control sobre el usuario.

Lejos de mejorar su política de privacidad, el estudio *Did you really agree to that? The Evolution of Facebook's Privacy Policy* revela que “las políticas de privacidad de Facebook en la última década son menos transparentes y resultan más difíciles de entender para los usuarios, incluyendo la opción sobre el uso de la información de cara a terceros”. Además, Facebook tendría que establecer “el uso que va a realizar de la información personal de los usuarios sin atentar contra su privacidad e informarles de si ciertos datos van a ser compartidos con terceros o se van a utilizar con fines publicitarios”¹⁵⁹. De los 33 criterios analizados, Facebook suspende en 22 de ellos. Una

¹⁵⁹ SHORE, J. y STEINMAN, J. (2015). *Did You Really Agree to That? The Evolution of Facebook's Privacy Policy*. Universidad de Harvard. Al respecto TELLO-DÍAZ, L. (2013). Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook. *Revista Comunicar*. Vol. XXI, nº41, pág. 206; es consciente de que “en la era de las nuevas tecnologías, los límites de la intimidad y la vida privada se han visto diluidos... Específicamente invasivas serán las técnicas empleadas para monitorizar la información obtenida en la red social Facebook, cuya arquitectura favorece la pérdida de control de la intimidad a través de la captación de pautas de comportamiento, el empleo de datos derivados de los perfiles, los cambios en la política de privacidad sin consentimiento y el reconocimiento facial”. Además, apunta que “la monetización de los datos personales es uno de los aspectos más controvertidos de Facebook, ya que implica no solo la revelación de información personal, sino el provecho económico de una información sustraída sin consentimiento expreso de sus propietarios... No hay olvidar que el perfil

clara muestra de que, en vez de mejorar, sus políticas de privacidad se han vuelto más opacas.

3.1.4. Desactivación y eliminación del perfil del usuario, protección de la vida privada electrónica (y de la intimidad)

Igualmente, cuando los usuarios de las redes sociales quieren eliminar definitivamente su cuenta, ésta no queda totalmente eliminada. En Facebook se da la oportunidad de desactivar o eliminar la cuenta de usuario. En el primer caso, ningún usuario podrá verla, pero se guardará la información del perfil durante un plazo de 14 días por si se decide volver a activarla. Si por el contrario, la intención es eliminarla, se borra de forma permanente de una manera sencilla. Primeramente, la cuenta se desactiva y se eliminará de forma permanente, siempre y cuando el usuario no entre en la cuenta durante ese periodo. Cuando se quiere eliminar una cuenta¹⁶⁰, se borra de forma permanente de Facebook, pero pueden permanecer en Internet copias visibles de dicha información, en la medida que se haya compartido con otros usuarios. Es decir, si existen imágenes en las que el usuario aparece, seguirán estando ahí, con la única salvedad de que, en vez de poner el nombre de la persona, aparecería catalogado como usuario de Facebook anónimo.

A su vez, en el caso de que el usuario haya facilitado a otros sitios web acceso a su información, éstos pueden conservar la información hasta el límite permitido por sus propios términos de servicio o políticas de privacidad. El problema, por tanto, no se produce cuando un usuario da de baja su cuenta en una red social, sino cuando esa información ha pasado de una red a otra, y ha traspasado muchas fronteras tecnológicas y geográficas.

en las redes sociales es el carnet de identidad del usuario, su información es de carácter privado y en consecuencia confidencial, si no existe consentimiento por parte del interesado. Sin embargo, la confidencialidad de los datos contenidos en el perfil se ha diluido, convirtiéndose en reclamo para las empresas”, pág. 209.

¹⁶⁰ Facebook se permite conservar cierta información para evitar el robo de identidades y otras conductas inadecuadas, a pesar de haberse solicitado la eliminación. También se crearán unas copias de seguridad, en las que la información eliminada y borrada puede permanecer en estas copias hasta un máximo de 90 días, pero no estará disponible para los demás.

Pero, esto no sucede con todas las redes sociales. Por ejemplo, en el caso de la red española Tuenti, desde su equipo gestor se asegura que cuando el usuario cancela su perfil, se borra por completo todo el rastro de la persona que lo ha eliminado. El nivel de exigencia no es el mismo en todas las redes sociales, y depende en gran medida de la legislación que en materia de protección de datos tenga el país donde está localizada la sede central de la red, ya que hay países que tienen una legislación más restrictiva que otros.

3.1.5 Regulación de los criterios sobre vida privada en las redes sociales

Ha quedado de manifiesto que existe un amplio vacío (cesión de información a páginas web asociadas, saturación de datos personales en Internet, inclusión en la red de información recopilada a través de software descargado, impunidad con la identificación de los menores) en lo que a políticas de privacidad se refiere en las redes sociales. Por este motivo, cada vez son más frecuentes los estudios e informes¹⁶¹ que se están realizando al respecto para abordar, en la medida de lo posible, cuáles son los mejores pasos a seguir para lograr el mayor grado posible de regulación de la privacidad. Uno de los últimos estudios, elaborado conjuntamente por la Agencia Española de Protección de Datos (AEPD)¹⁶² y El Instituto Nacional de Tecnologías de la Información (INTECO)¹⁶³, advierte sobre los riesgos para la privacidad y seguridad en redes sociales y sugiere mejoras en los sistemas de protección de los usuarios. Entre los aspectos que el estudio considera más importantes para abordar con la mayor garantía este tema se encuentran¹⁶⁴:

¹⁶¹ Guía sobre seguridad y privacidad de la tecnología, mayo 2010, realizada por la AEPD e INTECO; Informe de la AEPD 2004-0582 “Subcontratación de un encargado del tratamiento en tercer país que no ofrece nivel adecuado de protección”; Informe de la AEPD 2003-0101 “Cumplimiento de la LOPD como requisito previo a la transferencia”; e Informe de la AEPD 2001-0000 “Transferencias internacionales de datos para la realización de un tratamiento por cuenta del responsable del fichero”.

¹⁶² La AEPD es un ente de Derecho Público con personalidad jurídica propia y plena capacidad pública y privada, actúa con independencia de las Administraciones Públicas en el ejercicio de sus funciones.

¹⁶³ El INTECO está comprometido con la promoción de servicios de la Sociedad de la Información cada vez más seguros, que protejan los datos personales de los interesados, su intimidad, la integridad de su información y eviten ataques que pongan en riesgo los servicios prestados. Y, por supuesto, que garanticen un cumplimiento estricto de la normativa legal en materia de Tecnologías de la información y comunicación (TIC).

¹⁶⁴ *Estudio sobre la privacidad de los datos personales... ob. cit.* (2009), págs. 126-132.

- Redacción de condiciones de uso y políticas de privacidad con un lenguaje comprensible, para que cualquier tipo de usuario tenga claros sus derechos y obligaciones.
- Control de la indexación y almacenamiento de los perfiles por parte de los buscadores.
- Cambios en la configuración del nivel de privacidad, de forma que se establezca, por defecto, el máximo grado de seguridad en el perfil del usuario, ya que permiten por defecto la máxima difusión de información del usuario.
- Puesta a disposición del usuario de herramientas que le otorguen el control absoluto de la información que publica en la red; es decir, medios que limiten la posibilidad de etiquetar a otros usuarios en la red¹⁶⁵.
- Implantación de sistemas que faciliten la comprobación de la edad de los usuarios que intenten acceder al servicio¹⁶⁶.
- No publicación en los perfiles de excesiva información personal y familiar (ni datos que permitan la localización física), con especial cuidado a la hora de alojar contenidos gráficos y configurar cuidadosamente el grado de privacidad del perfil de usuario en la red social.
- No aceptación de solicitudes de contacto de forma descontrolada, sino únicamente de personas conocidas o con las que haya relación previa.

¹⁶⁵ La AEPD aboga por que antes de etiquetar a otro usuario, se reciba automáticamente una solicitud de aceptación o rechazo para confirmar si se permite a ese usuario que incluya el nombre de otro en una imagen.

¹⁶⁶ El objetivo de la Agencia Española de Protección de Datos es que se implanten sistemas que reduzcan los casos de suplantación de la identidad en los menores, bloqueando el acceso al usuario que utilizó el perfil de otro de forma ilegítima, y otros sistemas que detecten el nivel de seguridad de las contraseñas elegidas.

CAPÍTULO 4. EL DERECHO AL OLVIDO, UN PROBLEMA GLOBAL

4.1. EL DERECHO AL OLVIDO EN EUROPA

4.1.1. Francia, un referente en el derecho al olvido

Francia se ha convertido en un referente del derecho al olvido. No sólo por la aprobación de la Ley para una República Digital que garantiza a los usuarios el derecho a la muerte digital sino porque en mayo de 2009, el Senado presentaba el *Rapport d'information relatif au respect de la vie privée à l'heure des mémoires numériques* en el que reconoce el derecho al olvido. “Una pérdida de memoria destinada a proteger al individuo de su pasado, convirtiéndolo en el único archivero de su historia personal. El derecho al olvido pone en servicio la destrucción de datos y permite un anonimato irreversible. De todas maneras, la legislación relativa a la protección de datos personales se convierte en gran medida irrelevante para responder a los retos planteados por los motores de búsqueda de Internet. Además, la defensa del derecho al olvido no debe acarrear una pérdida de poder de los individuos ni significa que todo el mundo pueda escribir a voluntad su historia personal”¹⁶⁷. Por tanto, el desafío consiste en encontrar un equilibrio entre el derecho al olvido y la libertad de expresión e información. Eso sí, “garantizando el reconocimiento del derecho al olvido para actuar exigiendo la retirada de informaciones en los sitios webs y obligando a los buscadores a evitar la indexación de informaciones no deseadas. Lo que supone un notable paralelismo entre estas propuestas y la vía seguida por la AEPD para garantizar el derecho al olvido”¹⁶⁸. Una de las primeras sentencias dictadas en Europa contra Google fue la del *Tribunal de Grande Instance* de París, de 15 de febrero, en la que ordenaba al buscador “desindexar el nombre y apellidos de la señora Diana Z. de todos los enlaces pornográficos y borrar todos los resultados de búsqueda relacionados con ella en las direcciones www.google.com y www.google.fr”.

Hay autores, como Costaz, que son muy tajantes y consideran el derecho al olvido como un derecho fundamental, ya que “la afirmación de un derecho al olvido manifiesta el reconocimiento de los cambios del ser, porque el presente y el futuro no se reflejan en

¹⁶⁷ DÉTRAIGNE, Y., y ESCOFFIER, A. M. (2009). *Rapport d'information relatif au respect de la vie privée à l'heure des mémoires numériques*, pág. 104.

¹⁶⁸ RALLO LOMBARTE. A. (2014). *El derecho al olvido en Internet... ob. cit.*, pág. 192.

el espejo del pasado. Por lo tanto, la fuerza positiva en la vida afectiva y en la acción, el olvido aparece como una libertad fundamental del hombre y merece ser protegida por este derecho”¹⁶⁹. Desde la revolución francesa se aboga por el espíritu de las leyes y, como reconoce Terre, “el hambre que la libertad inspira es siempre emocionante y su discurso es más portador de espíritu que el silencio y la opresión. Además convendría no olvidar nunca que es un bien frágil que ha querido soplar la llama, aún a riesgo de apagarla”¹⁷⁰.

Al igual que sucede en España con la AEPD, en Francia, la CNIL¹⁷¹ es la agencia encargada de velar por los derechos de los ciudadanos en los temas relativos a la protección de datos. Su potestad fue reforzada por la Ley relativa a la protección de las personas físicas con respecto a los procesamientos de datos de carácter personal, de 6 de agosto de 2004. Pero anteriormente, como apunta García-Berrio, ante la existencia de diferentes tipos de informaciones nominativas que no estaban recogidas en la Ley 78/17 fue la CNIL la encargada de abordarlas, refiriéndose a “los datos manifiestamente nominativos, incluyendo aquí también aquellos ficheros considerados sensibles, y los datos indirectamente nominativos”. En referencia al ejercicio de los derechos de acceso a la información nominativa, “la CNIL estableció que el derecho de acceso se encuentra restringido en su ejercicio únicamente a las personas físicas que justifiquen su identidad y cuya demanda no hubiese sido motivada, especificando el amplio espectro de posibilidades para la determinación de la «duración de la puesta a disposición de la información»¹⁷² para el ejercicio concreto del derecho de comunicación”¹⁷³.

¹⁶⁹ COSTAZ, C. (1995). Le droit à l’oubli. *Gazette du Palais*, págs. 961-962.

¹⁷⁰ TERRE, F. (2002). *Libertés et droits fondamentaux*. Éditions Dalloz, pág. 6.

¹⁷¹ Fue creada por la Ley 78/17, de 6 de enero de 1978, relativa a la informática, archivos y libertades. Lo que la convierten en una de las más antiguas autoridades de control de la protección de datos personales. Su misión general es velar por el respeto de los derechos y las libertades de las personas, y asegurarse que los tratamientos de datos personales se conformen a las prescripciones de la Ley, vigilando muy de cerca las evoluciones de las tecnologías y las consecuencias que esas puedan tener para los derechos humanos, la vida privada, las libertades individuales o públicas.

¹⁷² Ley 78/17, de 6 de enero de 1978, modificado por la Ley 2004/801, de 6 de agosto de 2004. Artículo 35: “Los datos de carácter personal sólo podrán ser objeto de una operación de procesamiento por parte de un subcontratista, de una persona que actúa bajo la autoridad del responsable del procesamiento o de la del subcontratista, ante instrucción del responsable del procesamiento. Toda persona que procese datos de carácter personal por cuenta del responsable del procesamiento será considerado como subcontratista

El *Tribunal de Grande Instance* de París dictó una sentencia, siguiendo la doctrina de la STJUE sobre derecho al olvido, en la que obligaba a eliminar los enlaces de Google no sólo en el dominio francés sino en todo el mundo, siendo la primera sentencia al respecto en Europa. Los denunciantes exigían la retirada a Google de un enlace a una página de Facebook, vinculado con su nombre y apellidos, en la que aparecían informaciones difamatorias. La sentencia reconoce que “Google Inc. es sin duda el operador del motor de búsqueda y Google Francia es una filial al 100%, que se dedica a la promoción y venta de espacios publicitarios en relación con los términos de búsqueda, utilizando el motor de la tecnología de Google Inc, y garantiza, a través de la actividad que despliega, la financiación del motor de búsqueda”. Por eso, a raíz de la sentencia del TJUE de 13 de mayo de 2014, se considera que “una filial de Google Inc. en un Estado miembro de la Comunidad Europea es su representante en el Estado del que se trate y que las actividades del operador del motor de búsqueda y las de su filial en el Estado miembro de que se trate están estrechamente vinculadas”¹⁷⁴. El Tribunal decidió fallar a través de los denunciantes, obligando a Google a pagar 1.500 euros de indemnización y 1.000 euros más por cada día que los enlaces siguiesen accesibles, con un periodo máximo de dos meses para borrar por completo los enlaces.

El CNIL también se ha pronunciado al respecto y ha decidido sancionar a Google, obligándole a que se retiren los enlaces en todas sus versiones y para todos los usuarios no sólo para los dominios del país en el que se pone la reclamación. Después de varios meses de conflicto, la presidenta del CNIL, Isabelle Falque-Pierrotin, decidió rechazar los recursos de Google al considerar que “las extensiones geográficas son sólo caminos que dan acceso a la operación de procesamiento de datos. Una vez que la exclusión del

en el sentido de la presente ley. El subcontratista deberá presentar garantías suficientes para asegurar la aplicación de las medidas de seguridad y confidencialidad mencionadas en el artículo 34. Esta exigencia no liberará al responsable del procesamiento de su obligación de velar por el cumplimiento de estas medidas. El contrato que vincule al subcontratista con el responsable del procesamiento comprenderá la indicación de las obligaciones que incumben al subcontratista en materia de protección de la seguridad y de la confidencialidad de los datos y preverá que el subcontratista sólo podrá actuar ante instrucción del responsable del procesamiento”.

¹⁷³ GARCÍA-BERRIO HERNÁNDEZ, T. (2003). *Informática y libertades. La protección de datos personales y su regulación en Francia y España*. Colección Estudios de Derecho. Universidad de Murcia, págs. 401-405.

¹⁷⁴ *Tribunal de Grande Instance* de París, 16 de septiembre de 2014.

enlace es aceptada por el motor de búsqueda, se debe implementar en todas las extensiones, de conformidad con la sentencia del Tribunal de Justicia. Si este derecho se limita sólo a algunas extensiones, sería suficiente buscar en otra extensión con el fin de encontrar el resultado retirado de la lista, es decir, utilizar otra forma de acceso al tratamiento. Esto supondría quitar la eficacia de este derecho. En cualquier caso, el derecho a la exclusión de enlaces la lista nunca lleva a la supresión de la información en Internet, ya que se limita a evitar algunos de los resultados que se muestran después de una búsqueda. Por lo tanto, la información sigue siendo directamente accesible en la página web de origen o a través de una búsqueda con otros términos. Además, este derecho no es absoluto, al tener que conciliarse con el derecho de información público, en particular cuando el interesado sea una persona pública. Por último, contrariamente a lo que Google ha indicado, esta decisión no muestra ninguna voluntad por parte de la CNIL para aplicar extraterritorialmente la legislación francesa. Simplemente pide la plena observancia de la legislación europea por los jugadores no europeos que ofrecen sus servicios en Europa”¹⁷⁵.

En un contexto que mete en juego intereses contradictorios entre la privacidad y el derecho al olvido es necesario, como expone Boizard, definir el derecho al olvido como “un fenómeno físico natural. En consecuencia, querer definir un derecho al olvido, es tratar de dar un sentido jurídico a una noción física. Cuando el jurista considera una aplicación de un derecho al olvido digital se plantea una contradicción: recurre a un instrumento jurídico para alcanzar un resultado físico, resultado que la tecnología está destinada a combatir. De una manera tradicional, el derecho al olvido, tal como se ha considerado en los años 1960, reenvía a una realidad muy precisa. Se trata de un olvido impuesto con el objetivo de garantizar la paz social y el orden público. Es el caso en particular de las normas relativas a la prescripción de la acción civil o de la acción pública. Todo hecho prescrito no puede dar lugar a un enjuiciamiento o condena. En este marco, la elección de plazos de prescripción parece ser más una elección de la sociedad que de la protección de un derecho de la persona”¹⁷⁶. El derecho al olvido

¹⁷⁵ *Right to delisting: Google informal appeal rejected*. 21 de septiembre de 2015. Disponible en : <https://www.cnil.fr/fr/node/15814>.

¹⁷⁶ En este sentido, SELIGRAT GONZÁLEZ, V. M. (2015). El derecho al olvido digital. Problemas de configuración jurídica y derivados de su incumplimiento a la vista de la STS de 15 de octubre de 2015. *Actualidad Civil* nº12. Editorial La Ley. Diciembre, pág. 6; señala que “una vez transcurrido este tiempo

corresponde, por lo tanto, al derecho de respetar estas normas y aparece como un hecho objetivo”. Actualmente, la noción de derecho al olvido “se define esencialmente por su finalidad: se trata de eliminar cualquier riesgo que una persona, cuyos datos estén circulando en la red, por ella misma o por un tercero, sean permanentemente incómodos por la utilización de sus datos sin su conocimiento y, sea cual sea la antigüedad de los hechos o de los datos relativos a esta persona. Cabe subrayar, para aproximar los dos derechos, que al igual que el derecho a la vida privada se define por su finalidad. Cuando se invoca el derecho al olvido, se está reivindicando una prerrogativa que podría exigir el individuo que ciertos datos o acontecimientos concernientes al mismo que no sean de actualidad no sean accesibles nunca más. Es una sustracción de la memoria colectiva, pero no se trata de una sustracción total. En consecuencia si un derecho al olvido debe consagrarse, no lo será de forma absoluta”¹⁷⁷.

Lo que queda claro es que el derecho al olvido digital “limita la visión de una sociedad que detecta inmediatamente los actos perjudiciales de los individuos y de las instituciones que se aplica igualmente y hace que se formen las normas de *facto* (pero no de derecho) conforme a las reglas”¹⁷⁸ y supone “un cambio de paradigma, permitiendo el desarrollo de una memoria digital perfecta. Esta revolución digital ha operado un derrocamiento del equilibrio memoria/olvido. Por tanto, la exposición a una conservación atemporal de cualquier trazo que dejase en la memoria digital es, basándonos, en la reaparición intempestiva y dañable de una información que había caído en el olvido. Dicho de otra manera, la revolución digital no ha alterado el mecanismo del olvido, pero sí la efectividad del olvido. Lo que es preocupante son las consecuencias que se pueden derivar del desajuste del pasado vivido o percibido y el pasado digital: si el pasado del que nosotros recordamos cambia y evoluciona sin cesar, esto queda inscrito en la memoria digital que es fija en el tiempo”¹⁷⁹.

en virtud del cual la recogida de datos ha dejado de cumplir con la finalidad informativa inicial, se podrá seguir ejercitando el derecho a la información pero el mismo deberá estar limitado a dar divulgación del hecho noticioso, de manera que no podría aludirse a los sujetos objeto de noticia”.

¹⁷⁷ BOIZARD, M. (2015). *Le droit à l'oubli*. Faculté de droit et de science politique. Rennes, págs. 12-13.

¹⁷⁸ KAPLAN, D. (2010). *Informatique, libertés, identité*. Éditions Fyp, pág. 44.

¹⁷⁹ QUILLET, E. (2011). *Le droit à l'oubli numérique sur les réseaux sociaux*. Université Panthéon-Assas, pág. 8.

4.1.2. Italia apuesta por el principio de finalidad

Para el *Garante per la Protezione dei Dati Personali* –que ya en 2004¹⁸⁰ resolvió un caso de derecho al olvido basándose en el principio de finalidad¹⁸¹, como señala Simón, el derecho al olvido actuaría “como un instrumento que persigue el efectivo cumplimiento del principio de finalidad, que exige que los datos personales tan sólo se pueden utilizar para la finalidad concreta por la cual fueron registrados, y una vez ya no son necesarios a tal efecto se puede producir su cancelación”. La diferencia con la doctrina de la AEPD reside en “el hecho de que el Garante tutela la solicitud de los afectados en relación con el medio de comunicación, al que exige el deber de contextualización o actualización de la noticia, sin llegar a estimar tutelas de derechos frente a los buscadores de Internet. Lo contrario que la AEPD que ha mantenido una postura deferente con los medios de comunicación por jugar un papel clave en la opinión pública libre y sólo les ha recomendado el uso de protocolos de exclusión”¹⁸².

La sentencia de la Corte Suprema de Casación 5525/2012, de 5 de abril de 2012, sección civil Tercera, viene a reafirmar la teoría establecida por el *Garante* al considerar que “el titular del órgano de la información (en este caso, *Il Corriere della Sera*) almacena dicha información en Internet está sujeto a los criterios de proporcionalidad, necesidad, pertinencia, teniendo en cuenta la finalidad que permite el tratamiento legítimo para asegurar la contextualización y la actualización de las noticias de prensa que hayan sido objeto de información y tratamiento, protegiendo el derecho de la persona, a la que los datos se refieren, a su identidad moral o a su proyección social, así

¹⁸⁰ Decisión del *Garante* sobre el recurso *Reti telematiche e Internet - Motori di ricerca e provvedimenti di Autorità indipendenti: le misure necessarie a garantire il c.d. “diritto all'oblio”* (doc-web: 1116068), de 10 de noviembre de 2014.

¹⁸¹ *Codice in materia di protezione dei dati personali*, de 30 de junio de 2003. **Artículo 11:** “**1.** Los datos personales objeto de tratamiento serán: a) tratados de manera legal y justa; b) recogidos y registrados para fines determinados, explícitos y legítimos, y si son utilizados en otras operaciones de procesamiento ha de hacerse en términos compatibles con dichos fines; c) exactos y, cuando sea necesario, actualizados; d) adecuados, pertinentes y no excesivos para los fines para los que fueron recogidos o sucesivamente tratados; e) almacenados en una forma que permita la identificación de los datos por un período de tiempo no superior al necesario para los fines para los que fueron recogidos o sucesivamente tratados. **2.** Los datos personales tratados que violen las normas que rigen el tratamiento de datos personales no podrán ser utilizados”.

¹⁸² SIMÓN CASTELLANO, P. (2015). *El reconocimiento del derecho... ob. cit.*, págs. 229-230.

como para salvaguardar la proyección social de la identidad personal, la necesidad del sujeto de estar protegido de la divulgación de información (potencialmente) perjudicial debido a la pérdida de la actualidad de la misma, de modo que el tratamiento relativo ya no esté justificado e incluso sea susceptible de obstaculizar al sujeto en la explicación y el disfrute de su propia personalidad”. En definitiva, el medio de comunicación tiene la obligación de integrar y actualizar en la noticia inicial, las nuevas noticias producidas con posterioridad a los hechos expuestos, eximiendo de responsabilidad a los motores de búsqueda, con el fin de que los ciudadanos tengan el derecho a recibir una información completa y justa.

Es interesante observar, como apunta Gerardo, que Corte Suprema de Casación no declaró “la cancelación de la noticia sino más bien la contextualización y actualización de la noticia por el propietario del sitio web. Debido a que una noticia obsoleta no es una noticia verdadera. Este es un aspecto muy importante, ya que la noticia aparecida en la web no dura, como las de la prensa escrita, una mañana, un día, una semana, sino que permanece de forma duradera e imborrable y cualquiera puede leerla y releerla, dondequiera que se encuentren en el mundo, y puede utilizarla como fuente de información”. Y añade que “la noticia no es un resumen de los datos a merced de todos, ya que afecta a la persona y a su imagen en un momento histórico determinado, además, vale la pena recordar que los datos personales son una parte de la expresión de la personalidad del individuo. Por tanto, se le debe permitir a la persona para proteger su identidad poder pedir el derecho al olvido de lo que ya no es parte de su identidad personal y al derecho a la contextualización de sus datos, ya que una verdad obsoleta no es una verdad”¹⁸³.

¹⁸³ GERARDO, S. (2015). Dall’Habeas Corpus all’Habeas Data: il diritto all’oblio ed il diritto all’anonimato nella loro dimensione costituzionale. *Diritto Civile e Commerciale*, págs. 21-22. Por su parte, ALLEGRI, M. R. (2018). Diritto all’oblio, tutela della web reputation individuale e “eccezione giornalistica”: spunti giurisprudenziali. *Forum di Quaderni Costituzionali*, pág. 5; considera que esta sentencia lo que hace es generar “un derecho a contextualizar la información al presuponer que cualquiera que maneje un archivo en línea debe implementar un sistema de actualización constante de todos sus contenidos con la intención de que las personas no vean distorsionada su imagen social”; y MEZZANOTTE M. (2009). *Il diritto all’oblio. Contributo allo studio della privacy storica*. Edizioni Scientifiche Italiane.

Con anterioridad al *Codice in materia di protezione dei dati personali*, en Italia se había aprobado el *Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica* que estableció los criterios básicos entre el derecho a la información y los datos personales, exponiendo que: “en la recogida de datos de carácter personal que revelen el origen racial o étnico; creencias religiosas o filosóficas; opiniones políticas; pertenencia a sindicatos, asociaciones u organizaciones religiosas, filosóficas, políticas o sindicales; el estado de salud y la esfera sexual, el periodista garantiza el derecho a la información sobre asuntos de interés público, en comparación con la información esencial, evitando referencias a familiares u otras personas que no están implicadas en los hechos”¹⁸⁴. Por otro lado, considera información esencial aquella “de interés público que no entre en conflicto con el respeto a la vida privada cuando la información resulte indispensable u original en las formas en que se produjo; así como la calificación de los protagonistas. La privacidad de las personas que desempeñan funciones públicas debe ser respetada si las noticias o los datos no tienen nada que ver con su función o su vida pública” (artículo 6). Por último, también contempla la protección de los menores, exigiendo al periodista que “no publique los nombres de los menores involucrados en hechos noticiosos, ni proporcionar detalles capaces de llevar a su identificación. La protección del menor se extiende, dada la calidad de las noticias, a los hechos que no son específicamente delitos. El derecho del niño a la intimidad siempre debe primar sobre la crítica y la prensa, pero, sin embargo, si por razones de interés público de primer orden y con sujeción a los límites legales, el periodista decide difundir noticias o imágenes de menores, debe aceptar su responsabilidad de evaluar si la publicación es realmente de interés, de acuerdo con los principios y límites establecidos por la Carta de Treviso” (artículo 7).

En Italia también se aprobó un código para el tratamiento de datos personales con fines históricos (*Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici*). Su objetivo es asegurar que “el uso de los datos personales obtenidos en el ejercicio de la libertad de investigación histórica y el derecho a la educación y la información, así como en el acceso a los registros y documentos, respetarán los derechos, las libertades fundamentales y la dignidad de las personas interesadas, en

¹⁸⁴ *Codice di deontologia relativo al trattamento dei dati personali nell'esercizio dell'attività giornalistica*, de 29 de julio de 1998. Artículo 5.1.

particular el derecho a la intimidad y el derecho a la identidad personal”. Este código contiene “las disposiciones para el procesamiento de datos personales con fines históricos en relación con los documentos conservados en los archivos de las administraciones públicas, organismos públicos y privados declarados archivos de interés histórico”¹⁸⁵.

4.2. IBEROAMÉRICA, UN ABANICO DE LEYES Y RESOLUCIONES

Debido a la falta de una normativa común como sucede en Europa con la Directiva 95/46/CE y, hasta la entrada en vigor del nuevo Reglamento (UE) 2016/679, de 27 de abril, los países iberoamericanos empezaron a contemplar el derecho al olvido, sin saberlo, mucho antes que en Europa con la inclusión de los derechos de oposición y cancelación en el tratamiento de los datos personales. Además, adaptar la STJUE generaría algunos problemas en Iberoamérica, ya que, como señala Bertoni, “siguiendo el artículo 13 de la Convención Americana de Derechos Humanos¹⁸⁶, que prohíbe la censura previa y dispone controles posteriores proporcionales, no sería un trabajo sencillo adoptar el enfoque del derecho al olvido como el que se propone en esta

¹⁸⁵ *Codice di deontologia e di buona condotta per i trattamenti di dati personali per scopi storici*, de 5 de mayo de 2001. Artículo 1.

¹⁸⁶ Convención Americana de Derechos Humanos, de 22 de noviembre de 1969. Artículo 13: “1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: a) el respeto a los derechos o a la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas. 3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones. 4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2. 5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional”.

sentencia europea”. De ahí que considere que “para los países Latinoamericanos, que son parte de la Convención citada, la decisión del TJUE debería ser tomada sólo como un antecedente dictado en un contexto diferente y sobre la base de normativa diferente”¹⁸⁷.

El primer país en tomar medidas al respecto fue Brasil, que ya lo contempló en 1990, en su Código de Defensa del consumidor¹⁸⁸. Además, en abril de 2014 aprobó el Marco Civil de Internet, una ley cuyo objetivo es definir y proteger los derechos civiles, garantías y obligaciones de los usuarios en Internet, reconociendo que “en cualquier operación de recolección, almacenamiento, protección o tratamiento de registros, datos personales o de comunicaciones por proveedores de conexión y de aplicaciones de internet en las que por lo menos uno de estos actos ocurra en territorio nacional, deberá ser obligatoriamente respetada la legislación brasilera, los derechos a la privacidad y a la protección de los datos personales y al secreto de las comunicaciones privadas y de los registros”¹⁸⁹.

¹⁸⁷ BERTONI, E. (2014). *Derecho al olvido: ¿es problemática la decisión del Tribunal de Justicia de la Unión Europea para América Latina?* Disponible en: <http://ebertoni.blogspot.com.es/2014/05/derecho-al-olvido-es-problematica-la.html>.

¹⁸⁸ Ley 8078/90, de 11 de septiembre. Art. 43: “1. Las estadísticas y datos de consumidores deben ser objetivos, claros, verdaderos y en lenguaje de fácil comprensión, no pudiendo contener informaciones negativas referentes a un periodo superior a cinco años. 2. La apertura de la estadística, ficha, registro y datos personales deberá ser comunicada por escrito al consumidor, cuando no haya sido solicitada por él. 3. El consumidor, siempre que encontrare inexactitudes en sus datos y estadísticas, podrá exigir su inmediata corrección, debiendo el archivador, en el plazo de cinco días hábiles, comunicar la alteración a los eventuales destinatarios de las informaciones incorrectas. 4. Los bancos de datos y estadísticas relativas a consumidores, los servicios de protección al crédito y similares son considerados entidades de carácter público 5. Consumada la prescripción relativa al cobro de deudas al consumidor, los Sistemas de Protección al Crédito no proveerán ninguna información que pueda impedir o dificultar el nuevo acceso al crédito a los proveedores. 6. Toda la información mencionada en el encabezamiento de este artículo se pondrá a disposición en formatos accesibles, incluso para las personas con discapacidad a petición del usuario”.

¹⁸⁹ Artículo 11. Ley PLC 21/2014, *Marco Civil da Internet*, de 22 de abril.

Los casos chilenos¹⁹⁰ y uruguayos¹⁹¹ resultan más concretos, ya que ponen prescripción a los datos en sus leyes sobre Protección de datos personales. Algunos años más tardó México¹⁹² en regular el derecho al olvido, reconociendo que los datos han de ser cancelados cuando dejen de ser necesarios, sin llegar a fijar un plazo establecido para su cancelación. Por su parte, en Perú¹⁹³, se han establecido una serie de principios para la administración de los datos, con el fin de interpretar y aplicar la ley.

¹⁹⁰ Ley 19628/1999, de 28 de agosto, sobre Protección de la vida privada. Artículo 18: “En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible. Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal. Con todo, se comunicará a los tribunales de Justicia la información que requieran con motivo de juicios pendientes”.

¹⁹¹ Ley 17838/04, de 8 de septiembre, de Protección de datos personales para ser utilizados en informes comerciales y acción de habeas data. Artículo 9: “Los datos personales relativos a obligaciones de carácter comercial solo podrán estar registrados por un plazo de cinco años contados desde su incorporación. En caso que al vencimiento de dicho plazo la obligación permanezca incumplida, el acreedor podrá solicitar al titular de la base de datos, por única vez, su nuevo registro por otros cinco años. Este nuevo registro deberá ser solicitado en el plazo de treinta días anteriores al vencimiento original. Las obligaciones canceladas o extinguidas por cualquier medio, permanecerán registradas, con expresa mención de este hecho, por un plazo máximo de cinco años, no renovable, a contar de la fecha de la cancelación o extinción”.

¹⁹² Ley Federal de Protección de datos personales en posesión de los particulares, 5 de julio de 2010. **Artículo 11:** “El responsable procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados. Cuando los datos de carácter personal hayan dejado de ser necesarios para el cumplimiento de las finalidades previstas por el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados. El responsable de la base de datos estará obligado a eliminar la información relativa al incumplimiento de obligaciones contractuales, una vez que transcurra un plazo de setenta y dos meses, contado a partir de la fecha calendario en que se presente el mencionado incumplimiento”.

¹⁹³ Ley por la cual se dictan las disposiciones generales del habeas data y se regular el manejo de la información contenido en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y las provenientes de terceros países, de 31 de diciembre de 2008. Artículo 4: “Principios de la administración de datos. a) Principio de veracidad o calidad de los registros o datos. La información contenida en los bancos de datos debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el registro y divulgación de datos parciales, incompletos, fraccionados o que induzcan a error. b) Principio de finalidad. La administración de datos personales debe obedecer a una finalidad legítima de acuerdo con la Constitución y la ley. La finalidad debe informársele al titular de la información previa o concomitantemente con el otorgamiento de la autorización cuando ella sea necesaria

La razón de ser del derecho al olvido en Iberoamérica, puede extraerse, como señala Puccinelli, “de lo sostenido en tiempos de la primera integración de la Corte Constitucional colombiana y bajo el epígrafe «La cárcel del alma y el derecho al olvido», cuando resolvió sobre la negativa de una entidad financiera a eliminar el dato de una deuda que fue declarada prescripta judicialmente”¹⁹⁴. La sentencia recoge que “las sanciones o informaciones negativas acerca de una persona no tienen vocación de perennidad y, en consecuencia después de algún tiempo tales personas son titulares de un verdadero derecho al olvido. Los datos tienen por su naturaleza misma una vigencia limitada en el tiempo la cual impone a los responsables o administradores de bancos de datos la obligación ineludible de una permanente actualización a fin de no poner en

o en general siempre que el titular solicite información al respecto. c) Principio de circulación restringida. La administración de datos personales se sujeta a los límites que se derivan de la naturaleza de los datos, de las disposiciones de la presente ley y de los principios de la administración de datos personales especialmente de los principios de temporalidad de la información y la finalidad del banco de datos. Los datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o los usuarios autorizados conforme a la presente ley. d) Principio de temporalidad de la información. La información del titular no podrá ser suministrada a usuarios o terceros cuando deje de servir para la finalidad del banco de datos. e) Principio de interpretación integral de derechos constitucionales. La presente ley se interpretará en el sentido de que se amparen adecuadamente los derechos constitucionales, como son el *hábeas data*, el derecho al buen nombre, el derecho a la honra, el derecho a la intimidad y el derecho a la información. Los derechos de los titulares se interpretarán en armonía y en un plano de equilibrio con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables. f) Principio de seguridad. La información que conforma los registros individuales constitutivos de los bancos de datos a que se refiere la ley, así como la resultante de las consultas que de ella hagan sus usuarios, se deberá manejar con las medidas técnicas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado. g) Principio de confidencialidad. Todas las personas naturales o jurídicas que intervengan en la administración de datos personales que no tengan la naturaleza de públicos están obligadas en todo tiempo a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende la administración de datos, pudiendo sólo realizar suministro o comunicación de datos cuando ello corresponda al desarrollo de las actividades autorizadas en la presente ley y en los términos de la misma”.

¹⁹⁴ PUCCINELLI, Ó. (2012). El “derecho al olvido” en el derecho de la protección de datos. El caso argentino. *Revista Internacional de Protección de Datos* n°1, julio-diciembre, pág. 4. Universidad de los Andes.

circulación perfiles de personas virtuales que afecten negativamente a sus titulares, es decir, a las personas reales”¹⁹⁵.

En Argentina está regulado por la Ley de Protección de datos personales¹⁹⁶, pero es, concretamente en este país, en el que antes de que existiese el derecho al olvido como

¹⁹⁵ Sentencia Corte Constitucional de Colombia T-414/92, de 16 de junio. Consideración V de la Corte, que se completa en los siguientes términos: “Con el triunfo definitivo del Estado moderno en el siglo XVIII, depositario de las ideas de la Ilustración y del humanismo racionalista, se impuso una nueva manera de ver las relaciones entre los gobernantes y los gobernados y con ella una nueva manera de ver el castigo. El punto clave de esta última novedad puede ser explicado como un abandono de la preocupación medioeval por punir el cuerpo de los delincuentes -a través de los suplicios- en beneficio de un interés permanente por castigar su alma. Este cambio de objeto, que Foucault ha descrito en detalle como un cambio estratégico en el ejercicio del poder, se ha ido imponiendo a través de los últimos siglos hasta adquirir hoy plena manifestación en disciplinas sociales basadas en la imposición de reglas comerciales, de métodos de observación, de técnicas de registro, de procedimientos de indagación y de pesquisa, de aparatos de verificación y, en general, de tratamiento de informaciones que condicionan y manipulan el comportamiento ciudadano sin necesidad de ejercer una coacción o una amenaza de coacción física sobre los individuos. El encarcelamiento del alma en la sociedad contemporánea, dominada por la imagen, la información y el conocimiento, ha demostrado ser un mecanismo más expedito para el control social que el tradicional encarcelamiento del cuerpo. Por eso vale la pena preguntarse si estos dos tipos de encarcelamiento se ejercen de manera discriminada y estratégica en Colombia como mecanismo de control frente a dos sectores de población diferente a saber: la cárcel tradicional para la clase marginada del circuito económico y comercial y la cárcel del espíritu contra los demás violadores de las reglas disciplinarias impuestas por dicho circuito. Este derecho le fue abiertamente negado al peticionario tanto por la Asociación Bancaria de Colombia como por el Banco de Bogotá, con lo cual lo condenaron, sin fórmula de juicio, a una exclusión del sistema crediticio por término indefinido. Ello pese a que ambas entidades sabían que desde el 27 de abril de 1987 un Juez de la República, con la autoridad que le confiere la ley declaró prescrita la obligación contraída por el peticionario con el Banco de Bogotá. Por eso es a todas luces censurable la rebeldía del banco a reconocerle efectos a esta sentencia. Como lo es también, en mayor grado, la complicidad manifiesta con dicha conducta por parte de una entidad llamada a velar por los mejores intereses del gremio, como es el caso de la Asociación Bancaria de Colombia”.

¹⁹⁶ Ley de Protección de datos personales, de 30 de octubre de 2000. Artículo 4: “1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. 2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley. 3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. 4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario. 5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga

tal, algunos personajes públicos denunciaron a Google y Yahoo Argentina con la intención de que retirasen enlaces vinculados a sus nombres que dañaban su imagen. Citaremos dos ejemplos en los que las sentencias difieren a la hora de obligar a los buscadores a retirar la información asociado al denunciante. El motivo, según Uriondo, es “la ausencia de una legislación clara en la materia, que estimula interpretaciones contradictorias que menoscaban la seguridad jurídica, provocando numerosos fallos que marcan líneas interpretativas respecto a la naturaleza jurídica de la responsabilidad civil”¹⁹⁷.

En el primer caso, la actriz Andrea Paola Krum puso dos reclamaciones contra Yahoo Argentina y Google debido a que su imagen se encontraba vinculada con webs de contenido sexual, erótico y pornográfico el otro, pidiendo la eliminación de esos enlaces vinculado a su nombre. El juez de Primera Instancia decretó “una medida cautelar innovativa, solicitando a los buscadores Yahoo Argentina y Google Inc., y a los sitios web: www.argentinasm-famosas.com.ar, www.famosasyactrices.com que procediesen a eliminar la totalidad de las páginas de contenido sexual de oferta de sexo y de servicios de acompañantes que se vinculan a la demandante”¹⁹⁸. Ante las negativas y los recursos de los buscadores, la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal dictó en 2012 sentencia firme y definitiva disponiendo que los demandados deberán: “eliminar de forma definitiva en sus respectivas páginas de resultados de búsqueda la imagen y/o el nombre de la accionante, vinculados con sitios web de contenido sexual, erótico, pornográfico, de oferta de sexo y similares, con la única excepción de aquellos sitios que correspondan a ediciones digitales de medios de prensa. Eliminar y abstraerse de incluir toda imagen de la actora con sus buscadores de imágenes. Condenar a Google

conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley. 6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular. 7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados”.

¹⁹⁷ URIONDO DE MARTINOLI, A. (2013). Difamación a través de Internet. Vacío legal argentino. *Anuario Hispano-luso-americano de derecho Internacional* n°21, pág. 499.

¹⁹⁸ Expediente 60115/2006: “Krum, Andrea Paola c/ Yahoo de Argentina S. R. L. y otros daños y perjuicios”, de 24 de octubre.

Inc. y a Yahoo Argentina S.R.L. a abonar a la actora, en concepto de resarcimiento por daño moral, 75.000 y 15.000 pesos respectivamente”¹⁹⁹.

El segundo de los supuestos tiene que ver con la demanda puesta por la modelo Priscila Petre a Yahoo Argentina S.R.L. por los enlaces que ofrece vinculados al nombre de la demandante, afirmando que el buscador conoce de antemano los contenidos de los sitios creados por terceros, los preselecciona y se reserva la facultad discrecional de modificarlos en cualquier momento. La sentencia condenó “a Yahoo Argentina a tomar las medidas técnicas y organizativas a fin de evitar que a través de sus buscadores pueda hacerse vinculación entre el nombre e imagen de la actora y sitios de contenido pornográfico y de oferta de sexo y similares, obligándole al cese de uso antijurídico y no autorizado de la imagen y del nombre de la actora y a resarcir los daños y perjuicios (100.000 pesos) por haber procedido al uso comercial y no autorizado de la imagen de la actora y por haber avasallado sus derechos personalísimos a raíz de la vinculación de su nombre e imagen con los sitios cuestionados”²⁰⁰. Tras varias apelaciones, la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal condenó al buscador a “pagar 50.000 pesos a la modelo en concepto de resarcimientos por daños y perjuicios al no atender a la solicitud de eliminar contenidos injuriosos u ofensivos”. Eso sí, también dictaminó que “no era razonable imponer a la demandada –en ausencia de legislación específica que contemple todas las complejas variantes– la obligación sistemática de monitorear todas las páginas existentes en Internet a fin de ejercer un filtrado previo de todos los contenidos que resulten ilícitos o presumiblemente ofensivos según algún criterio. Aun cuando este mandato fuese de cumplimiento técnicamente posible, no resulta una obligación razonable para quien desempeña un papel relevante en cuanto a posibilitar con eficiencia el acceso de todos los usuarios a todo tipo de contenidos”²⁰¹. Con esta declaración, lo que consigue es evitar responsabilizar a Yahoo por los enlaces que contiene en su lista de búsquedas.

¹⁹⁹ Sentencia Sala J de la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, de 31 de agosto de 2012 (MJ-JU-M-74318-AR).

²⁰⁰ Expediente 9847/2007: “Prete, Priscila c/Yahoo de Argentina S.R.L. s/daños y perjuicios”, de 18 de septiembre.

²⁰¹ Sentencia Sala I de la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, de 6 de septiembre de 2012.

De esta manera, la Cámara Nacional, como expone Uriondo, “rechaza la posibilidad de encuadrar la cuestión en el ámbito de la responsabilidad objetiva pues extiende forzosamente los conceptos de cosa riesgosa y riesgo creado a una realidad particular y extraña a los contextos que dieron justificación a la elaboración de la responsabilidad con factor objetivo de atribución, puntualizando que era necesario un balance entre distintos intereses en juego, pues no se trata de un conflicto entre intereses puramente privados, sino que se enfrentan exigencias que hacen al interés general de la comunidad -acceso a la información, prohibición de censura previa, libertad de expresión- y los imperativos que protegen derechos fundamentales del individuo, los que conforman, asimismo, el interés público. Además, la eliminación indiscriminada de sitios web de los buscadores por el solo hecho de responder a un patrón general -una temática o palabra clave, por caso- comporta una inevitable afectación del acceso a la información por cuanto significa poner en un plano de igualdad los sitios de contenidos lícitos, los sitios de noticias y de información de interés público”²⁰².

4.3. ESTADOS UNIDOS, LA ANTÍTESIS DEL DERECHO AL OLVIDO

Estados Unidos difícilmente tendrá derecho al olvido porque “la ley en Estados Unidos es claramente favorable a la libertad de expresión”²⁰³, como señala Peltz-Steele, y no lo

²⁰² URIONDO DE MARTINOLI, A. (2013). Difamación a través de Internet... *ob. cit.*, pág. 502.

²⁰³ PELTZ-STEELE, R. J. (2013). The new american privacy. *Georgetown journal of international law*. Vol. 44, pág. 383. Una teoría que reafirma MORENO BOBADILLA, Á. (2019). El derecho al olvido digital: una brecha entre Europa y Estados Unidos. *Revista de comunicación* nº18 (1), págs. 267-268; al señalar que “en Estados Unidos, a diferencia de Europa, el interés público de la información no desaparece con el paso del tiempo, por lo que las historias que sean verídicas siempre estarán protegidas por dicho concepto. Es doctrina mayoritaria la tesis de que la configuración de un derecho al olvido digital en Estados Unidos puede estar en contradicción con la tradicional jurisprudencia de la Corte Suprema relativa a la privacidad”, pero para la autora, este argumento sería “realmente rebatible, ya que el derecho al olvido digital no defiende que la información se vuelva privada, sino que esta no sea accesible cada vez que se teclea el nombre de la persona que protagonizó la información en un buscador. Por lo tanto, esta seguirá existiendo cada vez que alguien quiera ejercer su derecho a investigar, ya que estará accesible en las hemerotecas de los diarios digitales”. Por su parte, MARTÍNEZ MARTÍNEZ, R. (2014). Privacidad Estados Unidos y España. Tan lejos, tan cerca. *Revista TELOS* (Cuadernos de Comunicación e Innovación) nº97. Fundación Telefónica, febrero-mayo, pág. 57; expone que “allí donde en EEUU operan principios de libre comercio, en la UE se refuerza la metodología del consentimiento expreso y la posición jurídica del afectado. Si en EEUU la eficacia de los derechos fundamentales entre

tendrá porque sus medidas de protección de la privacidad no se acercan a los objetivos de las leyes europeas en esta materia y eso que, los primeros en introducir el concepto de derecho a la privacidad fueron los norteamericanos Warren y Brandeis. El problema en los Estados Unidos surge, en primer lugar porque el derecho al olvido es difícil de ajustarlo con la Primera Enmienda y el derecho a la libertad de expresión, ya que un derecho que obligue a limitar los contenidos, podría ser interpretado como censura, ya que la Primera Enmienda da preferencia a la libertad de expresión sobre la privacidad, al contrario que en Europa, en la que la protección a la privacidad se equilibra frente a la libertad de expresión.

Un claro ejemplo de la preferencia a favor de la libertad de expresión fue la sentencia de la Corte Suprema de los Estados Unidos en el caso *New York Times Co. v. Sullivan*²⁰⁴,

particulares es muy débil, en la UE se afirma con rotundidad. En esencia, la regulación europea profundiza en su carácter tuitivo obligando a los operadores de matriz norteamericana a incorporar prácticas ajenas a su cultura jurídica”. Por eso, reconoce que tal vez vaya siendo hora de “recuperar el diálogo trasatlántico y encontrar un punto de encuentro sobre una propuesta conjunta de estándares internacionales de protección de datos y privacidad”.

²⁰⁴ L. B. Sullivan, uno de los tres Comisarios electos de la ciudad de Montgomery (Alabama) inició una acción civil por injurias contra cuatro individuos negros, clérigos del estado de Alabama, y contra The New York Times. El demandante alegó que fue injuriado por expresiones vertidas en un artículo publicado a toda página por The New York Times el 29 de marzo de 1960. El artículo, titulado “*Heed their rising voices*” (“Atended a las voces que se alzan”) comenzaba diciendo que “como todo el mundo sabe hoy, miles de estudiantes negros sureños participan en multitudinarias demostraciones pacíficas en afirmación de su derecho a vivir dignamente como lo garantizan la Constitución de los Estados Unidos”. Continúa diciendo que “en un esfuerzo por asegurar estas garantías se han encontrado con una ola de terror sin precedentes, creada por aquellos que niegan tal documento al que todo el mundo mira como modelo de la libertad moderna”. Párrafos posteriores tienen por objeto ilustrar tal ola de terror, describiendo algunos acontecimientos supuestamente acaecidos. De los diez párrafos del texto, el tercero y parte del sexto son la base del reclamo de Sullivan por injurias, aunque no ha sido mencionado por su nombre, él alega que tales expresiones importan atribuirle una mala conducta como comisario de Montgomery a cargo de la supervisión del Departamento de Policía, señalándose lo siguiente: “En Montgomery, Alabama, después de que los estudiantes cantaran *My Country, Tis of Thee*, sus líderes fueron expulsados de la Universidad y camiones de la policía armados con escopetas y gas lacrimógeno circundaron el predio de la Universidad estatal de Alabama. Cuando todo el cuerpo estudiantil se negó a inscribirse (para el nuevo ciclo lectivo), en protesta contra las autoridades estatales, el salón comedor fue cerrado con candado, en un intento de vencerlos por medio del hambre”. Además, “una y otra vez los violadores sureños han respondido a las protestas pacíficas del doctor King con intimidación y violencia.

de 9 de marzo de 1964. El Tribunal de primera instancia del condado de Montgomery le otorgó una indemnización por daños por la suma de 500.000 dólares y la Corte Suprema de Alabama confirmó tal sentencia. El juez William J. Brennan redactó la opinión de la Corte Suprema y señaló que “la protección que la Constitución ofrece a la libertad de expresión no depende de la verdad, popularidad o utilidad social de las ideas y creencias manifestadas. Pensamos que la garantía constitucional requiere una norma federal que prohíba a un funcionario público solicitar indemnización por injurias falsas relacionadas con su conducta como funcionario, a menos que pruebe que tales expresiones fueron hechas con malicia. Sostenemos hoy que la Constitución limita el poder de un Estado para determinar los daños por injurias en acciones que se hubieren promovido por funcionarios contra los críticos de su conducta oficial. En razón de que ésta es una acción de ese tipo, la regla que requiere la prueba de malicia resulta aplicable. Aplicando estos parámetros, consideramos que la prueba presentada a fin de probar la malicia carece de la claridad y convencimiento que la norma constitucional requiere, y por lo tanto no resulta suficiente para sostener la sentencia a favor del demandante bajo la aplicación de la regla. Aun asumiendo que constitucionalmente pudieran ser encontrados como habiendo autorizado el uso de sus nombres en la publicación, no hay prueba de ningún tipo que indique que ellos estuvieron al tanto de las expresiones erróneas o que fueron negligentes en ese respecto. La sentencia contra ellos carece de sustento constitucional”.

En cuanto al New York Times, el juez concluye que “actuaremos de igual manera ya que los hechos no demuestran que se hubiere actuado con dolo. A pesar de que el artículo no era sustancialmente correcto, a pesar de que las pruebas aportadas por los demandados tienden a probar que sí lo fue, tal opinión era cuanto menos razonable y no hay prueba para atacar la buena fe de los testigos que la sostuvieron. La falta de retractación por parte del periódico a requerimiento del señor Sullivan, a pesar de que se retractó posteriormente a requerimiento del gobernador Patterson, tampoco es una muestra adecuada de dolo a nivel constitucional. Si bien el no retractarse puede o no constituir tal prueba, hay dos razones que nos llevan a pensar que aquí no lo es. Primero, porque en una carta dirigida al señor Sullivan, aunque The New York Times

Han colocado bombas en su casa, y casi mataron a su mujer y su hijo. Han atacado su persona y lo han arrestado en siete ocasiones”.

admitió que el comedor nunca había sido cerrado, el diario cuestionó la posibilidad de que un error en la solicitada hubiera podido afectar al señor Sullivan. Segundo, porque el periódico no rechazó la posibilidad de una retractación de forma definitiva, sino que pidió una explicación acerca de cómo el actor habría sido afectado por la solicitada. Tampoco el retractarse en virtud del requerimiento del gobernador aportó la prueba necesaria. Es cuestionable que la falta de retractación que no es en sí prueba de dolo pueda convertirse retroactivamente en tal por una retractación subsecuente hecha a otra parte”. Por lo tanto, el fallo de la Corte Suprema de Alabama fue revocado, concluyendo que “un funcionario público no tiene derecho a recibir reparación por daños y perjuicios por una publicación difamatoria falsa relativa a su conducta oficial, salvo que pruebe que dicha publicación fue realizada con real malicia –es decir, que fue realizada con conocimiento de que era falsa o con imprudente descuido de si era falsa o no–. La circunstancia de que al periódico se le hubiera pagado por publicar la solicitada no altera tal conclusión”. (Voto de la mayoría, dictado por el juez William J. Brennan).

La ley norteamericana, como apunta el Centro de Estudios en libertad de expresión y acceso a la información “amparada en una protección robusta de la libertad de expresión, no contiene disposiciones especiales frente al manejo de información sensible o el proceso automatizado de datos, sino normas generales de responsabilidad civil. Este marco normativo se encuentra, sin duda, en la orilla opuesta del sistema europeo, que no solo contiene normas especiales en materia de datos, sino que también permite el establecimiento de controles previos de contenido”²⁰⁵. Como apunta Kersch, “la libertad de expresión ha sido en gran parte colonizada y domesticada por las élites políticas, burocráticas y legales. Lo que es admisible o inadmisible, hoy está determinado, no tanto por el flujo de la competencia política sino por las resoluciones de los jueces no de los tribunales federales. Los conflictos más importantes y debatidos por los jueces están relacionados con el derecho a las protestas en las clínicas de aborto o los esfuerzos para prohibir la obscenidad en Internet”²⁰⁶.

²⁰⁵ Iniciativa por la Libertad de Expresión en Internet (2012). *Derecho al olvido: entre la protección de datos, la memoria y la vida personal en la era digital*. Centro de Estudios en libertad de expresión y acceso a la información. Universidad de Palermo. Argentina, pág. 21.

²⁰⁶ KERSCH, K. I. (2003). *Freedom of speech. Rights and liberties under the law*. ABC-Clio, pág. 31.

Es cierto que “no todos los principios constitucionales en Estados Unidos protegen a las personas de los poderosos y no todos los principios de privacidad protegen a las personas de las presiones sociales, pero algunos lo hacen, y cuando lo hacen, restringen y frenan el poder. Al igual que en el ámbito jurídico, la utilización de los principios sociales que protegen a la gente presupone puntos de vista acerca de lo que es importante con respecto a la vida, la extralimitación, por parte de los poderosos, puede hacer fracasar la capacidad del individuo para localizar lo que es importante en su vida. Estos puntos de vista sobre la vida humana requieren sensibilidad a nuestros factores de potencialidad y vulnerabilidad que cambian con las circunstancias históricas y culturales”²⁰⁷. La administración Obama confirmó en 2011, como explica Bernal, “el apoyo a cualquier propuesta del Congreso sobre un proyecto de ley de privacidad, ya que se ha pensado que lo sugerido y previsto hasta ese momento, está muy limitado y enfocado por completo al uso comercial de datos, más que a cuestiones de mayor alcance, tratando a la gente mucho más como consumidores que como ciudadanos. Existen muchas razones para esta limitación: como el nivel de vigilancia que la NSA ha llevado a cabo y puesto de manifiesto con las denuncias de Edward Snowden sobre PRISM²⁰⁸ y otros programas”. Por esta razón, habría sido difícil para Obama pronunciarse claramente al respecto, teniendo un control de vigilancia gubernamental tan exhaustivo sobre los ciudadanos. “El proyecto PRISM sugería que las autoridades deben tener acceso directo a los servidores y a las grandes compañías de Internet, incluso pudiendo vulnerar los derechos humanos. Ésta tendría que ser una de las fortalezas principales de un enfoque basado en los derechos, principalmente, en los derechos del individuo. Las acciones de todos aquellos que violen dichos derechos, sean agentes gubernamentales o comerciales, pueden ser analizadas, evaluadas y, en su caso, opuestas tanto política como legalmente”²⁰⁹.

²⁰⁷ SCHOEMAN, F. D. (1992). *Privacy and social freedom*. Cambridge University Press, pág. 22.

²⁰⁸ Programa de vigilancia electrónica operado por la NSA que podía acceder a la información de los servidores de compañías como Microsoft, Google, Facebook o Apple. Además, sirvió para espiar llamadas telefónicas de millones de ciudadanos norteamericanos. Disponible en: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

²⁰⁹ BERNAL, P. (2014). *Internet Privacy Rights. Rights to Protect Autonomy*. Cambridge University Press. New York, pág. 272-273. Este autor es uno de los impulsores del derecho al olvido en Estados Unidos frente a autores como ROSEN, J. (2012). The right to be forgotten. *Stanford Law Review*. Vol. 64, pág. 88; que se muestra muy crítico al afirmar que “aunque Reding –vicepresidenta de la Comisión

Un claro ejemplo de que los Tribunales estadounidenses dan prioridad a la Primera Enmienda en lugar del derecho al olvido es el caso *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme and L'union Des Etudiants Juifs De France*. El Tribunal de Grande Instance de París había ordenado a Yahoo Inc. “a adoptar todas las medidas para disuadir y hacer imposible cualquier consulta en Yahoo.com para el servicio de subastas de objetos nazis y cualquier otro sitio o servicio que constituyen una disculpa por el nazismo y la impugnación crímenes nazis”. Además, se solicitó “a Yahoo Francia evitar la vinculación a enlaces que permitan ejercer la búsqueda en Yahoo.com, ya sea a partir de una árbol o de palabras clave que enlacen con páginas web o foros cuyo título o contenido, que constituyen una violación de la legislación francesa, enaltezcan el nazismo o pongan a la venta uniformes, insignias y banderas que recuerden a los usados o exhibidos por los nazis, debiendo interrumpir inmediatamente el acceso a las páginas para evitar que se incurra en las sanciones previstas por la legislación francesa o dar respuesta a las acciones iniciadas en contra de ella”²¹⁰.

Yahoo! Inc., con sede en California decidió recurrir la sentencia ante el Tribunal de Apelaciones de los Estados Unidos y éste acabó dándole, en parte, la razón al proveedor de servicios, ya que “sin duda, el discurso de odio que los acusados buscan suprimir es condenable pero, en este caso, no se podrá bloquear el acceso a esos datos al resto de usuarios de Estados Unidos, ya que se estaría violando la Primera Enmienda. No debemos permitir que una orden judicial extranjera pueda usarse como palanca para sofocar el discurso protegido por la Constitución. Por otra parte, de hacerse, se crearía un nuevo y preocupante precedente para los proveedores de servicios de Internet con sede en Estados Unidos, que pueden ser confrontados con las órdenes judiciales extranjeras que les obligarían a vigilar el contenido accesible a los usuarios de Internet

Europea y Comisaria de Justicia, Derechos Fundamentales y Ciudadanos– describió el nuevo derecho como una modesta expansión del derecho de privacidad de datos existentes, de hecho representa la mayor amenaza para la libertad de expresión en Internet en la próxima década. El derecho a ser olvidado podría hacer que Facebook y Google, por ejemplo, sean responsables de hasta el dos por ciento de sus ingresos globales si no eliminan las fotos que las personas publican sobre sí mismas y luego se arrepienten, incluso si las fotos ya se han distribuido ampliamente. A menos que el derecho se defina con mayor precisión, podría precipitar un choque dramático entre las concepciones europeas y estadounidenses del equilibrio adecuado entre la privacidad y la libertad de expresión, lo que lleva a un Internet mucho menos abierto”.

²¹⁰ Tribunal de Grande Instance de París, 22 de mayo de 2000. *Association "Union des Etudiants Juifs de France", la "Ligue contre le Racisme et l'Antisémitisme" / Yahoo! Inc. et Yahoo France*.

desde otro país”²¹¹. Por lo tanto, la sentencia podrá aplicarse en Estados Unidos sólo a los ciudadanos franceses, mientras que el resto de usuarios son libres de buscar aquellos contenidos que deseen en Yahoo.

Como vemos, no existe una ley norteamericana que proteja a los ciudadanos del derecho al olvido, pero sí hay ciertos estados que protegen la privacidad de un grupo concreto de población. Este es el caso de California que aprobó la *California's Privacy Rights for California Minors in the Digital World Act*, también conocida como “ley borrador” en la que se permite a “los menores eliminar o solicitar y obtener la eliminación del contenido o información publicada en un sitio web de Internet, servicios en línea o aplicaciones móvil. También prohíbe que un operador de un sitio web o servicio en línea dirija, a través de campañas de marketing o publicidad, productos específicos o servicios que los menores tienen prohibido su compra por ley. La ley también prohíbe la publicidad de determinados productos en base a información personal específica recogida de un menor de edad o el uso de aquella que revelada o recopilada por un tercero”²¹².

La Corte de Apelación 2ª de Estados Unidos en el caso *Martin v. Hearst Corporation*²¹³, de 28 de enero de 2015, rechazó la demanda de Martin contra los editores de los medios de comunicación por difamación, a pesar de que los cargos en su contra habían sido anulados por el Estado, al establecer que el “*Erasure Statute* no

²¹¹ Sentencia Corte de Apelación 9ª de Estados Unidos en el caso *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme and L'union Des Etudiants Juifs De France* (No. 01-17424), de 12 de enero de 2006.

²¹² *California's Privacy Rights for California Minors in the Digital World Act*. Calif. Bus. & Prof. Code 22580-22582. Senate Bill N°568, de 23 de septiembre de 2013.

²¹³ Lorraine Martin y sus dos hijos fueron detenidos el 20 de agosto de 2010, después que la policía sospechase que existe una red de tráfico de drogas, registró la casa y encontró marihuana, balanzas, bolsas de plástico, y material para trabajar con drogas. Martin y sus hijos fueron acusados de diversos delitos relacionados con la posesión de drogas. Los periódicos locales (*Connecticut Post*, *Stamford Advocate* y *Greenwich Time*), propiedad de Hearst Corporation, informaron del arresto, publicando varios artículos en línea. Más de un año después de que se publicasen las informaciones, el Estado decidió no continuar con el caso contra Martin, debido a que se anuló la causa penal contra ella, los registros de detención de Martin fueron borrados de conformidad con el *Erasure Statute* (Connecticut General Statutes § 54-142a - *Erasure of criminal records*).

produce efecto sobre los artículos publicados en relación a un arresto, ya que los datos publicados no contenían ningún dato sobre Martin que no fuese cierto”. El Tribunal dio más importancia al derecho del público a saber y ser informado que el derecho al olvido de Martin. Al respecto de este caso, Giampa sostiene que “muchas de las reivindicaciones que se hacen respecto a la privacidad no son relevantes para el derecho al olvido, ya que se ocupan de informaciones falsas o no reveladas, y han sido significativamente limitadas para proteger la libertad de expresión como en el caso *Martin v. Hearst Corporation*. Lo que Europa ha buscado a través del derecho al olvido es el tiempo, abordando la información que pueda ser potencialmente obsoleta, irrelevante, perjudicial o inexacta, mientras que los agravios contra la privacidad (*privacy torts*) en Estados Unidos proporcionan causa directa de la acción cuando la información se ha publicado, con muchas limitaciones”²¹⁴.

Hay que explicar que el concepto de privacidad que se quería aplicar se vinculaba con el derecho del individuo a ser dejado solo (*right to be let alone*) y no con el derecho al olvido (*right to be forgotten*). En este sentido, el juez Cooley ya se había pronunciado, con anterioridad a Warren y Brandeis, respecto al derecho a ser dejado solo, definiéndolo como: “el derecho de una persona a la total inmunidad personal. La correspondiente obligación es, no infringirla como un daño, tratando dicha proximidad como un elemento satisfactorio para extinguir la infracción del daño. Particularmente esta obligación va más allá de lo requerido en la mayoría de los casos, en los que normalmente un fin inesperado o una infracción sin éxito no son notificadas. Pero la extinción para una agresión física o daño engloba varios elementos que no presentan siempre un incumplimiento del deber, incluye normalmente un insulto, «meter miedo», una llamada repentina a la energía para una rápida y efectiva resistencia. Esto es muy parecido a un show para los nervios, empeorando la paz y tranquilidad individual durante un periodo mayor o menor. Hay, como consecuencia, amplias razones para el apoyo de una norma de ley que ataque un ley errónea, incluso cuando no hay tenido lugar la agresión. En realidad, en este caso, la ley va más allá y hace de este intento una ofensa criminal”²¹⁵.

²¹⁴ GIAMPA, G. (2016). *Americans have a right to be forgotten*. Law School Student Scholarship. Seton Hall University, págs. 13-14.

²¹⁵ COOLEY, T. M. (1879), *A treatise on the law of torts or the wrongs which arise independently of contract*. Callaghan. Chicago, pág. 33. La expresión acuñada por Cooley “to be let alone” sirve, según

El debate sobre el derecho a la privacidad, como indican Alderman y Kennedy, “no ha tenido una gran publicad dentro del marco Constitucional, pero para aquellos que están involucrados, el efecto en sus vidas es profundo. La cuestión de cuándo y bajo qué circunstancias deberíamos seguir reconociendo el delito contra la privacidad plantea cuestiones mucho más amplias como qué tipo de sociedad queremos ser y como priorizar nuestras libertades en contraposición a nuestras restricciones. Estas cuestiones están más marcadas y tienen más controversia cuando los delitos contra la privacidad van contra la Primera Enmienda, pues, aunque los delitos pueden utilizarse contra cualquiera, es más común que se utilicen contra los medios de comunicación. Entonces se produce un choque entre el derecho a ser dejado solo y el derecho a saber, en definitiva, un choque entre la privacidad y el periodismo”²¹⁶.

señala PROSSER, W. L. (1960). *Privacy. California Law Review*. Vol. 48, nº3, pág. 389; de único nexo de unión de los cuatro tipos de agravios que identificó la ley de privacidad americana: intrusión en el aislamiento, la soledad o los asuntos privados del demandante; divulgación pública de hechos privados vergonzosos sobre el demandante; publicidad que coloca al demandante bajo una imagen falsa ante los ojos del público; y apropiación en beneficio del demandado del nombre o la imagen del demandante. El problema surge, según Prosser, debido a que la ley “comprende cuatro supuestos distintos de responsabilidad, que no tienen casi nada en común, excepto que cada uno representa una interferencia en el derecho del demandante, por lo que debería ser obvio, al menos en algunos aspectos, que estos agravios estén sujetos a reglas diferentes, ya que lo enunciado sobre cualquiera de ellos al transferirse a otro, puede no ser aplicable en absoluto, dando lugar a confusión a la hora de aplicarse”. En la misma línea se expresa SOLOVE, D. J. (2009). *Understanding Privacy*. Harvard University Press, pág. 6; al considerar que “los tribunales a menudo tienen en cuenta una visión particular de la privacidad cuando evalúan si una actividad viola la privacidad. Como resultado, combinan distintos problemas de la privacidad a pesar de las diferencias significativas o no reconocen un problema por completo. En resumen, los problemas de privacidad con frecuencia se malinterpretan o se reconocen de manera inconsistente en la ley”.

²¹⁶ ALDERMAN, E. y KENNEDY C. (1997). *The right to privacy*. Vintage, pág. 157. Para CATE, F. H. (2001). *Privacy in Perspective*. The American Enterprise Institute. Washington, págs. 3-4; el concepto de privacidad, históricamente, se ha entendido desde una perspectiva personal, por eso considera que a la hora de definirla hay que tener en cuenta los siguientes aspectos: “autonomía individual (el derecho a tomar decisiones sobre el matrimonio o la familia sin interferencia del gobierno); soledad e intimidad (el deseo de limitar el acceso a un lugar a uno mismo); confidencialidad (secretos comerciales e información divulgada sujeta a una promesa de confidencialidad); anonimato (el deseo de no ser identificado); seguridad (para uno mismo o la información de uno); libertad de intrusión, ya sea física (un intruso) o tecnológica (una cámara oculta o micrófono); y control de la información sobre uno mismo”.

La jurisprudencia norteamericana, desde el caso *Silverman v. United States*, 365 U.S. 505, de 6 de marzo de 1961, durante cuatro décadas, reforzó, como señala Saldaña, “la noción de que la violación de la Cuarta Enmienda sólo tiene lugar cuando se produce una invasión física de la propiedad individual o una requisita material de efectos personales, habilitándose así a los agentes del gobierno a utilizar mecanismos de vigilancia electrónica que como los micrófonos no exigían la irrupción física en las propiedades o efectos personales de los ciudadanos”²¹⁷. En 1986, la Corte Suprema en el caso *Bowers v. Hardwick*, dictó una sentencia insólita, negando la protección a la conducta sexual privada, primando la criminalización de la sodomía en el propio domicilio en Georgia al no estar protegida por la Decimocuarta Enmienda. El juez Blackmun emitió un voto discrepante en el que no estaba para nada de acuerdo con la sentencia, ya que considera que “este caso se trata del más completo de los derechos y el más valorado por los hombres civilizados, es decir, el derecho a ser dejado solo” y reconoce que “el enfoque casi obsesivo de la Corte sobre la actividad homosexual es particularmente difícil de justificar a la luz de los términos utilizados en Georgia”. Blackmun va más allá al afirmar que “el sexo o condición de las personas que se involucran en el acto es irrelevante como materia para la ley estatal e implica una intromisión inconstitucional en su vida privada y su derecho de asociación íntima no depende en modo alguno de su orientación sexual, por lo que no veo ninguna base para la decisión del Tribunal” (Caso *Bowers v. Hardwick* (No. 85-140), 478 U.S. 186, de 30 de junio de 1986).

²¹⁷ SALDAÑA DÍAZ, M^a. N. (2012). The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis. *Revista de Derecho Político* nº85. UNED, pág. 229. La misma autora en La protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de la información personal en los Estados Unidos (2007). *Revista Iberoamericana de Filosofía, Política y Humanidades* nº18, págs. 114-115; expone que “existe un creciente interés en la doctrina y jurisprudencia norteamericanas por proteger con el máximo rango constitucional todo ámbito de información personal en el contexto de la sociedad tecnológica avanzada. No obstante, el interés individual en la protección de la información personal, se enfrenta, como en ningún otro momento, a los intereses colectivos de carácter público y general... Si, como viene defendiéndose desde Warren y Brandeis, una vida privada al amparo de injerencias no deseables permite el libre desarrollo de la personalidad, si la protección de la información personal fomenta el desarrollo de la autonomía individual y la autodeterminación personal, su protección es igualmente un criterio determinante del carácter democrático de toda sociedad. De ahí que la protección constitucional de zonas de privacidad de la información personal que aseguran nuestra autonomía individual sea garantía del carácter democrático y, por tanto, valor constitutivo de las actuales sociedades tecnológicas”

Posteriormente, el caso *Lawrence v. Texas*²¹⁸ (No. 02-102) 539 U.S. 558 (2003), 26 de marzo de 2003. La Corte Suprema aceptó la revisión del fallo de la Corte de Apelaciones de Texas. Después de estudiar el caso en profundidad, el juez Kennedy fue el encargado de redactar el fallo de la mayoría, en el que establecía que “la libertad protege a la persona de las intromisiones injustificadas por parte del gobierno en el hogar y otros lugares privados. En nuestra tradición, el Estado no está omnipresente en el hogar. Y otras esferas de nuestras vidas y existencias, fuera del hogar, en las cuales el Estado no debe tener una presencia dominante. La libertad se extiende más allá de límites espaciales. Ella supone una autonomía del ser que incluye la libertad de pensamiento, creencia, expresión y ciertas conductas íntimas. El caso presente conlleva la libertad de la persona tanto en su dimensión espacial como en otras más trascendentales”. Además, considera que “el caso involucra a dos adultos, los que, con completo y mutuo consentimiento, llevaron a cabo práctica sexuales comunes a la forma de estilo homosexual. Los demandantes tienen derecho al respeto de su vida privada. El Estado no puede hacer de su conducta sexual privada un crimen. Su derecho a la libertad les otorga bajo la cláusula de Debido Proceso (*Due Process Clause*) les otorga el más completo derecho a llevar a cabo sus conductas sin la intervención del gobierno”. (Punto 578). La importancia de esta sentencia radica en que la Corte Suprema estableció que el caso *Bowers v. Hardwick* “no fue correcto en el momento en que se falló y no lo es hoy en día. No debe mantenerse como precedente obligatorio y, por tanto, debe y es ahora invalidado”.

La formulación de la privacidad de Warren y Brandeis, bajo la clásica concepción del *right to be let alone*, para Saldaña, “sigue emergiendo en el discurso de la privacidad y no solo se ha enraizado en la tradición legal y constitucional norteamericana a lo largo del siglo XX, sino que continúa teniendo validez en la sociedad tecnológica avanzada de principios del siglo XXI, porque, desde sus orígenes, el derecho a la privacidad surge como una reacción ante las posibilidades invasivas de la tecnología, estando estrechamente alineada a la reciente doctrina que centra especialmente la atención en el

²¹⁸ En Houston, en 1998, varios oficiales de policía entraron en la vivienda de Lawrence, tras un aviso por desorden doméstico. Al entrar se encontraron a Lawrence teniendo sexo con otro hombre. Ambos fueron arrestados y acusados en base a la norma del Código Penal de Texas por coito desviado entre personas del mismo sexo. La Corte de Apelaciones de Texas decidió en contra de los implicados, basándose en el caso *Bowers v. Hardwick*.

aspecto informacional de la privacidad, es decir, el derecho al control sobre la información personal”²¹⁹.

El término privacidad, que no aparece en la Constitución de los Estados Unidos, ha generado un amplio debate político y una gran diversidad de opiniones al respecto. A pesar de ello, la Corte Suprema encontró, como señalan Abril y Pizarro, “tanto en las *Bill of rights* –término por el que se conocen las diez primeras enmiendas de la Constitución de los EEUU– como en la Decimocuarta Enmienda la protección del derecho a la privacidad relacionado con la libertad de asociarse, la integridad corporal, y las decisiones individuales acerca de la educación, la vida familiar y la sexualidad”. De ahí que, siguiendo esta línea, “el desarrollo del derecho constitucional estadounidense a la privacidad se ha enfocado en entenderlo como un derecho a lo físico, a la información, a decidir libremente, a la propiedad y a la libre asociación. Como es derecho y a la vez garantía constitucional, la privacidad también puede ser descrita como el derecho de los individuos frente a las interferencias gubernamentales en sus vidas privadas”²²⁰.

A pesar de que en Estados Unidos el derecho al olvido digital no está reconocido, el estado de California en un intento por proteger a los menores de Internet, aprobó el 23 de septiembre de 2013, la Senate Bill 568, bajo el título *Privacy Rights for California Minors in the Digital World*. Una ley que da la opción a los menores de 18 años a solicitar que se elimine de “forma permanente todo el contenido sea gráfico o escrito que ellos mismos hayan subido a las redes sociales”. El propietario del sitio web tiene la obligación de informar a los menores de que existe tal derecho e informarle sobre el proceso para realizar dicha solicitud cuando lo deseen. En el caso de que el contenido haya sido subido por una tercera persona, el menor no podrá solicitar que el contenido sea retirado, así como tampoco lo podrá hacer si el contenido se ha copiado y pegado en otro sitio web. La ley, que entró en vigor el 1 de enero de 2015, también prohíbe a las compañías de servicios en línea y a las redes sociales que recopilen o divulguen datos con el fin de comercializar productos o servicios prohibidos para la venta a menores de 18 años como alcohol, tabaco o armas.

²¹⁹ SALDAÑA DÍAZ, M. N. (2012), The right to privacy. La génesis de... *ob. cit.*, pág. 233-235.

²²⁰ ABRIL, P. y PIZARRO MORENO, E. (2014). La intimidad europea... *ob. cit.*, pág. 13-14.

Un gran paso para que las organizaciones de servicios en línea y redes sociales establezcan claramente un mecanismo para identificar a los menores que usan su sitio. También deberán establecer mecanismos legales y tecnológicos efectivos, así como políticas y programas para garantizar que cumplen con estas nuevas leyes de protección de la privacidad de los niños. Esto incluye proporcionar a los menores un método fácil para ejercer su "derecho al olvido".

CAPÍTULO 5. LA DOGMÁTICA DEL DERECHO AL OLVIDO

El derecho al olvido urge el examen diacrónico de la protección de la privacidad o de la privacidad misma. Es importante analizar si el paso del tiempo afecta sólo a la garantía de la privacidad (con el tiempo pierde vigor) o a la privacidad misma y es, entonces, lo íntimo lo que pierde vigor con el paso del tiempo. Lo primero afectaría a los plazos de prescripción y si fuese lo segundo, la protección de los derechos fundamentales no estaría sujeta a prescripción. Por lo que es necesario averiguar y lo abordaremos en este capítulo, si el derecho al olvido es un derecho fundamental o un derecho derivado de la libertad informática.

Esta disyuntiva también es abordada por Mieres al considerar que “se puede derivar un derecho al olvido que ponga límites a la perennidad de la información en línea. A partir del derecho a la protección de datos y del derecho a la intimidad o a la vida privada es posible articular la pretensión de las personas a no verse perseguidas por las informaciones del pasado”. En el caso de considerar que del derecho a la intimidad puede derivarse un derecho al olvido, “puede suscitar, a primera vista, alguna perplejidad, ya que el derecho a la intimidad se proyecta sobre datos íntimos, y resulta paradójico que un dato que ha sido público pueda, por el paso del tiempo, transmutar su calidad y devenir en privado o íntimo”. Para poder derivar un derecho al olvido digital del de protección de datos “es la proyección de este último a Internet, esto es, considerar que cualquier publicación de datos accesibles en la red constituye un tratamiento de datos personales que debe someterse a la normativa específica de protección. Además, el factor tiempo tiene una incidencia evidente sobre los datos que son objeto de tratamiento por un tercero, en la medida en que su paso puede hacer que el tratamiento de datos obsoletos resulte inadecuado, impertinente o excesivo, dando lugar a que el titular pueda ejercer su derecho de cancelación y oposición. De este modo, los derechos de cancelación y oposición proyectados sobre Internet permiten proteger el interés de las personas a obtener el olvido digital de datos pasados que les pueden perjudicar”²²¹.

²²¹ MIERES MIERES, L.J. (2014). *El derecho al olvido digital*. Fundación Alternativas, págs. 13-19. En este sentido, DAVARA RODRÍGUEZ, M. Á. (2013). El derecho al olvido en Internet. *Diario La Ley* nº 8.137, pág. 108; reconoce el derecho al olvido como “aquel que tiene el titular de un dato a que este sea borrado o bloqueado cuando se produzcan determinadas circunstancias y, en particular, a que no sea accesible a través de la red”.

5.1. EL DERECHO AL OLVIDO, ¿ES UN DERECHO FUNDAMENTAL?

Lo primero que tenemos que definir es si consideramos el derecho al olvido como un derecho fundamental. En primer lugar hay que recalcar que un derecho fundamental, como señala Bastida, es ante todo, “un derecho subjetivo, es decir, un apoderamiento jurídico (contenido del derecho) que la Constitución, atribuye a un sujeto para que pueda defender, asegurar o ejercer determinadas expectativas (objeto del derecho). Ese apoderamiento consistirá en la posibilidad de, con la fuerza normativa de la Constitución, exigir a un tercero, sea un poder público o un particular, el cumplimiento de un deber; (de actuar, en unos casos, o de abstenerse de actuar, en otros). Sólo son fundamentales los derechos que participan de la fundamentalidad de la norma fundamental del ordenamiento jurídico, la Constitución, lo cual significa que ésta, como fuente jurídica directamente aplicable establece esos derechos y los dota de una disponibilidad por su titular potencialmente inmediata, y, como fuente de las demás fuentes del ordenamiento, preserva a los derechos fundamentales de su alteración o vulneración por normas infraconstitucionales (y en algunos casos incluso constitucionales) y los hace indisponibles por el legislador”. Además, las dos características que tipifican a un derecho fundamental “derivan de la doble dimensión de la Constitución en cuanto fuente jurídica: como fuente sobre las demás fuentes y como fuente suprema de eficacia directa. En la primera vertiente, la Constitución regula la producción de normas y sus destinatarios son el legislador y los demás poderes públicos, a los que les está vedada la libre disposición sobre los derechos constitucionalmente establecidos. En la otra vertiente, la Constitución actúa como fuente que crea directamente relaciones jurídicas. Dotada de eficacia inmediata, su destinatario puede ser cualquiera y su objeto cualquier ámbito vital. La doble participación en la condición de la Constitución como fuente hace que los derechos fundamentales sean inatacables y de eficacia potencialmente inmediata”²²².

Parece claro, como apunta Sánchez de Diego, que para que “un derecho sea fundamental ha de encontrarse recogido en la Constitución dentro del apartado dedicado a los derechos fundamentales y con la máxima protección constitucional. La protección

²²² BASTIDA FREIJEDO, F. J., (2004). *Concepto y modelos históricos de los derechos fundamentales en Teoría General de los derechos fundamentales en la Constitución Española de 1978*. Tecnos, págs. 25-26.

que otorga el artículo 53 en relación con el 81 de la CE es triple: desarrollo mediante Ley Orgánica que respete su contenido esencial, protección ante la justicia ordinaria mediante un procedimiento preferente y sumario y, en último término, posibilidad de amparo constitucional”²²³. Por su parte, Villaverde, considera que “la función de los derechos fundamentales es la de ser garantes de la libertad del ciudadano, que lo es justo por ser libre, y también de un espacio en el que se ejerce la condición de ciudadanía que debe ser público. Su sentido último en el Estado democrático es ser la causa jurídica del espacio para la vida pública en la que nos encontramos con el otro, donde es indispensable encontrarse con el otro, aunque la presencia del otro, del distinto nos perturbe e incluso moleste o incomode”²²⁴.

El objeto de un derecho fundamental, como apunta el mismo autor, “es una esfera de libertad individual, es decir, aquel ámbito de la realidad vital de un individuo en la que el ordenamiento jurídico les garantiza su autodeterminación sobre las conductas posibles que en el mismo puedan tener lugar, sin sometimiento a poder público alguno, ni siquiera el impuesto por la ley. En principio, todos los comportamientos posibles que quepan dentro del ámbito de la realidad definido abstractamente en el precepto que contiene el derecho fundamental son merecedores de la protección iusfundamental”. El ámbito de realidad protegido iusfundamentalmente “puede venir expresa y directamente definido por el derecho fundamental mediante un permiso constitucional: la indicación de una esfera vital del individuo en el que son posibles comportamientos muy dispares (derecho a la intimidad, art. 18.1, por ejemplo, donde puede entenderse protegido desde los trámites de adopción de un menor hasta, incluso, los datos económicos de un sujeto) o de un comportamiento genérico (libertad de expresión, art. 20.1 CE, donde las conductas protegibles deben poder encajar en el significado del término expresión)”²²⁵.

El estudio de los derechos fundamentales tiene como referencia ineludible los derechos humanos, aunque, como reconoce Bastida, “conviene dejar claro que unos y otros no son exactamente lo mismo. Se pueden sintetizar en tres los modelos históricos de

²²³ SÁNCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, M. (2010). De la libertad de expresión al derecho de acceso a la información pública. *Comunicación y pluralismo* nº9, pág. 23.

²²⁴ VILLAVERDE MENÉNDEZ, I. (2007). *Ciberconstitucionalismo. Las TIC... ob. cit.*, págs. 21-22.

²²⁵ VILLAVERDE MENÉNDEZ, I. (1998). Esbozo de una teoría general de los derechos fundamentales. *Revista jurídica de Asturias* nº22.

fundamentación de los derechos, aunque en puridad sólo el modelo iusracionalista (iusnaturalista) y el modelo positivista tienen un engarce inmediato”. En lo que se refiere al modelo positivista, “una primera aproximación y en términos harto generales se puede decir que este modelo transforma los derechos humanos en derechos fundamentales. Los incorpora como un elemento esencial del sistema jurídico, que los reconoce y garantiza con la fuerza irresistible del único derecho válido, el derecho positivo, es decir, los respalda con el uso lícito de la fuerza física que ostenta en monopolio el Estado. Reclamar un derecho fundamental no consistirá en apelar sin más al respeto a un derecho natural de la persona. La apelación no tendrá virtualidad ante los poderes públicos si ese derecho no está previamente positivado, o sea, incorporado y garantizado como derecho positivo, único alegable ante los tribunales. De ahí que la declaraciones de derechos, hechas inicialmente al margen de las constituciones, aparezcan hoy en día integradas de una u otra manera en ellas, ya como adhesión a su texto (Preámbulo de la Constitución Francesa de 1958), ya como elenco de derechos fundamentales explícitamente reconocidos (la mayoría de las constituciones, incluida la nuestra, Caps. I y II del Título I CE), ya como instrumento para la interpretación de éstos (art. 10.2 CE)”²²⁶.

Hay autores como Simón que defienden el derecho al olvido como un derecho fundamental implícito derivado del artículo 10.1 de la CE (“La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social”). Dicho artículo, como señala, “reconoce la autonomía del individuo, su libertad de actuar y decidir libremente su proyecto vital, así como la posibilidad de alterarlo, modificarlo e innovarlo tantas veces como quiera, e incluso, no tenerlo. Tanto la prescripción de los antecedentes penales como la anonimización de las sentencias preservan este bien jurídico, protegiendo la dignidad humana y el libre desarrollo de la personalidad”. Por tanto, el derecho al olvido “se configuraría así como un derecho de libertad del ciudadano a poder escoger cuándo y dentro de qué límites procede revelar datos e informaciones que forman parte de su identidad, protegiendo a los individuos frente a la difusión de todas las informaciones pasadas que les puedan afectar en el

²²⁶ BASTIDA FREIJEDO, F. J. (2005). El fundamento de los derechos fundamentales. *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja* n°3, págs. 41-43.

futuro, con indiferencia de si afectan o no a los derechos a su vida privada”²²⁷. En este sentido, no estamos de acuerdo con dicha afirmación, ya que el aseverar que los individuos pueden protegerse de todas las informaciones, afecten o no los derechos de su vida privada, quiere decir que cada individuo puede diseñar a su antojo su pasado y solicitar porque sí que se borren aquellas noticias que consideren que pueden pasarles factura, aunque no afecten a los derechos de su vida privada, sin tener en cuenta otros derechos fundamentales como la libertad de información o libertad de expresión que sí estarían probados y avalados. Por tanto, el derecho al olvido no puede ser un derecho absoluto y debe conectarse con la libertad de expresión.

Para Mieres, esta consideración de Simón es “indudablemente audaz y tiene el mérito de afrontar directamente las dificultades de encaje que presenta el derecho al olvido en el molde de los derechos fundamentales específicos, pero, de acuerdo con la jurisprudencia constitucional²²⁸, el artículo 10.1 CE no constituye un derecho

²²⁷ SIMÓN CASTELLANO, P. (2012). *El régimen constitucional del derecho al olvido digital*. Tirant lo Blanch. Valencia, pág. 118. Hay autores como Cobacho y Burguera que abogan porque el derecho al olvido es una extensión del derecho de cancelación y oposición al señalar que: “este derecho per se, no constituye una novedad material, un derecho de perfiles inéditos, como un amalgama de derechos ya existentes, cuya aleación ha dado lugar a una construcción de nuevo cuño, que pretende responder con eficacia a necesidades derivadas de la irrupción del panorama jurídico de Internet y de las nuevas tecnologías”. COBACHO LÓPEZ, Á., y BURGUERA AMEAVE, L. (2013). *Responsabilidad de los webmasters y derecho al olvido digital*, pág. 386; en VALERO TORRIJOS, J. (2013). *La protección de los datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*. Thomson Reuters-Aranzadi.

²²⁸ STC 53/1985, de 11 de abril. FJ8: “Junto al valor de la vida humana y sustancialmente relacionado con la dimensión moral de ésta, nuestra Constitución ha elevado también a valor jurídico fundamental la dignidad de la persona, que, sin perjuicio de los derechos que le son inherentes, se halla íntimamente vinculada con el libre desarrollo de la personalidad (art. 10) y los derechos a la integridad física y moral (art. 15), a la libertad de ideas y creencias (art. 16), al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1). Del sentido de estos preceptos puede deducirse que la dignidad es un valor espiritual y moral inherente a la persona, que se manifiesta singularmente en la autodeterminación consciente y responsable de la propia vida y que lleva consigo la pretensión al respeto por parte de los demás”. Opinión reiterada en la STC 91/2000, de 30 de marzo. FJ7: “Como hemos afirmado en varias ocasiones, proyectada sobre los derechos individuales, la regla del art. 10.1 CE implica que, en cuanto valor espiritual y moral inherente a la persona, la dignidad ha de permanecer inalterada cualquiera que sea la situación en que la persona se encuentre, constituyendo, en consecuencia un *mínimum invulnerable* que todo estatuto jurídico debe asegurar. De modo que la Constitución española salvaguarda absolutamente

fundamental en sí mismo ni es fuente de nuevos derechos fundamentales tácitos. Este precepto constitucional tiene, primeramente, una función interpretativa a la hora de determinar el contenido constitucionalmente declarado de los derechos fundamentales reconocidos y, también, cumple la función de dar cobijo a lo que se ha dado en llamar libertades constitucionales. Se trata de libertades negativas que exigen de los poderes públicos un deber de abstención, de no interferencia. En cambio, el derecho al olvido exige una conducta activa por parte de sus destinatarios: dejar de dar publicidad o corregir cierta información o dato obsoleto. En este sentido, la tutela que demanda el derecho al olvido frente a las informaciones obsoletas se articula a través de remedios de reintegración del derecho, como la acción inhibitoria, dirigida al cese o limitación de la divulgación de la información obsoleta, o la acción de rectificación, cuando el paso del tiempo haya hecho que una información en su día no objetable devenga en incompleta, equívoca o engañosa”²²⁹.

Sorprende el caso de Simón que, además de intentar articular el derecho al olvido como un derecho fundamental implícito derivado del artículo 10.1, ha buscado encajar dicho derecho en el marco del derecho fundamental a la protección de datos personales que se establece en el artículo 18.4 de la CE. En realidad, como señala “tal artículo sólo establece un mandato legislativo que la doctrina jurisprudencial se ha encargado de convertir en derecho fundamental, con el siguiente objeto: «la singularidad del derecho a la protección de datos, pues, por un lado, su objeto es más amplio que el del derecho a la intimidad, ya que el derecho fundamental a la protección de datos extiende su garantía no sólo a la intimidad en su dimensión constitucionalmente protegida por el art. 18.1 CE, sino a lo que en ocasiones este Tribunal ha definido en términos más amplios como esfera de los bienes de la personalidad que pertenecen al ámbito de la vida privada, inextricablemente unidos al respeto de la dignidad personal (...) El derecho fundamental a la protección de datos amplía la garantía constitucional a aquellos de esos datos que sean relevantes para o tengan incidencia en el ejercicio de cualesquiera derechos de la persona, sean o no derechos constitucionales y sean o no relativos al

aquellos derechos y aquellos contenidos de los derechos «que pertenecen a la persona en cuanto tal y no como ciudadano o, dicho de otro modo (...) aquéllos que son imprescindibles para la garantía de la dignidad humana» (STC 242/1994, de 20 de julio, FJ 4; en el mismo sentido, SSTC 107/1984, de 23 de noviembre, FJ 2 y 99/1985, de 30 de septiembre, FJ 2)”.

²²⁹ MIERES MIERES, L. J. (2014). *El derecho al olvido... ob. cit*, págs. 11-12.

honor, la ideología, la intimidad personal y familiar a cualquier otro bien constitucionalmente amparado» (STC 292/2000, de 30 de noviembre, FJ 6)”. El derecho fundamental a la protección de datos se configura como un derecho que “garantiza a las personas un poder de control respecto el uso y el destino de sus datos personales, utilizando un concepto amplio de dato personal, que va más allá de datos relativos a la intimidad y que se extiende a cualquier dato que permita identificar a las personas. En concreto, por dato personal se entiende cualquier información referente a personas físicas identificadas o identificables²³⁰. Precisamente, por este motivo, la regulación en materia de protección de datos será de aplicación a toda la información que permite identificar a las personas y que está disponible en Internet”²³¹.

Con anterioridad a esta sentencia, el TC en su sentencia 231/1988, de 2 de diciembre, empezó a asentar las bases del significado del derecho a la intimidad considerando que “el derecho a la intimidad personal y familiar se extiende, no solo a aspectos de la vida propia y personal, sino también a determinados aspectos de la vida de otras personas con las que se guarde una especial y estrecha vinculación, como es la familiar; aspectos que, por la relación o vínculo existente con ellas, inciden en la propia esfera de la personalidad del individuo que los derechos del art. 18 de la C.E. protegen” (FJ4).

Por primera vez, el Tribunal Supremo en su sentencia 19/2019²³², de 11 de enero de 2019, resolvió a favor del derecho a la protección de datos del reclamante frente al

²³⁰ LOPD. Artículo 3.a).

²³¹ SIMÓN CASTELLANO, P. (2011). *El Régimen Constitucional del Derecho al olvido en Internet en Neutralidad de la red y otros retos para el futuro de Internet*. Actas del VII Congreso Internacional Internet, Derecho y Política Universitat Oberta de Catalunya. Huygens. Barcelona, págs. 396-397.

²³² El caso está relacionado con una noticia publicada en el Diario El País y en el blog <http://cotodecazaserradogalineiro.blogspot.com/>, en la que se hacía referencia a que “los agentes de medio ambiente habían sorprendido a tres «furtivos» que eran trabajadores directos de la Administraron gallega, relatando seguidamente el enfrentamiento entre dichos «furtivos» y los agentes, que finalmente habían sido sancionados. También hace referencia a que los «presuntos furtivos» recibieron asimismo denuncia de Seprona que se desplazó al coto y que los guardias de Seprona identificaron a los «furtivos» que reconocieron que estaban cazando jabalíes. Se hace constar que los tres fueron multados por haber estacionado el vehículo en medio de una pista forestal, incumpliendo la ley de Incendios en Galicia”. El TS considera que los hechos publicados no responden a la realidad, al menos al relato que se contiene en la sentencia de la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia de Galicia, en

derecho a la libertad de expresión del buscador de Google al precisar que “aunque reconoce el interés público de la noticia y el interés legítimo de los internautas, resultaba necesario tomar en consideración, siguiendo los criterios expuestos en la jurisprudencia del Tribunal Constitucional y en la doctrina del Tribunal de Justicia de la Unión Europea así como la del Tribunal Europeo de Derechos Humanos, los riesgos que para el respeto a la vida privada del reclamante pudiera tener la divulgación de aspectos referidos a sus actividades de ocio. Por ello, estimamos que debía ponderarse adecuadamente tanto que la noticia se refería a hechos atribuidos a un funcionario público, que, aunque ocupase el puesto de jefe forestal de la Xunta de Galicia en Ourense, sus actuaciones carecían de particular notoriedad pues no ha quedado acreditado en autos que se trate de un personaje público o que desempeñase, indiciariamente, un papel destacado en la vida pública de esa Comunidad Autónoma, lo que diluye en gran medida el interés público de la información difundida a través de internet, así como que la noticia había perdido actualidad, teniendo en cuenta el tiempo transcurrido desde que se produjeron los hechos, lo que limita la trascendencia para la formación de una opinión pública informada, libre y plural en una sociedad democrática”.

En definitiva, en su fallo, el TS reconoce no haber lugar al recurso de casación de Google contra la sentencia de la Sección Primera de la Sala de lo Contencioso Administrativo de la Audiencia Nacional, de 18 de julio de 2017, porque “no cabe negar el carácter sensible que para la vida privada el derecho de protección de datos personales del reclamante tiene la difusión a través de internet por el buscador de Google, de diversa información que le relaciona sin justificación suficiente con la comisión de una infracción como cazador furtivo, por lo que la ausencia de exactitud de la información facilitada en los enlaces ofrecidos por el buscador de Google y su carácter lesivo para la privacidad, consideración social y profesional del reclamante, determina que, en la ponderación de intereses que la Sala debe efectuar, y a la vista de

la que se dice literalmente, que los agentes se habían reunido con diversos cazadores para «formar la cuadrilla previamente autorizada para ejercitar la caza en el terreno cinegético ordenado denominado PenaMaior, de cuyas resultas se producen unos incidentes por los cuales extienden aquellos denuncias a tres de ellos por proferir amenazas...»”. Lo que es evidente es que no es lo mismo, como reconoce el TS, “estar cazando como «furtivos», según aparece la noticia en El País y en el blog, al relato de hechos de la sentencia Tribunal Superior de Justicia de Galicia”.

los hechos expuestos, consideramos, compartiendo en este punto el criterio de la resolución combatida, que debe prevalecer en éste supuesto, el derecho a la protección de datos del reclamante sobre el derecho a la libertad de expresión del buscador de Google, y que el tratamiento de los datos personales del denunciante sin su consentimiento, realizado por el demandante no encuentra amparo en el legítimo ejercicio de la libertad de información, al no tener constancia de su veracidad, por lo que el reclamante ostenta un derecho a que dicha información no se vincule a su nombre a través de los buscadores de Internet”.

Además, en la sentencia, el TS expone que “el reconocimiento al derecho al olvido digital comporta otorgar al interesado la facultad de solicitar ante la entidad proveedora de servicios de motor de búsqueda en internet y ante la Agencia Española de Protección de Datos, conforme a lo dispuesto en el artículo 6 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, que cancele, suprima o prohíba la indexación de aquellos datos de la lista de resultados proporcionada por el motor de búsqueda obtenidos a partir de su nombre que se revelen inexactos, en la medida que cabe impedir injerencias ilegítimas en el derecho a la vida privada y familiar y en el derecho a la protección de datos personales. La decisión de la entidad responsable del tratamiento de datos o de la autoridad de control deberá necesariamente justificarse, para lograr ese justo equilibrio entre la libertad de información y el derecho al respeto a la vida privada con base en la valoración de la naturaleza y trascendencia de la información para el público y el tiempo transcurrido desde que se originó la noticia, puesto que el tratamiento de datos originariamente lícito puede devenir con el tiempo incompatible con la salvaguarda de los derechos personalísimos”.

Podríamos afirmar, por tanto, que el derecho al olvido no es un derecho fundamental, principalmente, por dos motivos. En primer lugar, obviamente, porque no aparece como tal recogido en la CE. En segundo lugar, el objeto principal de dicho derecho es borrar información del pasado de una persona que ésta considera innecesaria u obsoleta, considerando, en todo momento, que es veraz. En este sentido, la articulación del derecho al olvido se puede realizar a través de los derechos de rectificación o cancelación, estando, por tanto, limitado por los derechos constitucionales. Además, en el caso de que la información sea confusa o engañosa, podemos considerar el derecho al olvido como un derecho instrumental del derecho al honor.

5.2. DIFERENCIAS ENTRE INTIMIDAD Y VIDA PRIVADA

Es importante distinguir entre el concepto de privacidad, o mejor dicho vida privada, como recoge el artículo 8 del CEDH y el de intimidad, concretado por la CE en su artículo 18.1. Para Ignacio Villaverde, “la privacidad-vida privada es el género, la intimidad una de sus especies, y la autonomía personal puede ser o no su objeto”. El TEDH ha dado a la vida privada un concepto más amplio que “se extiende a las decisiones que tome el individuo sobre sus relaciones con terceros que tengan una conexión directa con su condición de persona y el libre desarrollo de su personalidad, mientras que la perspectiva española es más restrictiva, debido a que carecemos de un derecho fundamental genérico cuyo objeto sea el libre desarrollo de la personalidad o, simplemente, su libertad genérica de actuar como considere más conveniente”. El objeto del artículo 18.1 CE “no es la decisión sobre cómo vivir o una espacio que objetiva y materialmente quepa considerar como vida privada, sino la decisión sobre qué de nosotros pueden conocer los demás. En la CE se garantiza la intimidad, entendida no como lo íntimo, sino la decisión sobre qué queda reservado a la mirada ajena”²³³. Concretando, la intimidad es “el derecho de la persona a impedir cualquier intromisión sobre aquel ámbito de su vida privada, que considera vedado a los demás, salvo que medie su consentimiento”²³⁴.

Por su parte, Ruíz Miguel considera que “para interpretar el artículo 18 CE, es imprescindible acudir a la jurisprudencia del TEDH sobre la misma materia sobre la que recaiga el artículo 18 CE. El Convenio opera como norma de mínimos, de suerte que las exigencias que se deriven de dicho tratado en la interpretación por el TEDH de este derecho deberán ser cubiertas por el ordenamiento español; pues, de lo contrario, habría una violación del artículo 8 del meritado documento. Como se ha considerado, el control de constitucionalidad solo opera a partir del artículo 18 CE y no desde el artículo 8 CEDH. Sin embargo, en la medida en que dicho precepto, interpretado por el

²³³ VILLAVERDE MENÉNDEZ, I. (2013). La intimidad, ese “terrible derecho” en la era de la confusa publicidad virtual. *España Jurídico Journal of Law*. Vol 14, nº3, págs. 59-61.

²³⁴ CARRILLO LÓPEZ, M. (2008). La intimidad, las celebridades y el derecho a la información. *Diario La Ley* nº 6.979, año XXIX, pág. 1.

TEDH, incida sobre la materia regulada en el artículo 18 CE este deberá ser integrado e interpretado conforme a aquél”²³⁵.

Paulatinamente, como señala Murillo, se ha ido estableciendo que “los rasgos del derecho a la intimidad no permiten responder a los riesgos que proceden de la recopilación, tratamiento, almacenamiento y transmisión de datos personales por medio de las posibilidades que ofrecen la informática y la telemática o, si se prefiere, las Tecnologías de la Información y de las Comunicaciones. En este nuevo cambio, los instrumentos de tutela de la intimidad no son útiles en la mayor parte de los casos. Desde luego no lo son en todos aquellos supuestos en los que la información personal que se recaba y utiliza con propósitos variados no pertenece a ninguno de esos círculos que componen la intimidad”²³⁶.

Con Internet presente, la intimidad es más vulnerable, ya que “la red no condiciona jurídicamente nuestra autonomía personal (salvo casos de acoso cibernético) ni nuestra vida privada, sino nuestra intimidad en la medida en que en ella divulgamos o divulgan información relativa a nuestra persona”²³⁷. Por este motivo, podemos considerar el derecho al olvido como un mecanismo de protección de la intimidad en el tiempo, permitiendo a las personas evitar que se vulnere dicho derecho por contenidos divulgados en Internet.

5.3. EL DERECHO AL OLVIDO COMO DIMENSIÓN DEL CONTROL DE LOS DATOS PERSONALES

El derecho al olvido está, como apuntan Guasch y Soler, “íntimamente relacionado con el derecho a la protección de datos”, ya que, aunque “no existe en nuestra legislación una regulación concreta del derecho al olvido, una parte de la doctrina ha venido usando dicho término para referirse a otros derechos recogidos en la LOPD. Los derechos que

²³⁵ RUIZ MIGUEL, C. (1994). *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*. Civitas, Madrid, pág. 123.

²³⁶ MURILLO DE LA CUEVA, P. L. (2006). *El derecho a la libertad informática*. Documentos TICs (Derecho de las Tecnologías de la Información y Comunicación), págs. 4-5.

²³⁷ VILLAVERDE MENÉNDEZ, I. (2013). La intimidad, ese “terrible derecho... *ob. cit.*, pág. 62.

recoge que están íntimamente relacionados con el derecho al olvido, serían los derechos de oposición y de cancelación”²³⁸.

El derecho fundamental a la protección de datos personales aparece, por primera vez, recogido en las sentencias del TC 290/2000 y 292/2000, de 30 de noviembre, que, como señala Villaverde, “tienen la singularidad de que son ellas y, no sus antecedentes, las que formulan un derecho fundamental que no está expresamente mencionado en la CE. El apartado 4 del art.18 CE contiene a todas luces una reserva de ley y, sin embargo, el TC termina por convertir en cierto lo insinuado en otros de sus anteriores pronunciamientos: en ese apartado 4 hay un derecho fundamental implícito. El TC, digámoslo con claridad, inventa un derecho fundamental (hay que decir que con gran fortuna, aunque acaso no fuese aconsejable que el TC acudiese a esta técnica con frecuencia) donde no existía. Y lo hace sin acudir a razonamientos ligados a la dignidad y los derechos inviolables del art.10.1 CE; simplemente considera que en el art.18.4 CE, sin mayor explicación, se contiene un derecho fundamental y no sólo una reserva de ley. La consecuencia inmediata es que la LOPD 15/1999, de 13 de diciembre, deja de ser la norma que cumple con dicha reserva y que en ciertos extremos desarrolla los derechos fundamentales al honor y a la intimidad personal y familiar, para transformarse en la norma de desarrollo (art. 81.1 CE) del derecho fundamental a la protección de datos personales”²³⁹.

Como recoge el TC, “el derecho fundamental al que estamos haciendo referencia garantiza a la persona un poder de control y disposición sobre sus datos personales. Pues confiere a su titular un haz de facultades que son elementos esenciales del derecho fundamental a la protección de los datos personales, integrado por los derechos que corresponden al afectado a consentir la recogida y el uso de sus datos personales y a conocer los mismos. Y para hacer efectivo ese contenido, el derecho a ser informado de quién posee sus datos personales y con qué finalidad, así como el derecho a oponerse a

²³⁸ GUASCH PORTAS, V. y SOLER FUENSANTA, J. R. (2015). El derecho al olvido en Internet. *Revista de Derecho* nº16. UNED, págs. 992-993.

²³⁹ VILLAVARDE MENÉNDEZ, I. (2006). *La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos personales*, pág. 49; en FARRIOLS I SOLÁ, A. (coord.) (2006). *La protección de datos de carácter personal en los centros de trabajo*. Editorial Cinca. Colección Estudios Laborales.

esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos. En suma, el derecho fundamental comprende un conjunto de derechos que el ciudadano puede ejercer frente a quienes sean titulares, públicos o privados, de ficheros de datos personales, partiendo del conocimiento de tales ficheros y de su contenido, uso y destino, por el registro de los mismos. De suerte que es sobre dichos ficheros donde han de proyectarse, en última instancia, las medidas destinadas a la salvaguardia del derecho fundamental aquí considerado por parte de las Administraciones Públicas competentes” (STC 290/2000, de 30 de noviembre. FJ7).

Dicha sentencia concluye que “la exigencia constitucional de protección de los derechos fundamentales en todo el territorio nacional requiere que éstos, en correspondencia con la función que poseen en nuestro ordenamiento (art. 10.1 CE), tengan una proyección directa sobre el reparto competencial entre el Estado y las Comunidades Autónomas ex art. 149.1.1 CE para asegurar la igualdad de todos los españoles en su disfrute. Asimismo, que dicha exigencia faculta al Estado para adoptar garantías normativas y, en su caso, garantías institucionales. A este fin la LORTAD ha atribuido a la Agencia de Protección de Datos diversas funciones y potestades, de información, inspección y sanción, para prevenir las violaciones de los derechos fundamentales antes mencionados. Y dado que la garantía de estos derechos, así como la relativa a la igualdad de todos los españoles en su disfrute es el objetivo que guía la actuación de la Agencia de Protección de Datos, es claro que las funciones y potestades de este órgano han de ejercerse cualquiera que sea el lugar del territorio nacional donde se encuentren los ficheros automatizados conteniendo datos de carácter personal y sean quienes sean los responsables de tales ficheros” (FJ14). Por tanto, “la garantía de los derechos fundamentales exigida por la Constitución así como la de la igualdad de todos los españoles en su disfrute la que en el presente caso justifica que la Agencia de Protección de Datos y el Registro Central de Protección de Datos puede ejercer las funciones y potestades a las que antes se ha hecho referencia respecto a los ficheros informatizados que contengan datos personales y sean de titularidad privada radicados en Cataluña” (FJ15).

La sentencia TC 254/1993²⁴⁰, de 20 de julio, ha concretado, según señala Villaverde, “no sin cierta confusión, el contenido constitucional de lo que se conoce en la doctrina y jurisprudencia comparadas como derecho a la autodeterminación informativa”. Esta sentencia interpreta el artículo 10.2 CE, “permitiendo que una norma infraconstitucional sirva para precisar el contenido de los derechos fundamentales que la Constitución reconoce y no de otros derechos reconocidos en sedes distintas. Todo derecho fundamental, dada su formulación abstracta, requiere de un proceso de concreción de su contenido en el que, en virtud de dicho artículo, deben emplearse los tratados sobre derechos humanos, que ofrecen al intérprete criterios objetivos y congruentes sobre el contenido de las normas de derechos fundamentales. No puede confundirse la abstracción propia de las normas que garantizan derechos fundamentales con una supuesta apertura de su programa normativo a cualquier contenido jurídico posible que le venga incorporado por la concreta dogmática de los derechos fundaméntales que el intérprete elija para su concreción o por la remisión al contenido que prescriban normas internacionales o, incluso, normas nacionales infraconstitucionales. Una cosa es concretar el contenido de un derecho fundamental y otra muy distinta es crear nuevos derechos fundamentales sin tener en cuenta lo prescrito por la propia Constitución”²⁴¹.

Cuando la Constitución, como apunta Alonso García, “se aplica por primera vez a un nuevo presupuesto de hecho, lo que en realidad se produce es una actualización de la norma fundamental. La subsunción de un supuesto de hecho en un precepto

²⁴⁰ En la demanda se pide que se declare contraria a los arts. 18.1 y 4 de la Constitución la denegación presunta de la Administración, y que se le ordene acceder a la petición de información instada ante ella. El demandante solicitó, mediante escrito, que se le comunicase si la Administración del Estado o cualquier organismo de ella dependiente, dispone de ficheros automatizados donde figuren sus datos de carácter personal. En caso afirmativo, que se le indicase la finalidad principal de dichos ficheros, la autoridad que los controla y su residencia habitual y que se le comunicasen los datos existentes en dichos ficheros referidos a su persona, de forma inteligente y sin demora. El interesado fundó su solicitud en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981, y ratificado por Instrumento de 27 de enero de 1984, publicado en el BOE de 15 de noviembre de 1985, haciendo constar que entró en vigor de forma general y para España el 1 de octubre de 1985, tras haber sido ratificado por cinco de los Estados contratantes, de conformidad con lo establecido en su art. 22.2.

²⁴¹ VILLAVARDE MENÉNDEZ, I. (1994). Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993. *Revista española de Derecho Constitucional* n°41, pág. 187-195.

constitucional no implica tarea alguna de interpretación en su estricto sentido jurídico. Este fenómeno, a veces designado como concretización, llega a suponer una auténtica creación de un sistema de normas subconstitucionales que se denomina oficialmente doctrina, que opera como una norma-marco para sucesivas funciones de subsunción, equivaliendo, si el creador de la norma subconstitucional es el intérprete auténtico, a la Constitución misma”. En todos los sistemas con jurisdicción constitucional, “consideramos un hecho indiscutible que el intérprete judicial interpreta y formula normas derivadas de la Constitución, bien expresa, bien implícitamente. Denominamos interpretación, no tanto a la determinación del sentido jurídico de la norma, lo que realmente es la interpretación en estricto sentido técnico-jurídico, como al estudio del origen de tales normas subconstitucionales. Aunque resulta obvio que toda norma subconstitucional aclara el sentido de la norma primaria, el intérprete que tiene que aplicarla, judicialmente opera planteándose la legitimidad y validez de la norma subconstitucional que hace a la norma primaria funcional, no tratando tanto de averiguar su sentido como examinando a su luz las hipotéticas normas subconstitucionales posibles para ver cuál de entre ellas se ajusta más a la norma primaria. Esta óptica hace que podamos pretender que, dentro de las categorías de la teoría general del Derecho, sea la de la interpretación la que más se ajusta a la elaboración de normas subconstitucionales”²⁴².

El TC reconoce en su sentencia 254/1993, de 20 de julio, que “nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales. En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama la informática” (FJ6). Además, “cuando se opera con una reserva de configuración legal es posible que el mandato constitucional no tenga, hasta que la

²⁴² ALONSO GARCÍA, E. (1984). *La interpretación de la Constitución*. Centro de Estudios Constitucionales. Madrid, págs. 1-5.

regulación se produzca, más que un mínimo contenido, que ha de verse desarrollado y completado por el legislador. Pero de aquí no puede deducirse sin más que los derechos a obtener información ejercitados por el demandante de amparo no forman parte del contenido mínimo que consagra el art.18 CE con eficacia directa, y que debe ser protegido por todos los poderes públicos y, en último término, por este Tribunal a través del recurso de amparo (art.53 CE)” (FJ6).

Esta sentencia también plantea el problema de cuál deba ser ese contenido mínimo, provisional, en relación con este derecho que el ciudadano debe encontrar garantizado, aun en ausencia de desarrollo legislativo del mismo. “Un primer elemento, el más elemental, de ese contenido, es, sin duda, negativo, respondiendo al enunciado literal del derecho: el uso de la informática encuentra un límite en el respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos (STC 11/1981, de 8 de abril, FJ8). Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España. Pues, como señala el Ministerio Fiscal, la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data). En este sentido, las pautas interpretativas que nacen del Convenio de protección de datos personales de 1981 conducen a una respuesta inequívocamente favorable a las tesis del demandante de amparo. La realidad de los problemas a los que se enfrentó la elaboración y la ratificación de dicho tratado internacional llevan a la conclusión de que la protección de la intimidad de los ciudadanos requiere que éstos puedan conocer la existencia y los rasgos de aquellos ficheros automatizados donde las Administraciones públicas conservan datos de carácter personal que les conciernen, así como cuáles son esos datos personales en poder de las autoridades” (FJ7).

El TC parece querer fundamentar, según Villaverde, “el amparo a la luz del contenido del artículo 8 del CEDH, pero concibiendo el apartado 4 del artículo 18 CE como sede de un nuevo derecho fundamental de configuración legal: la libertad informática. El TC enturbiará sus razonamientos al intentar aplicar al caso su doctrina de los derechos fundamentales de configuración legal”. En el caso de que “el legislador prohibiese o

dificultase de forma tal el derecho a la autodeterminación informativa del individuo en lo tocante a la intimidad o al honor o no contemplase ese derecho para proteger otros intereses (cuya determinación y el alcance de su protección deja el constituyente en manos del legislador), estaría vulnerando los derechos fundamentales del artículo 18.1 en particular o los que se vieran afectados por la medida legislativa. Cosa distinta es que el legislador pueda establecer un derecho de prestación a cargo del Estado, convirtiendo su deber de publicidad, objeto del derecho a ser informado sobre la existencia, contenido y finalidad de ficheros automatizados, en un deber de información sobre esos datos o ampliar uno y otro deber a los ficheros no automatizados o cuya titularidad sea privada y no pública. Es en estos casos de creación de derechos de prestación, como ha destacado Ignacio de Otto y Pardo, donde cobra virtualidad la reserva de ley del artículo 53.1, dado el riesgo que late, cuando se derivan de un derecho de libertad derechos de prestación, de que la prestación imponga límites al mismo derecho de libertad que le sirve de fuente o a otros derechos de libertad”²⁴³.

El derecho fundamental a la protección de los datos “amplía la garantía constitucional a aquellos datos que sean relevantes o tengan incidencia en el ejercicio de cualquiera de los derechos de la persona, y por tanto con independencia de que sean o no relativos al honor, la ideología, la intimidad personal y familiar o cualquier otro constitucionalmente amparado. Luego, el objeto de la libertad informática no se reduce a la protección de los datos relativos a la intimidad o al honor de la persona como en un principio cabía pensar, sino que se extiende también a otros, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, ya sean fundamentales o no”. Además de la diferencia en el objeto, el derecho a la protección de datos presenta otra característica diferenciada del derecho a la intimidad y “es el poder jurídico que confiere a la persona de imponer a terceros el deber de abstenerse de toda intromisión en su esfera íntima, así como la estricta prohibición de hacer uso de los datos que hayan sido conocidos a través de la red informática”²⁴⁴.

Para Lucas Murillo, “hablar del derecho a la autodeterminación informativa es hablar de la protección de los datos de carácter personal, del mismo modo que tratar de la

²⁴³ VILLAVARDE MENÉNDEZ, I. (1994). *Protección de datos personales...ob. cit.*, págs. 202-210.

²⁴⁴ CARRILLO LÓPEZ, M. (2003). *El derecho a no ser molestado. Información y vida privada*. Aranzadi. Navarra, págs. 96-97.

protección de datos de carácter personal es tratar del derecho a la autodeterminación informativa. Hay, pues, plena coincidencia y la diferencia de denominaciones obedece a que, la primera, acuñada por Alemania y utilizada por su Tribunal Constitucional Federal en su Sentencia de 15 de diciembre de 1983 sobre la Ley del Censo, se fija en la principal facultad que encierra este derecho: la de que su sujeto, su titular, es decir, cualquier persona, decida, consienta de forma informada y libre el uso por terceros de datos que le conciernen. En cambio, la segunda denominación es la acogida por la LOPD, por nuestro TC y por el artículo 8 de la CEDH, utiliza una expresión que pretende denominar el conjunto de medios jurídicos a través de los cuales se satisface aquella facultad”. El autor prefiere hablar de autodeterminación informativa porque “si bien se trata de una fórmula poco estética, es, sin embargo, más precisa pues apunta al núcleo del derecho, a su aspecto sustantivo, mientras que la protección de los datos personales es su manifestación instrumental y, por eso, tiene un carácter técnico que le priva de capacidad significativa”. La sociedad aún no es consciente de “los derechos que nos asisten frente a la utilización por terceros de nuestros datos personales, sin una extendida conciencia en la sociedad de los riesgos que depara el uso incontrolado de la información personal que nos afecta y, por tanto, sin que los propios interesados sean conscientes de los peligros que les acechan, ni asuman, por tanto, su defensa frente a ellos, será difícil lograr un nivel de tutela satisfactorio”²⁴⁵.

El derecho al olvido puede considerarse, como destaca Durán, “un derecho derivado del derecho fundamental a la libertad informática o autodeterminación informativa, nace en respuesta al fenómeno de Internet y a dos de las características más importantes de esta red de comunicación: su memoria absoluta y la universalización de la información que en ella se encuentra cuando aparezcan en la página web original, ya que realmente es la indexación lo que facilita la difusión no querida de los datos. En realidad, el pretendido derecho al olvido no es algo tan novedoso ni la eliminación de los datos se configura como facultad distinta de la revocación del consentimiento, la oposición y la cancelación, de tal manera que puede concluirse que no es más que la manera de hacer

²⁴⁵ MURILLO DE LA CUEVA, P. L. (2008). El derecho a la autodeterminación informativa y la protección de datos personales. *Azpilcueta: Cuadernos de Derecho* n°20, pág. 44-51.

referencia generalizada al ejercicio de aquellas facultades, con el contenido específico que tiene cada una de ellas”²⁴⁶.

5.3.1. El derecho al olvido como seña de identidad personal

La identidad de una persona se puede definir, como señala Benavente, apoyándose en el diccionario de la RAE, como “el conjunto de rasgos propios de la misma que la caracteriza frente a los demás, así como la propia conciencia que la persona tiene de ser ella misma y distinta a las demás, en relación con su entorno contiguo o más cercano, en nuestro caso político y cultural y por ende jurídico”²⁴⁷.

El derecho al olvido amplía, como explica Gomes de Andrade, “el alcance del derecho a la identidad personal, abarcando no solo el derecho a construir la futura historia de nuestra identidad, sino también el derecho a borrar nuestro pasado, jugando un papel esencial no en el proceso de construcción de la identidad, sino en el proceso de deconstrucción de la identidad, permitiendo construir después identidades nuevas y diferentes. La conceptualización del derecho al olvido desde la perspectiva de la identidad, por otra parte, sigue la línea antiesencialista mediante la cual la ley ha estado regulando la identidad personal. De hecho, la ley ha dotado a los individuos con más y más instrumentos legales con los que pueden influir y cambiar aspectos de su identidad. Las personas, hoy en día, tienen derecho a romper las cadenas de filiaciones, modificar nombres, abandonar nacionalidades y cambiar de sexo. El derecho al olvido puede desarrollar un papel muy importante para que una persona pueda reconstruir su narrativa identitaria, teniendo la certeza de que las identidades pasadas no ponen en peligro ese proceso”. Para el autor, el derecho al olvido “está en el núcleo del interés y valor principales que trata de lograr el derecho a la identidad personal: el interés por la propia singularidad, el interés por ser diferente de los demás y de uno mismo, es decir, del que uno era antes. En consecuencia, el derecho al olvido –como parte del derecho a la identidad personal– está íntimamente ligado a la capacidad de reinventarse, de tener una

²⁴⁶ DURÁN RUIZ, F. (2014). *Autodeterminación informativa y derecho al olvido en la Unión Europea, particularidades respecto de los menores de edad*. Actas del VII simposio de Las sociedades ante el reto digital, págs. 173-174.

²⁴⁷ BENAVENTE MORADA, P. (2013). Identidad y contexto inmediato de la persona. *Anuario de la Facultad de derecho* nº17. Universidad Autónoma de Madrid, pág. 107.

segunda oportunidad, de empezar de nuevo y presentar una identidad renovada al mundo”²⁴⁸.

Una violación a la privacidad, como señalan Abril y Pizarro, “deja a la persona a merced de la querrela y el escrutinio públicos. Esta desnudez ante el mundo exterior entrega a la persona y a su sentido de auto vulnerabilidad de una manera ofensiva a su dignidad humana. Una mirada a la privacidad enfocándose en el aspecto de la dignidad humana implica inevitablemente el reflejo del desarrollo de la personalidad *per se* y del yo interior. Desde este punto de vista, la privacidad implica 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. Al hacer esto, el individuo divulga aspectos de su privacidad en diferentes ambientes y en diferentes contextos. El riesgo mayor es la falta de capacidad de libremente administrar qué información privada fue divulgada y en qué contexto, lo cual conlleva a consecuencias sociales catastróficas”. El derecho a la protección de la vida privada, “plantea la creación y el mantenimiento de una identidad personal, una intimidad, y de una comunidad. Así, los países europeos siguen de una u otra forma esta noción centrada en la protección de la dignidad humana y, consecuentemente, la entienden como un derecho inherente a la personalidad. La consagración legislativa suprema de esa noción aparece recogida en el artículo 8.1 de la CEDH”²⁴⁹.

En el contexto de Internet, para De Terwangne, “la privacidad no se debe interpretar como intimidad sino más bien como autonomía individual, la capacidad de elegir, de tomar decisiones informadas, en otras palabras, a mantener el control sobre diferentes aspectos de nuestra propia vida. Esta dimensión de la privacidad significa autonomía informativa o autodeterminación informativa”. Si nos centramos en los datos personales que circulan por Internet, “la autonomía individual está en relación directa con la información personal. La libre determinación sobre la información significa tener el

²⁴⁸ GOMES DE ANDRADE, N. N. (2012). El olvido: El derecho a ser diferente... de uno mismo Una reconsideración del derecho a ser olvidado. *Revista de Internet, Derecho y Política* nº13, febrero. Universitat Oberta de Catalunya, pág. 88.

²⁴⁹ ABRIL, P. y PIZARRO MORENO, E. (2014). La intimidad europea frente a la privacidad americana. *Revista InDret*. Barcelona, pág. 9.

control sobre nuestra información personal, es decir, es el derecho de los individuos a decidir qué información sobre ellos mismos será revelada, a quién y con qué objetivo”. El concepto de información personal o datos personales “debe interpretarse en un sentido amplio, ya que no debe estar vinculado a la idea de la intimidad personal propia de un planteamiento clásico de la privacidad. Más bien significa cualquier información relacionada con una persona física (datos profesionales, comerciales y datos hechos públicos). En Europa, esta autodeterminación informativa ha sido reconocida y protegida como un derecho a la protección de los datos personales”²⁵⁰.

Por tanto, podemos considerar que la relación del derecho al olvido con el derecho a la identidad personal no es más que una forma distinta de interpretar la relación del derecho al olvido con el de la protección de datos personales, ya que la identidad como conjunto de rasgos propios de la persona, cuando nos referimos a Internet, se relaciona directamente con los datos personales que son los que configuran realmente la personalidad humana.

5.4. EL RECONOCIMIENTO DEL DERECHO AL OLVIDO COMO UN DERECHO DE SUPRESIÓN

El reconocimiento del derecho al olvido se formalizó con la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, aplicable desde el 25 de mayo de 2018 y donde, por primera vez, aparece recogido dicho concepto. Eso sí, no deja de ser un concepto asociado al derecho de supresión y no aporta nada nuevo a las medidas que se venían adoptando hasta ahora por las diferentes agencias europeas de protección de datos, ya que el interesado “tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernen y abstenerse de darles más difusión”²⁵¹. Además, cuando el responsable del tratamiento

²⁵⁰ DE TERWANGNE, C. (2012). Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. *Revista de Internet, Derecho y Política* nº13, febrero. Universitat Oberta de Catalunya, págs. 54-55.

²⁵¹ Así lo recoge el artículo 17.1, que señala también los supuestos en los que el responsable estará obligado a suprimir dichos datos siempre que concurra alguna de las circunstancias siguientes: “a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados

haya hecho públicos los datos y esté obligado suprimirlos, según recoge el Reglamento (UE) 2016/679, “teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos”²⁵².

Desde su entrada en vigor, se prevé, como apunta Ordóñez, “un desarrollo legislativo del derecho al olvido que ejercerá la Comisión Europea en cuanto a la determinación de sus criterios y requisitos en sectores y situaciones específicas de tratamiento de datos; las condiciones para la supresión de enlaces, copias o réplicas de datos personales procedentes de servicios de comunicación accesibles al público; y los criterios y condiciones para limitar el tratamiento de datos personales”²⁵³. Un avance significativo, ya que, como expone Martínez, “el hecho de que exista una protección reforzada para los usuarios a través de un mayor control sobre sus propios datos personales, a través

de otro modo; 4.5.2016 ES Diario Oficial de la Unión Europea L 119/43 b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico; c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2; d) los datos personales hayan sido tratados ilícitamente; e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento; f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1”.

²⁵² Artículo 17.2. En el siguiente artículo, se exponen los casos en los que los apartados 1 y 2 del Reglamento no se aplicarán cuando el tratamiento sea necesario: para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones”.

²⁵³ ORDÓÑEZ SOLÍS, D., *La protección judicial de los derechos en Internet en la jurisprudencia europea*. Colección de derecho de las nuevas tecnologías. Editorial Reus. Madrid, 2014. Págs. 29-30.

del derecho al olvido digital, supone un paso importante hacia la reafirmación de que la dignidad y libertad personal deben tener garantías específicas a través de una autodeterminación informativa que permita a los usuarios colocarse en igualdad de condiciones para enfrentarse a los daños potenciales que brinda la hipermnesia del mundo virtual y el uso que de sus datos el mercado y la sociedad haga de ellos”²⁵⁴.

Hasta la entrada en vigor del reglamento, el denominado derecho al olvido no se encontraba recogido como tal en ninguna legislación, aunque la AEPD aplicaba la LOPD y, en concreto, los derechos de cancelación, oposición y rectificación para aplicarlo. Ahora, se reconoce como un derecho, eso sí, de supresión de datos o imágenes. El nuevo Reglamento reconoce que: “los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen y un derecho al olvido si la retención de tales datos infringe el presente Reglamento o el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento. En particular, los interesados deben tener derecho a que sus datos personales se supriman y dejen de tratarse si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo, si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen, o si el tratamiento de sus datos personales incumple de otro modo el presente Reglamento. Este derecho es pertinente en particular si el interesado dio su consentimiento siendo niño y no se es plenamente consciente de los riesgos que implica el tratamiento, y más tarde quiere suprimir tales datos personales, especialmente en internet. El interesado debe poder ejercer este derecho aunque ya no sea un niño. Sin embargo, la retención ulterior de los

²⁵⁴ MARTÍNEZ LÓPEZ-SÁEZ, M. (2017). Los nuevos límites al derecho al olvido en el sistema jurídico... *ob. cit.*, pág. 176. PIÑAR MAÑAS, J. L. (dir.) (2017). *Reglamento general de protección de datos ob. cit.*, págs. 14-15; añade que este nuevo modelo de uso responsable de la información “incrementa la idea de responsabilidad proactiva y el ámbito de la autorregulación, pero al mismo tiempo se fortalece el aspecto institucional, a nivel nacional y de la Unión Europea. Además, no es en absoluto más sencillo que el anterior. De entrada, las reglas del juego son más uniformes a nivel de la Unión Europea, pero al mismo tiempo se deja mayor margen de apreciación y valoración a los responsables y encargados. La falsa idea de que es suficiente el cumplimiento formal de las obligaciones que fijan la ley y el reglamento ha de quedar definitivamente superada. A partir de ahora será necesario adoptar decisiones propias en función de los tratamientos de datos que se lleven cabo y de la naturaleza de éstos. Algo que va a estar mucho más al alcance de las grandes compañías y Administraciones públicas, pero no tanto de las pymes y pequeños organismos públicos”.

datos personales debe ser lícita cuando sea necesaria para el ejercicio de la libertad de expresión e información, para el cumplimiento de una obligación legal, para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, por razones de interés público en el ámbito de la salud pública, con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, o para la formulación, el ejercicio o la defensa de reclamaciones” (considerando 65).

Además, a fin de reforzar el derecho al olvido en el entorno en línea, “el derecho de supresión debe ampliarse de tal forma que el responsable del tratamiento que haya hecho públicos datos personales esté obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales que supriman todo enlace a ellos, o las copias o réplicas de tales datos. Al proceder así, dicho responsable debe tomar medidas razonables, teniendo en cuenta la tecnología y los medios a su disposición, incluidas las medidas técnicas, para informar de la solicitud del interesado a los responsables que estén tratando los datos personales” (considerando 66). Entre los métodos para limitar el tratamiento de datos personales cabría “incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema”. (Considerando 67).

Lo que queda claro con la aprobación de este reglamento, como apunta Berrocal, es que el derecho al olvido “no es un derecho absoluto, pues, tiene unos límites que establece el artículo 17 en su apartado 3²⁵⁵ y que exige en cada caso un juicio ponderado

²⁵⁵ El artículo 17.3 recoge que: “Los apartados 1 y 2 no se aplicarán cuando el tratamiento sea necesario: a) para ejercer el derecho a la libertad de expresión e información; b) para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable; c) por razones de interés público en el ámbito de la salud pública de conformidad con el artículo 9, apartado 2, letras h) e

atendiendo entre otros criterios: la naturaleza privada o pública de la información, la relevancia pública o no de la misma, el contexto en que se divulga, el interés del público en disponer de la información que puede variar en función del papel que la persona afectada desempeñe en la vida pública y el tiempo transcurrido que puede determinar que la información deje de tener actualidad, interés público o en fin, vigencia pública y ya no resulte pertinente para la finalidad informativa que ha de cumplir y que, en su momento, cumplió”. La autora relaciona este derecho de supresión de los datos con “la prescripción de oficio o a instancia de parte de los antecedentes penales, con la anonimización de las sentencias, con la amnistía o el indulto”²⁵⁶.

5.5. LÍMITES DEL DERECHO AL OLVIDO

5.5.1. Las hemerotecas digitales como estandartes de la libertad de información

La sentencia del TC 58/2018, de 4 de junio de 2018 cambia completamente esta idea al reconocer “expresamente el derecho al olvido como facultad inherente al derecho a la protección de datos personales, y por tanto como derecho fundamental²⁵⁷, lo que supone

i), y apartado 3; d) con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en la medida en que el derecho indicado en el apartado 1 pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento, o e) para la formulación, el ejercicio o la defensa de reclamaciones”.

²⁵⁶ BERROCAL LANZAROT, A. I. (2017). *Derecho de supresión de datos... ob. cit.*, pág. 298.

²⁵⁷ PIÑAR MAÑAS, J. L. (2018). *El derecho al olvido... ob. citada*, reconoce que “esta afirmación es de enorme relevancia. Lo que trae consigo una consecuencia lógica: el reconocimiento como derecho fundamental supone la automática aplicación de la jurisprudencia relativa a los límites de los derechos fundamentales, en particular el límite que suponen otros derechos; y entre ellos, especialmente, la libertad de información (art. 20.1.d) de la Constitución). Centrándose el Tribunal en la libertad ejercida en el entorno de las hemerotecas digitales, a las que se circunscribe el asunto”. En este sentido, TORRES MANRIQUE, J. I. (2018). Analizando el derecho fundamental al olvido a propósito de su reciente reconocimiento y evolución. *Revista general de derecho constitucional* nº27, págs. 6-7; señala que “*a priori* podemos colegir la naturaleza de oportunidad entre los derechos fundamentales a la privacidad y al olvido. En el primer caso, se ejercita principalmente *ex ante*, esto es, de manera anterior a la posible publicación de la información, a diferencia del segundo, donde siempre se manifiesta *ex post*, es decir, luego de haberse publicado, ya sea con el consentimiento o no del perjudicado... Así, postulamos que el derecho fundamental al olvido, proviene de un derecho más amplio, que el denominado derecho a Internet. A la vez, el derecho a la intimidad guarda estrecha relación con el derecho al olvido; existiendo entre ellos una relación de género y especie, respectivamente”.

la automática aplicación al mismo de la jurisprudencia relativa a los límites de los derechos fundamentales” (FJ 6). En el caso concreto de la sentencia, “se identifica la libertad de información [art. 20.1 d) CE] como el derecho fundamental que podría actuar como límite del derecho de autodeterminación sobre los propios datos personales”. Los datos personales cuya supresión se solicita por las personas recurrentes están contenidos en la hemeroteca digital de Ediciones El País, y el recurso de amparo está relacionado con el “rechazo a ocultar los nombres de las personas recurrentes u oscurecerlos a través del uso de sus iniciales. No estamos, por tanto, ante un nuevo conflicto con los motores de búsqueda de los que han ocupado al Tribunal Supremo (por todas, SSTS 1917/2016, de 21 de julio; 1618/2016, de 4 de julio; 210/2016, de 16 de marzo), sino ante un conflicto circunscrito al uso de nombres propios como criterio de búsqueda y localización de noticias en el entorno de una hemeroteca digitalizada” (FJ 6). En este contexto, los derechos que colisionan son, de un lado, “el derecho a la supresión de datos de una base informatizada (art. 18.4 CE), en relación mediata e instrumental con la garantía del derecho al honor y la intimidad de las personas a las que conciernen los datos (art. 18.1 CE) y las libertades informativas *ex art. 20.1 d) CE*”.

En España, el artículo 20.1 CE garantiza la libertad de expresión y la libertad de información. Mientras que en otras Constituciones, como expone Bastida, “el reconocimiento de la libertad de información se entiende implícito en el de libertad de expresión, el art.20.1 menciona en apartados distintos el derecho a expresar y difundir libremente los pensamientos, ideas y opiniones (apartado a) y el derecho a comunicar o recibir libremente información veraz (apartado d) sea cual sea el medio de difusión empleado. Inicialmente el TC no dio mayor importancia a este reconocimiento y consideró el apartado d) como una mera explicación de la libertad de expresión (STC 6/1981²⁵⁸, de 16 de marzo)”²⁵⁹. Si nos atenemos a las consideraciones del Reglamento

²⁵⁸ FJ4: “La libertad de expresión que proclama el art. 20.1 a) es un derecho fundamental del que gozan por igual todos los ciudadanos y que les protege frente a cualquier injerencia de los poderes públicos que no esté apoyada en la Ley, e incluso frente a la propia Ley en cuanto ésta intente fijar otros límites que los que la propia Constitución (arts. 20.4 y 53.1) admite. Otro tanto cabe afirmar respecto del derecho a comunicar y recibir información veraz (art. 20.1.d), fórmula que, como es obvio, incluye dos derechos distintos, pero íntimamente conectados. El derecho a comunicar que, en cierto sentido, puede considerarse como una simple aplicación concreta de la libertad de expresión y cuya explicitación

(UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 que en su artículo 17 señala que se excluye de la delimitación del derecho al olvido “el tratamiento de información con fines periodísticos”.

En nuestro sistema constitucional, como apunta Urías, “parece prohibida la limitación de derechos, en el sentido de que los derechos son lo que son, y su fuerza radica en que no pueden ser restringidos ni limitados por el poder en perjuicio de los ciudadanos. Aunque la limitación está prohibida, sí es posible la delimitación, que sería la operación por la cual se aclara cuál es el contenido de un derecho”. Aplicado todo esto a la libertad de información, “hay que entender que el legislador no puede establecer límites a la libertad de información que cubra la difusión de informaciones veraces y públicamente relevantes a través de cualquier medio de difusión y sin incluir insultos. En cambio, sí puede delimitar la libertad de información y decidir que no está incluido en ésta, por ejemplo, la difusión de informaciones televisivas pornográficas en determinados horarios”²⁶⁰.

Fue a raíz de la STC 20/1992, de 14 de febrero, cuando el TC define la libertad de información y entiende que tiene un objeto distinto al de libertad de expresión y establece que “es un derecho al que la Constitución dispensa, junto a otros de su misma dignidad, la máxima protección, y su ejercicio está ligado, como repetidamente hemos dicho (desde la STC 6/1981, FJ3), al valor objetivo que es la comunicación pública libre, inseparable de la condición pluralista y democrática del Estado en que nuestra comunidad se organiza. Pero cuando tal libertad se quiere ejercer sobre ámbitos que pueden afectar a otros bienes constitucionales, como son el honor y, en este caso, la intimidad, es preciso para que su proyección sea legítima, que lo informado resulte de interés público (STC 171/1990, de 12 de noviembre. FJ5), pues sólo entonces puede

diferenciada sólo se encuentra en textos constitucionales recientes, es derecho del que gozan también; sin duda, todos los ciudadanos, aunque en la práctica sirva, sobre todo, de salvaguardia a quienes hacen de la búsqueda y difusión de la información su profesión específica; el derecho a recibir es en rigor una redundancia (no hay comunicación cuando el mensaje no tiene receptor posible), cuya inclusión en el texto constitucional se justifica, sin embargo, por el propósito de ampliar al máximo el conjunto de los legitimados para impugnar cualquier perturbación de la libre comunicación social”.

²⁵⁹ BASTIDA FREIJEDO, F. J. (1994). *El régimen jurídico de la comunicación social*. Instituto de Estudios Económicos. Madrid, pág. 7.

²⁶⁰ URÍAS, J. (2003). *Lecciones de derecho de la información*. Tecnos. Madrid, pág. 169.

exigirse de aquellos a quienes afecta o perturba el contenido de la información que, pese a ello, la soporten en aras, precisamente, del conocimiento general y difusión de hechos y situaciones que interesan a la comunidad. Tal relevancia comunitaria, y no la simple satisfacción de la curiosidad ajena, con frecuencia mal orientada e indebidamente fomentada, es lo único que puede justificar la exigencia de que se asuman aquellas perturbaciones o molestias ocasionadas por la difusión de una determinada noticia, y reside en tal criterio, por consiguiente, el elemento final de valoración para dirimir, en estos supuestos, el conflicto entre el honor y la intimidad, de una parte, y la libertad de información, de la otra” (FJ3).

La libertad de información tiene una función esencial para el correcto funcionamiento del Estado social y democrático de Derecho, de acuerdo a “los requisitos básicos de tutela de los derechos fundamentales basados en el control represivo o *a posteriori* del ejercicio del derecho. La CE rechaza cualquier vía que pueda suponer la institucionalización de un control preventivo, que es la forma habitual empleada en los regímenes autoritarios”. Por esta razón, la CE establece “dos cláusulas de exclusión de control *a priori* al ejercicio de los derechos reconocidos en el artículo 20: la censura previa y el secuestro administrativo de publicaciones, programas o soportes de comunicación”²⁶¹. El TEDH subrayó en su sentencia en el caso *Handyside v. Reino Unido*, de 29 de abril de 1976, que los órganos del Convenio, en el ejercicio de su misión revisora, deben prestar la máxima atención a los principios característicos de una sociedad democrática, afirmando que “la libertad de expresión constituye uno de los fundamentos esenciales de tal sociedad, una de las condiciones primordiales para su progreso y para el desarrollo de los hombres. Al amparo del artículo 10.2 es válido no sólo para las informaciones o ideas que son favorablemente recibidas o consideradas como inofensivas o indiferentes, sino también para aquellas que chocan, inquietan u ofenden al Estado o a una fracción cualquiera de la población. Tales son las demandas del pluralismo, la tolerancia y el espíritu de apertura, sin las cuales no existe una sociedad democrática. Esto significa especialmente que toda formalidad, condición, restricción o sanción impuesta en la materia debe ser proporcionada al fin legítimo que se persigue. Por otra parte, cualquiera que ejerce su libertad de expresión asume deberes y responsabilidades, cuyo ámbito depende de su situación y del procedimiento técnico

²⁶¹ CARRILLO LÓPEZ, M. (2003). *El derecho a no ser molestado... ob. cit.*, pág. 58.

utilizado. Analizando, como en este supuesto, si las restricciones o sanciones procuraban una protección de la moral, que las hiciera necesarias en una sociedad democrática, el Tribunal no podría hacer abstracción de los deberes y responsabilidades del interesado” (Punto 49).

El TEDH también asentó en su sentencia caso *Lingens c. Austria*²⁶², de 8 de julio de 1986, la diferencia entre libertad de expresión y derecho a la información, basándose en el artículo 10 del CEDH (“1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones e ideas sin que puedan injerirse en ellas las autoridades públicas y sin consideración de fronteras. Este artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa. 2. El ejercicio de estas libertades, que implica deberes y responsabilidades, podrá someterse a determinadas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que sean medidas necesarias en una sociedad democrática para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones reservadas o para garantizar la autoridad y la imparcialidad del Poder Judicial”). La cuestión tratada en los artículos del demandante tenía “un interés fundamental en la discusión política general de Austria en las fechas en que ocurrieron los hechos. Los artículos se publicaron poco después de las elecciones generales y antes de la formación de un nuevo Gobierno. Con anterioridad a las elecciones muchos creían posible que el Kreisky formaría Gobierno de coalición con el Partido Liberal si su propio partido, el socialista, no lograba obtener la mayoría absoluta. Y aunque el resultado de las elecciones puso de manifiesto que no habría Gobierno de coalición, las relaciones entre los señores Kreisky y Peter suscitaban todavía la atención general, sobre todo desde que el Director del Centro de

²⁶² El periodista austríaco Lingens fue denunciado por el ex canciller, Bruno Kreisky, que promovió dos procedimientos penales contra él al considerar difamatorios algunos trozos de los artículos publicados en la revista *Profil*, en los que se censuraba la actitud de Kreisky, al que criticaba por proteger, por motivos políticos, a Friedrich Peter, Presidente del Partido Liberal de Austria, y a otros antiguos miembros de las SS que participaban en la vida política austríaca y le acusaba de falta de tacto hacia las víctimas de los nazis (Puntos 8-19).

Documentación Judía, señor Wiesenthal, dio a conocer poco después de las elecciones la participación, hasta entonces no publicada, del señor Peter en una brigada de las SS. Los ataques en público del señor Kreisky al señor Wiesenthal a este respecto provocaron una gran emoción. En la medida en que los hechos de que se trata ya del conocimiento público fueron relatados o expuestos de nuevo en los artículos, no se alegó al ejercitar el señor Kreisky su acción contra el demandante que se hubieran recogido indebidamente las declaraciones de aquél sobre los señores Peter y Wiesenthal o las circunstancias en que se hicieron las declaraciones. A los efectos del artículo 10.1 del Convenio se puede decir, por consiguiente, que no fue afectado el derecho del demandante de comunicar informaciones”. Realmente, el TEDH sólo sancionó al periodista porque “expresó en la prensa determinadas opiniones sobre el comportamiento del señor Kreisky, considerándolo muy cercano al «peor oportunismo» y como «inmoral» e «indigno», es decir solamente fue atacado el derecho del demandante de comunicar sus ideas” (Puntos 61-65).

La libertad de información no puede restringirse mediante ningún tipo de censura previa y así lo recoge la sentencia de TC 187/1999, de 25 de octubre, que la define como “la intervención preventiva de los poderes públicos para prohibir o modular la publicación o emisión de mensajes escritos o audiovisuales. La presión de ciudadanos o grupos de ellos para impedir esa difusión, aunque consiga obtener el mismo resultado, puede llegar a ser una intromisión en un derecho ajeno, con relevancia penal en más de un caso y desde más de un aspecto, pero no censura en el sentido que le da la Constitución. Tampoco encaja en este concepto la que a veces ha dado en llamarse autocensura, utilizada en algunos sectores -la cinematografía o la prensa-, en algunos países o en algunas épocas para regular la propia actividad y establecer corporativamente ciertos límites. Más lejos aún del concepto constitucionalmente proscrito está la carga, con su cara y reverso de derecho-deber, que permite e impone a los editores y directores un examen o análisis de texto y contenidos, antes de su difusión, para comprobar si traspasan, o no, los límites de las libertades que ejercen, con especial atención a los penales. Se trata de algo que, en mayor o menor grado, precede siempre a la conducta humana, reflexiva y consciente de que el respeto al derecho ajeno es la pieza clave de la convivencia pacífica. En tal sentido hemos dicho ya que la «verdadera censura previa» consiste en «cualesquiera medidas limitativas de la elaboración o difusión de una obra del espíritu, especialmente al hacerlas depender del previo examen oficial de su

contenido» (STC 52/1983, de 17 de junio. FJ5). Por ello el derecho de veto que al director concede el art.37 de la Ley de Prensa e Imprenta de 18 de marzo de 1966 no puede ser identificado con el concepto de censura previa (SSTC 171/1990 y 172/1990, de 12 de noviembre). Tampoco lo es la autodisciplina del editor, cuya función consiste en elegir el texto que se propone publicar, asumiendo así los efectos positivos o negativos, favorables o desfavorables de esa opción, como puedan ser el riesgo económico y la responsabilidad jurídica (STC 176/1995, de 11 de diciembre)” (FJ5).

Internet no es más que “un mero conducto de transmisión y como tal, no comporta una alteración cualitativa de los elementos esenciales que determinan el régimen jurídico de la comunicación pública. La puesta a disposición a través de la red de contenidos audiovisuales no deja de ser, en última instancia, una actividad homologable a la que se hace cuando esos mismos productos se difunden por otros medios”²⁶³.

El conflicto entre el derecho al olvido y el ejercicio de la libertad de expresión e información por los medios de comunicación puede darse, según Mieres, en dos hipótesis principales: “la publicación actual de una información pasada y el mantenimiento de noticias publicadas en los archivos digitales del medio de comunicación accesibles en línea. El primer grupo de casos puede resolverse a partir de los criterios consolidados sobre los conflictos entre los derechos de la personalidad y las libertades comunicativas. El segundo, en cambio, presenta algunas peculiaridades que precisan una adaptación de los criterios generales de ponderación”.

Al respecto, considera que “la publicación nueva de una información pasada puede lesionar el derecho al olvido como proyección del derecho a la intimidad o del derecho al honor. Esa información pasada puede afectar negativamente la opinión que los demás hayan de formarse de nosotros, por lo que, con independencia de que sea verdadera, por su contenido distorsionador de la imagen y reputación que merece la persona puede considerarse lesiva de su honor. En uno y otro caso, el conflicto con el derecho a la libertad de información debe resolverse a partir de la apreciación de un interés público actual que justifique la imposición al afectado del deber de tolerar esa nueva publicación”. Otro aspecto importante que podría solucionar el conflicto entre la

²⁶³ GUICHOT REINA, E. (coord.) (2015). *Derecho de la comunicación*. Iustel. Madrid, págs. 199-200.

libertad de información y el derecho al olvido podría partir de la obligación “de los medios de comunicación de actualizar o contextualizar de aquellas noticias publicadas y accesibles en sus hemerotecas digitales que devengan inexactas o incompletas con el paso del tiempo, limitando el derecho al olvido de los afectados. El alcance de ese deber no puede extenderse a cualquier tipo de información, sino sobre aquellas que por su contenido tengan una capacidad significativa de afectar los derechos de los particulares (el caso central es el de la información sobre investigaciones penales que posteriormente no se confirman o sobre una condena inicial que se revoca después)”²⁶⁴.

La organización Reporteros sin Fronteras publicó en 2012 su informe anual en el que fue bastante crítico con el derecho al olvido y, sobre todo, con la propuesta de directiva, por parte de la vicepresidenta de la Comisión Europea y Comisaria de Justicia, Derechos Fundamentales y Ciudadanos, Viviane Reding, que permita a cualquier persona solicitar la supresión de contenidos de carácter personal por razones legítimas, delimitando considerablemente la libertad de información. Consideran que “un derecho al olvido generalizado, consagrado en una ley, sería difícil de conciliar con la libertad de expresión y de información en línea” Además, “sería difícil de aplicar en la práctica y podría plantear una obligación imposible a editores de contenidos y empresas de alojamientos a la hora ejecutar la supresión completa de los contenidos en línea”. La organización plantea un debate a fondo para determinar “si los derechos individuales no están ya suficientemente garantizados por las disposiciones legales vigentes sobre el derecho a la privacidad, los delitos de prensa y la protección de datos”²⁶⁵.

La Comisión Europea de Justicia, a través de una carta elaborada por Matthew Newman, portavoz de Viviane Reding, no tardó en responder a dicho informe y aclarar los puntos más conflictivos sobre el derecho al olvido, recordando que “la aplicación del derecho al olvido dentro de la legislación europea de protección de datos no afectará el trabajo de los periodistas para informar sobre contenidos de interés público y, en ningún caso, impedir el papel crucial de los periodistas en nuestra sociedad. La idea es dar más control a los usuarios para que puedan solicitar que su información personal (perfiles, fotos o contactos) que aparece en línea, pueda eliminarse de forma permanente si ellos

²⁶⁴ MIERES MIERES, L. J. (2014). *El derecho al olvido... ob. cit.*, págs. 28-38.

²⁶⁵ *Beset by online surveillance and content filtering, netizens fight on.* (<https://rsf.org/en/reports/beset-online-surveillance-and-content-filtering-netizens-fight>). Informe publicado el 12 de marzo de 2012.

no quieren que esta información sea utilizada y si no hay ninguna razón legítima para retener dichos datos”. Por tanto, el objetivo no es que alguien borre todos sus datos, sobre todo, si “la retención de los datos es necesario para la ejecución de un contrato o para el cumplimiento de una obligación legal, los datos podrían mantenerse durante el tiempo necesario para tal fin”²⁶⁶.

No hay que olvidar, como reconoce Cotino, que “toda la información y expresión de interés o relevancia pública en internet goza de protección constitucional, aunque no proceda de un clásico medio de comunicación social”. En el conflicto entre libertad de información y protección de datos pueden resultar útiles algunas pautas para determinar “qué información tiene interés público con independencia de su origen, así como establecer concreciones sobre algunos requisitos o garantías de la veracidad y diligencia tanto respecto de los contenidos, como de quiénes son sus autores (necesidades de identificación de quienes introducen contenidos en la red). Asimismo es de interés que la legislación parta de que los grandes prestadores o intermediarios son agentes, instrumentos y vehículos esenciales de las libertades informativas en el mundo actual, lo cual debe tenerse bien presente en cualquier regulación de su régimen jurídico o en la imposición de deberes o restricciones. Es posible atribuir la protección constitucional de las libertades informativas al tiempo de exigir para ello condiciones de diseño por defecto de los servicios o aplicaciones”²⁶⁷.

Cuando colisionan las libertades informativas con el derecho a la protección de datos hay que atender, según Simón, “a tres criterios: el interés público, el estudio del contexto en el que se difunde la información y aplicar el principio de proporcionalidad concebido por el Tribunal Constitucional. La veracidad sería un criterio irrelevante, ya que por sí sola no excluye la ilegitimidad de la intromisión, que se produce por el

²⁶⁶ Viviane Reding responds to Reporters Without Borders’ criticism of “right to be forgotten”. (<https://rsf.org/en/news/viviane-reding-responds-reporters-without-borders-criticism-right-be-forgotten>). Información publicada el 16 de marzo de 2012.

²⁶⁷ COTINO HUESO, L. (2015). *El conflicto entre las libertades de expresión e información en internet y el derecho a la protección de datos. El derecho al olvido y sus retos: “un falso derecho, a juzgar por un falso tribunal”*; en BEL, I. y CORREDOIRA L. (coord.) (2015). *Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia*. Centro de Estudios Políticos y Constitucionales. Madrid, págs. 430-431.

tratamiento y publicación de unos datos personales sin el consentimiento de su titular. De hecho, la veracidad es presupuesto para que se produzca el daño al derecho fundamental a la protección de datos personales, siendo, únicamente determinante para la legitimidad de la publicación, la relevancia pública de los datos que se han divulgado”²⁶⁸.

De ahí que sea preciso fijar las garantías del individuo respecto de los contenidos en internet. Para ello, “cabe impulsar la existencia de medios ágiles y efectivos para los usuarios de contenidos, imponer protocolos de actuación así como aclarar las subsidiarias vías administrativas o judiciales respecto del control de contenidos en internet”²⁶⁹.

Para buscar un equilibrio entre el derecho al olvido y la libertad de información, el TC ha reconocido en su sentencia 240/1992, de 21 de diciembre “la prioridad de la información cuando sea veraz y de interés público frente a los derechos de la personalidad”. Eso sí, habría que entrar a valorar cada caso concreto para poder discernir con total claridad si la información que se publica tiene interés público, dando por supuesto su veracidad, ya que si no estaríamos hablando además de un delito de injurias y calumnias. Por lo tanto, cada caso necesita un estudio suficiente para valorar la información y saber si la difusión de hechos pasados, irrelevantes a primera vista, puede causar a la persona implicada inconvenientes en su vida.

El derecho a la intimidad, como límite a la libertad de información, “debe ser interpretado restrictivamente”, como establece la STC 197/1991 (*Sara Montiel I*), de 17 de octubre, lo que supone que “los personajes públicos, por el hecho de serlo, y aún menos sus familiares, hayan de ver sacrificado ilimitadamente su derecho a la intimidad. El que la información publicada se refiera a un personaje público no implica de por sí

²⁶⁸ SIMÓN CASTELLANO, P. (2011). *El Régimen Constitucional del derecho... ob. cit.*, págs. 213-214.

²⁶⁹ COTINO HUESO, L. (2014). *La STJUE del caso Google vs AGPD de 2014. Algunos “olvidos” y otras tendencias negativas respecto de las libertades informativas en Internet*. Ponencia en el seminario de la Facultad de Derecho de Valencia: Google, el derecho al olvido y la responsabilidad de prestadores e intermediarios. Valencia, pág. 23. Véase también MINERO ALEJANDRE, G. (2017). Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea. *Anuario jurídico y económico escurialense* nº50, págs. 13-58.

que los hechos contenidos en la misma no puedan estar protegidos por el derecho a la intimidad de esa persona, que constituye siempre un límite del derecho a la intimidad. Las personas que, por razón de su actividad profesional, como aquí sucede, son conocidas por la mayoría de la sociedad, han de sufrir mayores intromisiones en su vida privada que los simples particulares, pero ello no puede ser entendido tan radicalmente, como se sostiene en la demanda, en el sentido de que el personaje público acepte libremente el riesgo de lesión de la intimidad que implica la condición de figura pública”. Además, “no toda información, que se refiere a una persona con notoriedad pública, goza de esa especial protección, sino que para ello es exigible, junto a ese elemento subjetivo del carácter público de la persona afectada, el elemento objetivo de que los hechos constitutivos de la información, por su relevancia pública, no afecten a la intimidad, por restringida que ésta sea. El problema en cada caso es el de identificar los límites que debe soportar el derecho a la intimidad cuando exista un interés público al conocimiento de determinados hechos que pueda legitimar la invasión de la esfera privada del personaje público” (FJ4).

Relacionado con la relevancia pública de la información, el TC ha subrayado en su sentencia 12/2012²⁷⁰, de 30 de enero que “dado que la protección constitucional se ciñe a la transmisión de hechos noticiables por su importancia o relevancia social para contribuir a la formación de la opinión pública, tales hechos deben versar sobre aspectos conectados a la proyección pública de la persona a la que se refiere, o a las características del hecho en que esa persona se haya visto involucrada. De manera que, «sólo tras haber constatado la concurrencia de estas circunstancias resulta posible afirmar que la información de que se trate está especialmente protegida por ser susceptible de encuadrarse dentro del espacio que a una prensa libre debe ser asegurado en un sistema democrático» (STC 29/2009, de 26 de enero, FJ4)” (FJ4).

El TC concluyó que en “la intromisión en los derechos fundamentales de terceros resultante del ejercicio de la libertad de información sólo será legítima en la medida en

²⁷⁰ Una periodista contratada por la productora Canal Mundo Producciones Audiovisuales, acudió a la consulta de una esteticista y naturista, haciéndose pasar por una paciente, por lo que fue atendida por ésta en la parte de su vivienda destinada a consulta, ocasión utilizada por la primera para grabar la voz y la imagen de la segunda por medio de una cámara oculta. La grabación se emitió en el programa PVP del Canal 9 de la Televisión Autonómica Valenciana.

que la afectación de dichos derechos resulte adecuada, necesaria y proporcionada para la realización constitucional del derecho a la libertad de información” (FJ6). En cuanto al interés general del reportaje estableció que “resulta procedente señalar que, aun cuando la información hubiera sido de relevancia pública, los términos en que se obtuvo y registró, mediante el uso de una cámara oculta, constituyen en todo caso una ilegítima intromisión en los derechos fundamentales a la intimidad personal y a la propia imagen. En cuanto a la vulneración de la intimidad, hay que rechazar en primer lugar que tanto el carácter accesible al público de la parte de la vivienda dedicada a consulta por la esteticista/naturista, como la aparente relación profesional entablada entre dicha persona y la periodista que se hizo pasar por una paciente, tengan la capacidad de situar la actuación de la recurrente extramuros del ámbito del derecho a la intimidad de aquélla, constitucionalmente protegido también en relaciones de naturaleza profesional. La Sentencia del Tribunal Supremo impugnada señala correctamente que la relación entre la periodista y la esteticista/naturista se desarrolló en un ámbito indudablemente privado. No existiendo consentimiento expreso, válido y eficaz prestado por la titular del derecho afectado, es forzoso concluir que hubo una intromisión ilegítima en el derecho fundamental a la intimidad personal” (FJ7).

Al respecto, Gómez de Liaño señaló que el TC "ha dejado herido de muerte el formato de la cámara oculta. La sentencia supone un adiós definitivo a la captación intrusiva con fines periodísticos. El Alto Tribunal ha zanjado un conflicto que, en cierto modo, había ya frenado el TS. La razón de la importancia de la STC 12/2012 estriba en que es la primera vez en que el máximo intérprete de la Carta Magna se ha pronunciado sobre todo el conjunto de las singularidades que rodean a la grabación videográfica íntegra. Hasta hace unos años, en España las filmaciones clandestinas, muy populares en otros países como Reino Unido y Estados Unidos, apenas tenían acogida en el ámbito periodístico. Pero, poco a poco, fueron ocupando un espacio propio y la feroz e implacable lucha por las audiencias en televisión ha llevado a un uso abusivo y desmedido de las cámaras ocultas respecto de las cuales se predicaban propiedades benéficas para formar una opinión libre en una sociedad democrática”²⁷¹.

²⁷¹ GÓMEZ DE LIAÑO FONSECA-HERRERO, M. (2012). La prohibición constitucional del uso de cámaras ocultas en el marco del denominado periodismo de investigación. *Revista Derecom* nº13, pág. 2.

Para Villaverde lo que se enjuicia en la sentencia “no es la información divulgada (el intrusismo profesional y las prácticas fraudulentas de ciertas profesiones o en la prestación de ciertos servicios), que goza de relevancia pública y es veraz. Lo que se enjuicia es el modo en que se obtuvo esa información y que la forma en la que fue obtenida haya sido divulgada”. Por lo que considera que lo que debió analizar el TC es “si la difusión de las imágenes y sonidos captados con la cámara oculta para apoyar en ellos la información relativa a esas prácticas merecía o no el amparo constitucional. Si esa información se hubiera divulgado sin hacer uso de esas imágenes y sonidos, el juicio del TC debiera haber sido favorable a otorgar el amparo del artículo 20.1 d) CE a los periodistas. Su manto protector se hubiera extendido en consecuencia al medio para obtenerla. Si, por el contrario, y como así fue, se hace uso de ellas, el TC debió examinar, no la información, sino si era necesario emplear esas imágenes y sonidos para su divulgación. Y es aquí donde se comparte el juicio negativo del TC: la divulgación de esas imágenes y sonidos era innecesaria y por ello pierde el amparo que sí tiene la información que se divulgaba”. Por esa razón, a los medios “les hubiera bastado con divulgar esa información y reservarse las imágenes y sonidos para la prueba de la veracidad de los hechos narrados, preservando lo así obtenido en el secreto periodístico. Pero las cosas sucedieron de otra forma”²⁷².

5.5.1.1. ¿La “tasa Google” vulnera la libertad de información?

La entrada en vigor el 1 de enero de 2015 de la Ley de Propiedad Intelectual, más conocida como Ley Lassalle, obliga a los editores y autores a percibir una compensación económica cuando los agregadores de Internet (Google News) enlacen y distribuyan sus contenidos²⁷³. Esta tasa supone un nuevo límite a los derechos de

²⁷² VILLAVERDE MENÉNDEZ, I. (2012). A propósito de la reciente jurisprudencia del Tribunal Constitucional sobre el empleo de “cámaras ocultas”. *Revista Derecom* nº13, pág. 26.

²⁷³ Artículo 32.2 de la LPI: “La puesta a disposición del público por parte de prestadores de servicios electrónicos de agregación de contenidos de fragmentos no significativos de contenidos, divulgados en publicaciones periódicas o en sitios Web de actualización periódica y que tengan una finalidad informativa, de creación de opinión pública o de entretenimiento, no requerirá autorización, sin perjuicio del derecho del editor o, en su caso, de otros titulares de derechos a percibir una compensación equitativa. Este derecho será irrenunciable y se hará efectivo a través de las entidades de gestión de los derechos de propiedad intelectual. En cualquier caso, la puesta a disposición del público por terceros de cualquier imagen, obra fotográfica o mera fotografía divulgada en publicaciones periódicas o en sitios Web de actualización periódica estará sujeta a autorización. Sin perjuicio de lo establecido en el párrafo anterior,

propiedad intelectual, de forma que, sin necesidad de autorización de los editores, los agregadores de noticias pueden citar fragmentos de éstas, pero estarán obligados a pagar una compensación obligatoria. Su aplicación ha llevado al servicio de noticias Google News en España a cerrar, ya que, según explicaba Richard Gingras, responsable de Google News, “la situación no es sostenible porque el servicio no obtiene beneficios”. Por lo tanto, los usuarios españoles que, desde el 16 de diciembre de 2014, tecleen news.google.es serán redirigidos al centro de ayuda de Google donde se les informará del cierre y sus motivos²⁷⁴.

El conflicto puede surgir al considerar que la supresión de Google News coarta la libertad de información y el acceso a ello de los usuarios. El Ministerio de Educación, Cultura y Deporte emitió un comunicado en el que aseguraba que “a pesar de la

la puesta a disposición del público por parte de prestadores de servicios que faciliten instrumentos de búsqueda de palabras aisladas incluidas en los contenidos referidos en el párrafo anterior no estará sujeta a autorización ni compensación equitativa siempre que tal puesta a disposición del público se produzca sin finalidad comercial propia y se realice estrictamente circunscrita a lo imprescindible para ofrecer resultados de búsqueda en respuesta a consultas previamente formuladas por un usuario al buscador y siempre que la puesta a disposición del público incluya un enlace a la página de origen de los contenidos”.

²⁷⁴ Texto que se encuentran los usuarios cuando intentan acceder a Google News España: “Lamentamos tener que informarte que Google Noticias ha cerrado en España y que las publicaciones de los editores españoles ya no aparecen en Google Noticias, a raíz de los recientes cambios en la legislación española. Comprendemos que usuarios como tú podáis estar descontentos con esta nueva situación y por ello queremos explicarte las razones por las cuales hemos tomado esta decisión. Google Noticias es un servicio gratuito, que utilizan y aprecian millones de usuarios de todo el mundo y que en la actualidad se encuentra disponible en más de 70 ediciones internacionales y en 35 idiomas. Incluye desde los periódicos nacionales, hasta las pequeñas publicaciones locales, medios especializados y blogs. Los editores pueden elegir si quieren que sus artículos aparezcan en Google Noticias o no y, por razones de peso, la inmensa mayoría opta por su inclusión. Google Noticias crea un verdadero valor para estas publicaciones al dirigir tráfico de usuarios a sus sitios web, lo que a su vez les ayuda a generar ingresos publicitarios. Tras la aprobación de la reforma de la Ley de Propiedad Intelectual hemos tenido que cerrar el servicio de Google Noticias en España. Esta nueva legislación obliga a cualquier publicación española a cobrar, quiera o no, a servicios como Google Noticias por mostrar el más mínimo fragmento de sus publicaciones. Dado que Google Noticias es un servicio que no genera ingresos (no mostramos publicidad en el sitio web), este nuevo enfoque resulta sencillamente insostenible. Desde Google vamos a seguir manteniendo nuestro compromiso de ayudar y trabajar con el sector de la información, al igual que con nuestros miles de socios en todo el mundo, incluidos los de España, para ayudarles a incrementar sus lectores e ingresos en Internet”.

suspensión del servicio de Google News, el acceso a la información en Internet continúa garantizado, ya se puede acceder a ésta bien directamente en las webs de los medios de comunicación o como resultado de la indexación de la noticia por motores de búsqueda y en los demás agregadores de contenidos informativos”. Además, quiso dejar claro que “los usuarios o las redes sociales están exentos de pago alguno por hacer uso de estos servicios de contenidos informativos o por acceder a ellos a través de enlaces”. Por lo tanto, “la Ley de Propiedad Intelectual en nada obstaculiza la libertad de información, siempre dentro del respeto y protección a los derechos de propiedad intelectual de los autores”²⁷⁵.

5.5.2. La libertad de expresión vs. Derecho al olvido

Partimos de la base de que la libertad de expresión viene recogida en la CE y se configura como un derecho fundamental en nuestro ordenamiento jurídico. Además, el CEDH le da también una especial relevancia en su artículo 10. El Tribunal de Estrasburgo dictó recientemente dos sentencias (caso *Gutiérrez Suárez c. España*²⁷⁶, de 1 de junio de 2010, y caso *Otegui Mondragón c. España*²⁷⁷, de 15 de marzo de 2011) en

²⁷⁵ Comunicado del Ministerio de Educación, Cultura y Deporte, de 11 de diciembre de 2014.

²⁷⁶ “El 18 de diciembre de 1995, el periódico de tirada nacional *Diario 16*, del que el demandante era director en el momento de los hechos, publicó, en primera página, una información relativa a la introducción en Algeciras de 4.638 kilogramos de hachís, ocultados en el doble fondo de un camión de la sociedad *Domaines Royaux* que pertenece a la familia real Alaouí, dedicado a la exportación de cítricos y frutas tropicales. El camión salido de Tánger tenía por destino el mercado central de Madrid. El artículo aparecía en primera página bajo el título: «Una sociedad familiar de Hassan II implicada en tráfico de estupefacientes». En la página 12 se publicaba un artículo más desarrollado bajo el título: «Cinco toneladas de hachís descubiertas en una carga de la empresa Hassan II». En el texto del artículo se mencionaban los artículos publicados en *El Mundo*, *Le Monde* y *Herald Tribune* que hacían referencia al tráfico de estupefacientes como principal fuente de divisas de Marruecos e implicaba a algunas personalidades políticas marroquíes próximas al monarca” (Punto 6).

²⁷⁷ “El 21 de febrero de 2003, por resolución del Juez Central de Instrucción nº 6 del Audiencia Nacional, se acordó la entrada y registro de los locales del diario *Euskaldunon Egunkaria*, en razón de los presuntos vínculos del Diario con ETA. Fueron detenidas diez personas, que eran los principales responsables del Diario (miembros del consejo de administración y Redactor Jefe). Después de cinco días de detención incomunicada, los interesados se quejaron de haber sufrido malos tratos durante la detención preventiva. El 26 de febrero, el Presidente de la Comunidad Autónoma recibió al Rey de España para participar en la inauguración de una central eléctrica en la provincia de Vizcaya. Durante una rueda de prensa celebrada el mismo día en San Sebastián, el demandante, como portavoz del grupo parlamentario Sozialista

las que condenó a España por vulnerar el derecho a la libertad de expresión, en las que, a pesar de reconocer que la libertad de expresión no es un derecho absoluto, ha establecido claramente las condiciones que deben cumplir los Estados para que sean compatibles con el Convenio anteriormente citado, exigiendo, como recoge Isabel Serrano, “que la medida restrictiva esté prevista por la ley; que la limitación esté justificada por alguno de los fines establecidos en el apartado 2 del artículo 10 del Convenio; y que la medida sea necesaria dentro de una sociedad democrática”. Esta última condición, “hace referencia a dos aspectos esenciales: la necesidad de la injerencia en una sociedad democrática y la proporcionalidad entre la medida y el objetivo que se persigue conseguir”²⁷⁸.

“La libertad de expresión y el riesgo de que el derecho al olvido pudiera convertirse en una modalidad de censura”, como reconoce Artemi Rallo, obliga a “la necesidad de conciliar dicho conflicto”. Las dudas generadas obligaron a “negar el carácter absoluto del derecho al olvido frente al resto de derechos y, en particular, ante las libertades de expresión e información, proclamando, además, que el derecho al olvido tampoco podría implicar un derecho al borrado de la historia”²⁷⁹.

5.5.2.1. Una nueva libertad de expresión a través de la red

La libertad de expresión ha cambiado con la llegada de Internet, ya que la red facilita la comunicación y permite “gozar de tribunas de expresión y de visibilidad a casi

Abertzaleak, expuso la evaluación política hecha por su grupo de la situación del Diario Egunkaria. En respuesta a una cuestión planteada por un periodista, afirmó, refiriéndose a la visita del rey al País Vasco, que «era patético» y que era una «verdadera vergüenza política». Añadió que inaugurar un proyecto con el Rey de los españoles, que era el jefe supremo último de la Guardia civil y el jefe supremo de las Fuerzas armadas españolas, era absolutamente lamentable. Con respecto a lo acontecido durante la operación policial contra el Diario *Egunkaria*, añadió que el Rey era el jefe de los que habían torturado a las personas detenidas en el marco de dicha operación. Se expresó en estos términos: «¿Cómo es posible que se fotografien hoy en día en Bilbao con el Rey español, cuando el Rey español es el jefe máximo del Ejército español, es decir, el responsable de los torturadores y que ampara la tortura y que impone su régimen monárquico a nuestro pueblo mediante la tortura y la violencia?» (Puntos 8-10).

²⁷⁸ SERRANO MAÍLLO, I. (2011). El Derecho a la libertad de expresión en la jurisprudencia del Tribunal Europeo de Derechos Humanos: Dos casos españoles. *Teoría y Realidad Constitucional* nº28. UNED, págs. 582-583.

²⁷⁹ RALLO LOMBARTE, A. (2015). *El debate europeo sobre el derecho al olvido en internet*. Capítulo extraído de *Hacia un nuevo derecho de protección de datos*. Tirant lo Blanch. Valencia, págs. 729-730.

cualquier ciudadano, es un agente dinamizador del pluralismo de primer orden. Su potencial le permite albergar manifestaciones expresivas que exceden de los límites de lo aceptado por nuestro ordenamiento”. Por lo tanto, lo interesante es saber si las limitaciones que han de ponerse a la libertad de expresión en Internet han de ser más restrictivas. En ese sentido, “la liberalización que suponía Internet respecto del acceso a una tribuna pública generalizó el temor a que fuera empleada para propagar contenidos violentos, indecentes o delictivos y pareció aconsejar la adopción de medidas preventivas e incrementar el rigor con el que se valoraría posibles excesos expresivos, por encima de los umbrales que marcarían la legitimidad del discurso en otro foro o canal”. Pero, jurídicamente, “esa reacción no está justificada y olvida el hecho de que la libertad de expresión sirve precisamente a la emisión de opiniones que, en muchos casos, pueden ser tenidos por hirientes u ofensivas”²⁸⁰.

En este sentido, es cada vez más intensa la línea doctrinal, en la que se encuentra Teruel, que viene afirmando “la necesidad de reinterpretar las libertades de expresión y de información en la forma estrictamente reconocida por la letra de nuestra Constitución, para afirmar un *ius communicationis*, un derecho a la comunicación en el que se dé tutela a todo el proceso comunicativo entendido en toda su extensión, reconociendo la libertad de expresarse en su vertiente activa, pero también la dimensión pasiva y los derechos a recibir y acceder a la información, entendida ésta a su vez en su sentido más amplio (informaciones, opiniones, valoraciones...)”. Un derecho que, como añade, encontraría su anclaje en “los textos internacionales de derechos humanos, particularmente en la Declaración Universal de los Derechos Humanos, que en su art. 19 reconoce, más que la libertad de expresión entendida estrictamente, este derecho de comunicación”²⁸¹.

El TS ratificó en su sentencia 3164/2008, de 26 de junio. Sala de lo Contencioso-administrativo (número de recurso: 6818/2003), las sanciones impuestas por la AEPD a la Asociación contra la Tortura por ofrecer en su página web un listado que contenía

²⁸⁰ GUICHOT REINA, E. (coord.) (2015). *Derecho de la comunicación... ob. cit.*, págs. 215-216.

²⁸¹ TERUEL LOZANO, G. (2010). *La libertad de expresión en Internet y sus garantías constitucionales en el control de contenidos de páginas web*. *Magister Iuris Constitutionalis*, pág. 121.

datos sobre funcionarios públicos en actuaciones relativas a torturas²⁸². La Sala ante la afirmación de los infractores de que los datos expuestos tienen carácter público afirma que "la probada publicación vía internet de lo que sin duda y como hemos dicho constituye un fichero con los nombres y apellidos de funcionarios públicos denunciados por la comisión de delitos de maltrato o tortura no es una manifestación de los derechos a la libre expresión, y a la información que no puede atribuirse sin más la actora, con la mera remisión a sus fines sociales, sino una clara vulneración del derecho fundamental consagrado en el apartado 4 del art.18 de la Constitución, al que tan extensamente nos hemos referido, infringiendo el art.11 de la Ley 15/99, cuyo artículo 3, en su apartado i) define la cesión o comunicación de datos como toda revelación de datos realizada a una persona distinta del interesado" (FJ9).

Las formas de expresión y comunicación con la llegada de Internet han cambiado y así lo refleja la AEPD en su Resolución 00211/2010²⁸³, de 26 de febrero, que, como reconoce Cotino, fue "desafortunada" al recoger que "un ciudadano no puede atreverse a alegar libertad de expresión, pretendiendo reservarla sólo para los medios de

²⁸² La AEPD recibió denuncia de la Dirección General de la Policía informando que vía internet y a nombre de la Asociación contra la Tortura se ofrecía un listado de datos sobre policías, guardias civiles y políticos implicados en actuaciones relativas a torturas. Adjuntándose listado en el que consta el nombre del funcionario, su situación en relación con la denuncia por tortura (investigación, condenado, absuelto), el lugar de los hechos, la fecha y la identificación del caso. La Agencia adoptó la medida cautelar de cesar de forma inmediata el tratamiento de los datos y su difusión vía Internet. Decisión que fue confirmada por la Sección Primera de la Sala de lo Contencioso-administrativo de la Audiencia Nacional en su sentencia 62/2001, de 12 de enero. Asimismo acordó iniciar procedimiento sancionador. La AEPD basa sus motivos en el art.7.5 de la LO 15/1999, en el que se afirma que "los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones Públicas competentes en los supuestos previstos en las respectivas normas reguladoras". Por lo tanto no está prohibido en nuestro sistema tratar datos de carácter personal relativos a la comisión de infracciones penales o administrativas por entidades distintas de la Administración Pública competente, con independencia del origen público o privado del dato.

²⁸³ Las páginas web del imputado no pueden ser consideradas medios de comunicación social sin que quepa invocar el ejercicio y prevalencia del derecho de libertad de información que derivaría en una prevalencia general que aboliría de facto la protección de datos personales. Y que desvirtuaría el equilibrio entre derechos sostenido sobre el derecho de la sociedad a ser informada a través de los medios de comunicación y el de los ciudadanos a la autodeterminación informativa y privacidad sostenido sobre el derecho de protección de datos.

comunicación clásicos”. Una circunstancia en la que Cotino está de acuerdo, ya que “reservar de manera excluyente la protección más intensa de las libertades a los medios de comunicación clásicos es un punto de partida que amordaza la libertad de expresión e información en la red bajo la espada de Damocles de severísimas sanciones administrativas o penales”²⁸⁴. La corriente que concentra la protección de la libertad de expresión en internet a favor de los medios clásicos, es la que lleva a que “sea muy difícil sino imposible localizar al autor real de una información ilícita en la red y a que sólo un profesional de la información cuente con el derecho a no revelar las fuentes”. Además, subyace “la realidad de la escasa fiabilidad de la información no profesional que inunda internet, así como la frivolidad, banalidad e irresponsabilidad tan habitual de los millones de usuarios de blogs y redes sociales cuando difunden o información”²⁸⁵.

Esta resolución fue, posteriormente, anulada por lesionar la libertad de expresión por la sentencia AN 170/2012, de 11 de abril. Sala de lo Contencioso-administrativo (nº de recurso: 410/2010), en la que establece que “la resolución se limita a afirmar que las páginas web del imputado no pueden ser consideradas un medio de comunicación social por lo que no cabe invocar la prevalencia del derecho de libertad de información. Esta concepción ha sido superada por la jurisprudencia, pues ni resulta un requisito excluyente del tratamiento el que el dato no se haya obtenido de una fuente accesible al público, ni en la ponderación de los derechos fundamentales en conflicto es posible sostener que los derechos de libertad de expresión e información están reservados para los medios de comunicación social (prensa radio y televisión) y la página web del imputado no lo sea. Ambas afirmaciones, al margen de que carecen de la necesaria justificación, no pueden ser compartidas por este Tribunal. Tanto el derecho a la libertad de expresión como el derecho a comunicar y difundir información son derechos individuales cuya titularidad no queda restringida a los profesionales de los medios de comunicación, sino que, por el contrario, la ostentan todas las personas físicas (así lo recogió el TC en su sentencia 165/1987, de 27 de octubre, en la que «la libertad de información es, en términos constitucionales, un medio de formación de opinión pública en asuntos de interés general, cuyo valor de libertad preferente sobre otros derechos fundamentales y entre ellos el derecho al honor, puesto de manifiesto por la STC

²⁸⁴ COTINO HUESO, L. (2015). *El conflicto entre las libertades de expresión... ob. cit.*, pág. 398.

²⁸⁵ COTINO HUESO, L. (2014). *La STJUE del caso Google vs AGPD... ob. cit.*, págs. 13-14.

104/1986, de 17 de julio, viene determinado por su condición de garantía de la opinión pública, que es una institución constitucional al Estado democrático que los poderes públicos tienen especial obligación de proteger. Este valor preferente alcanza su máximo nivel cuando la libertad es ejercitada por los profesionales de la información a través del vehículo institucionalizado de formación de la opinión pública, que es la prensa, entendida en su más amplia acepción. Esto, sin embargo, no significa que la misma libertad no deba ser reconocida en iguales términos a quienes no ostentan igual cualidad profesional, pues los derechos de la personalidad pertenecen a todos sin estar subordinados a las características personales del que los ejerce, sino al contenido del propio ejercicio... »). Y con mayor motivo aun es inadmisibile sostener que el derecho de libertad de expresión está reservado a los periodistas. De modo que ni es posible descartar que un particular puede ejercer legítimamente sus derechos constitucionales de la libertad de expresión y a comunicar información, ni puede circunscribirse el ejercicio de estos derechos a los medios convencionales de comunicación (prensa, radio, televisión), excluyendo otras formas de comunicación que existen en la actualidad, tales como las páginas web o noticias online. Debe recordarse, en tal sentido, que la Constitución reconoce el derecho a expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción y el derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión. Todo ello, sin perjuicio de que la protección que dispensan estos derechos en su confrontación con otros deba entenderse reforzada cuando su ejercicio se produce por los profesionales de la información o por los medios de comunicación convencionales, pero sin olvidar que la comunicación, hoy en día, no se circunscribe a los medios de comunicación tradicionales sino a otros medios muy diversos, propiciados por la actual tecnología, en los que internet ocupa un papel muy relevante para obtener y difundir información veraz y para expresar libremente las propias opiniones e ideas” (FJ9).

La justicia española ya se ha pronunciado al respecto de la difusión de opiniones en Twitter. El juzgado de 1ª Instancia número 5 de Pamplona en su sentencia 213/2012, de 15 de octubre, condenó a Ana Pineda, concejala de UPN en el Ayuntamiento de Pamplona, por intromisión ilegítima en el honor de la diputada y edil de Nafarroa Bai, Uxue Barkos, por unos comentarios publicados en Twitter. El juez considera en la sentencia que Pineda transmitió la idea que Barkos estaba “haciendo uso de su enfermedad con fines políticos y partidistas”, lo que constituye una vulneración al honor

de la política de Nafarroa Bai. El magistrado dictamina que, en este caso, no prevalece el derecho a la libertad de expresión sobre el derecho al honor, condenando a Pineda a: “proceder a la supresión de los mensajes de su cuenta de Twitter; abstenerse en el futuro de llevar a cabo nuevos actos de intromisión en cualquier ámbito, medio o plataforma de comunicación que vulneren el derecho al honor de Uxue Barkos; y hacer público el siguiente mensaje a través de su cuenta de Twitter, manteniéndolo en la web durante al menos dos meses. El texto del mensaje era el siguiente: "Publico este tuit en cumplimiento de la sentencia de 11.10.12 del juzgado de 1ª instancia 5 de Pamplona, que declara que los tuits que remití el 18.03.11 vulneran el honor de Doña Uxue Barkos (si el texto no cabe en un solo tweet, se enviará en varios hasta completarlo, uno a continuación del otro)”²⁸⁶. En cambio, el fallo libera de responsabilidad al ex director del Área de Hacienda del Ayuntamiento de Pamplona, Iñigo Huarte, quien retuiteó los comentarios difamatorios publicados por la edil. Por lo tanto, según la justicia española, retuitear mensajes no conlleva el mismo grado de implicación que publicar opiniones en Twitter. Lo novedoso de la sentencia es que, de una u otra forma, considera a Twitter como un medio de comunicación.

Actualmente, la interacción entre el marco europeo de protección de datos y la libertad de expresión es confusa e insatisfactoria. El nuevo reglamento Europeo de Protección de Datos recoge en su artículo 80 el tratamiento de datos personales y la libertad de

²⁸⁶ El día 18 de marzo de 2011, el Ayuntamiento de Pamplona celebraba un Pleno en el que, entre otras cuestiones, se debatía una moción del grupo municipal de UPN sobre explotación sexual, que perseguía que el Ayuntamiento no contratara inserciones publicitarias en los medios que incluyen anuncios de servicios de prostitución Uxue Barkos, que había sido intervenida quirúrgicamente para la extirpación del cáncer de mama quince días antes, debía acudir a la misma hora de inicio del pleno a una revisión médica, tras la cual iba a acudir (por primera vez tras el anuncio de su enfermedad y la intervención quirúrgica a la que se había sometido) al Pleno del Ayuntamiento. Cuando Barkos llegó a la sede del Consistorio, el pleno estaba debatiendo la moción del grupo UPN sobre explotación sexual. Los periodistas (al parecer todos menos uno) que cubrían la sesión abandonaron la Sala de Plenos y se dirigieron a la entrada del Edificio donde entrevistaron a la concejala de Nafarroa Bai. En ese momento, Pineda envió en abierto desde su BlackBerry, a través de su cuenta de Twitter el siguiente mensaje: “Barkos hace su desembarco mediático xa distraer a los medios de la propuesta de UPN contra la explotación sexual de mujeres en medios”, publicando posteriormente otros tres tuits, en los que se transmite la idea de que Barkos está haciendo uso de su enfermedad con fines políticos y partidistas, para sacar a los medios del pleno cuando se está debatiendo una moción del adversario político y que afecta a un grupo de información afín a su ideología.

expresión²⁸⁷ y aportará más claridad al asunto. El potencial concepto restrictivo de, como apunta Erdos, “propósitos periodísticos del artículo 80 debe, por lo tanto, sustituirse por el propósito de producir y difundir información, opinión e ideas para beneficio del público, concebido como un colectivo que debería gozar del beneficio de sus profundos fines específicos” Mientras que las actividades llevadas a cabo por los individuos en páginas webs o redes sociales “no constituyen por sí mismas casos expresos pensados únicamente para el público, en su conjunto, ya que son de gran importancia para facilitar y mantener la libertad de expresión a través de la promoción de la expresión individual”. Sin embargo, para Erdos, el artículo 80 “debe ampliarse para permitir también las derogaciones oportunas para los datos específicos y los regímenes de exportación de datos”²⁸⁸. Eso sí, el nuevo reglamento europeo permite a los Estados miembros garantizar derogaciones más amplias en el campo de la libertad de expresión “para proteger los derechos y libertades del interesado o de otras personas”²⁸⁹.

Internet es, como apunta Teruel, “un espacio extraordinario para el desarrollo de las libertades públicas, pero, entre todas ellas, qué duda cabe que la libertad de expresión es

²⁸⁷ Artículo 80: “1. Los Estados miembros dispondrán exenciones o excepciones a las disposiciones relativas a los principios generales del Capítulo II, los derechos del interesado del Capítulo III, el responsable y el encargado del Capítulo IV, la transferencia de datos personales a terceros países y a organizaciones internacionales del Capítulo V, las autoridades de control independientes del Capítulo VI y la cooperación y la coherencia del Capítulo VII en lo referente al tratamiento de los datos personales efectuado exclusivamente con fines periodísticos o de expresión literaria o artística, para conciliar el derecho a la protección de los datos de carácter personal con las normas que rigen la libertad de expresión. 2. Cada Estado miembro notificará a la Comisión las disposiciones legislativas que adopte de conformidad con el apartado 1, a más tardar en la fecha especificada en el artículo 91, apartado 2, y, sin demora, cualquier modificación posterior de las mismas”.

²⁸⁸ ERDOS, D. (2012). *Confused? Analysing the Scope of Freedom of Speech Protection vis-à-vis European Data Protection*. Universidad de Oxford, págs. 33-35.

²⁸⁹ Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Artículo 21.1.f): “El Derecho de la Unión o de un Estado miembro podrá limitar, por medio de medidas legislativas, el alcance de las obligaciones y de los derechos previstos en el artículo 5, letras a) a e), en los artículos 11 a 20 y en el artículo 32, cuando tal limitación constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar la protección del interesado o de los derechos y libertades de otras personas”.

la reina de Internet, ya que ofrece un espacio sin fronteras ni límites, sin controles para la expresión y para la comunicación, para la información, para la interacción entre ciudadanos del mundo. La pregunta sería entonces cuál es el modelo que debemos aplicar a Internet”. A esto, como indica el autor, le dio respuesta la Corte Suprema estadounidense (caso *ACLU v. J. Reno*²⁹⁰, 96-511, de 26 de junio de 1997), extrayendo “dos grandes principios que han de forjar las bases rectoras de toda regulación que de Internet se desarrolle. En primer lugar, en Internet no se verifican las circunstancias que justifican una mayor regulación, de lo que se deduce a *sensu contrario* que cualquier restricción específica aplicada en consideración únicamente del ejercicio de la libertad de expresión a través de este medio resultará inconstitucional. Y, en segundo término, es necesario proteger la autonomía del nuevo medio dado su importante carácter democratizador, de lo que se desprende entonces que el Estado tiene un especial deber de fomentar la realización de la libertad de expresión en este espacio más que de buscar medios para censurarlo”. La libertad de expresión la libertad ejercida a través de Internet “queda sometida únicamente a los límites generales de la misma, y, por tanto, de asociarse a algún modelo en concreto debiera vincularse con el régimen de la prensa escrita, que no cuenta con limitaciones específicas, aunque es cierto que Internet tiene unas características muy especiales, por lo que no le podrá ser de aplicación de manera directa el modelo propio de la prensa escrita. Así, deberá reputarse inconstitucional cualquier imposición de requisitos administrativos previos al acceso o a la creación de medios de información en Internet, pero también cualquier variación en los límites materiales civiles o penales que con carácter general existen para la misma”²⁹¹.

²⁹⁰ El Tribunal Supremo norteamericano declaró la inconstitucionalidad de la ley federal *Congress Decency Act* que había sido promulgada el 8 de febrero de 1996. “Esta Ley declaraba ilegal el uso de ordenadores y de las líneas telefónicas para transmitir material indecente y preveía severas penas de privación de libertad y multas para los nuevos tipos penales. Es la primera vez que una Ley norteamericana regulaba específicamente la libertad de expresión en Internet. El ejercicio de la libertad de expresión en el nuevo medio se limitaba gravemente, imponiéndole un régimen más estricto que a su ejercicio en la radiodifusión. Las sentencias que son objeto de este artículo han establecido que la regulación que imponía la Ley atenta contra la Primera Enmienda al ser inconstitucional” en FERNÁNDEZ ESTEBAN, M. L. (1998). Limitaciones constitucionales e inconstitucionales a la libertad de expresión en Internet. *Revista Española de Derecho Constitucional* nº53, págs. 283-284.

²⁹¹ TERUEL LOZANO, G. (2010). Apuntes generales sobre la libertad de expresión en Internet. *Anales de Derecho*. Vol. 28, págs. 137-139.

Somos de la misma opinión que Teruel y no consideramos que la justicia tenga que crear procedimientos de control distintos para regular la libertad de expresión en Internet, con aplicar los mismo criterios que para la prensa escrita sería suficiente. Eso sí, tendrían que buscarse soluciones más rápidas que las establecidas por los Tribunales para atajarla. En lo que respecta al derecho al olvido, ateniéndonos a la STJUE la libertad de expresión no se vería afectada, ya que las medidas son tomadas por el motor de búsqueda y no por el editor de la página web.

5.5.2.2. Cuestiones de responsabilidad en el ejercicio de la libertad de expresión a través de Internet

El Juzgado de 1ª Instancia número 44 de Madrid en su sentencia 00184/2007²⁹², de 19 de septiembre, dictó una sentencia favorable a favor del demandante frente a la página web por vulnerar su derecho al honor. La sentencia considera que el “sitio web Alasbarricadas.org infringe la obligación establecida por el artículo 10 de la LSSICE 34/02, de 11 de julio, al no información alguna en su página web sobre del responsable o titular de la página o su domicilio para establecer una comunicación directa efectiva. Así al pinchar cualquier enlace de la página para contactar con los responsables solo se facilita el correo electrónico info@alabarricadas.org, siendo preciso al actor contratar una agencia de detectives para averiguar la identidad del titular del sitio web, que resultó el demandado y como tal proveedor de contenidos de la citada web, responsable solidario con los autores de los contenidos publicados. Una vez averiguada su identidad se le dirigió escrito por burofax, solicitando la retirada inmediata de los contenidos atentatorios al honor del actor e identificación de los autores materiales de los contenidos vejatorios especificados, tanto al domicilio obtenido por la investigación privada, como al aportado por el mismo demandado al registrar el dominio "alabarricadas.org", los cuales no pudieron entregarse al tratarse de un destinatario desconocido. Se insta así a través de la demanda además de la indemnización referida la

²⁹² En este caso, Ramoncín denunció a la citada web por unas expresiones publicadas contra su persona tales como “pedante, creído, tocapelotas/ovarios, farandulero, feo pasado por los quirófanos, mal artista, mal politiquillo, mal presentador de programas de tv, chupacámaras”. Además, uno de los comentarios vertidos por uno de los integrantes de la página web señalaba que: “solo siento no haber estado en el último festival que estuvo pa descalabrarle con un pedrolo del veinte”. Acompañando a la información aparecía una fotografía manipulada del actor, en la que aparece con la cabeza cortada.

inmediata retirada de los contenidos atentatorios al honor del actor, con publicación de la sentencia en medios de difusión, semejantes” (FJ1).

En este caso el juzgado establece que “tanto las expresiones vertidas en la web, como la fotografía adjunta, implican una clara y evidente lesión al honor del actor, excediendo de la mera crítica o puesta en conocimiento de los demás de una simple información, (así el primer mensaje establece claramente que solo abre el tema para expresar su odio visceral al personaje), constituyendo los mensajes y expresiones claros insultos, incluso amenazantes para su integridad física, dirigidos simplemente a la vejación y menosprecio del afectado y tenidos por tales en el concepto público, menoscabando los mismos su fama, buen nombre y prestigio profesional, con independencia de que el mismo haya tenido o mantenga posiciones controvertidas de cara al público, sujetas a crítica y opinión, por la misma posición pública asumida voluntariamente, sobre todo en las polémicas cuestiones referidas a la SGAE. Así resulta de la simple lectura de los mensajes y visionado de la fotografía e incluso la propia parte demandada no discute este extremo, habiendo alegado que ha retirado de forma inmediata los mensajes y expresiones en cuanto los ha conocido, evidenciando con sus propios actos que estima lesivo su contenido al honor de la persona, al margen de la alegación sobre que la propia postura y trayectoria polémica del actor, deba tenerse en cuenta a hora de fijar un quantum indemnizatorio y graduar el alcance de la lesión en términos económicos.

Debe así concluirse que en este caso, el derecho de crítica a la figura del actor en su actividad profesional, no ampara la fotografía, que lo representa con la cabeza cortada, ni los ofensivos insultos a la persona misma que se recogen, al manifestar los usuarios de la web sus opiniones”. (FJ4). La sentencia condenó al demandado a “eliminar de su sitio web las expresiones y la fotografía que atentaba contra el derecho al honor del actor, así como a publicar la sentencia en su página web y a abonar, en concepto de indemnización, 6.000 euros”.

Por su parte, la AP de Lugo, sección 1ª, en su sentencia 00538/2009²⁹³, de 9 de julio, absolvió de responsabilidad a los administradores de un foro por los comentarios que en

²⁹³ A principios del año 2007, y dentro de la página web referida, los demandados diseñaron el foro "mindoniense.com" facilitando así que los usuarios directamente insertaran sus comentarios en relación con los distintos temas de debate creados en su seno. Así, en el tema abierto «Coplas electorais de Mondoñedo», una usuaria publicó el siguiente comentario: «La verdad es que tienen toda la razón. Soy de

él se hacían. La sentencia viene a señalar, apoyándose en la LSSICE 34/2002, de 11 de julio, que “no se estima que los prestadores de servicios deban responder de dicha vulneración del Derecho al Honor emitido por los usuarios, habiéndose archivado las diligencias penales previas por falta de autor. Con independencia de la dificultad en el rastreo de la red para la identificación de los ordenadores y consecuentemente usuarios de los que remitieron los mensajes, no se estima que, en este caso concreto, los creadores del foro tuvieran un conocimiento efectivo de que la información fuera ilícita. Resulta obvia la dificultad de interpretación de tal expresión, los penalistas hablan de un dolo particularmente intenso, y los civilistas de un conocimiento constatable en todos sus extremos. Como anteriormente se reseñó e interpreta la Doctrina, el legislador delimita una serie de supuestos de hecho garantizando que, si se cumplen las condiciones previstas en las mismas, el prestador no podrá ser declarado responsable de los contenidos ilícitos de terceros que dicho prestador haya transmitido, alojado o enlazado. Dentro del alojamiento se contemplan no solo la actividad básica de los prestadores de alojamiento de sitios web, sino también los comentarios de terceros en un blog, el de artículos en un wiki, o el de mensajes en un foro, realizándose una función por los demandados subsumible en el supuesto contemplado en el art.16 de la LSSICE. Dicho precepto contiene una presunción, debiendo declararse probado dicho conocimiento efectivo a que se refiera el apartado a) (cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada) y el prestador conociera la

Mondoñedo pero vivo fuera, pq aquí es imposible encontrar trabajo, en los últimos años Mondoñedo ha bajado muchísimo, en vida, en gente, en actividad en general. Me cuentan que el alcalde y sus "amigos" hacen y deshacen a su antojo, hasta que Bagema (una empresa constructora) le hizo gratis la casa al alcaldillo a cambio de favores políticos en obras municipales y demás. La verdad es que no me extraña nada». En el mismo foro, otro usuario publicó: «Mais que constructor ESPECULADOR ou alguén pensa que ese mandante vaise poner a traballar poñendo ladrillos? Bagema fíxolle a casa gratis a cambio de favores (todo Mondoñedo o sabe). Recalificou os terreos e construíse onde él lle interesaba, e agora que deixa o pobo afogado e morto, logo de chupar do bote durante 8 anos (xa que como abogado non vale nin para firmar) vaise tan pancho a enriquecerse a costa de outros». La actividad de administración de la página web www.mindoniense.com permite definir a los demandados, con la finalidad de determinar el régimen de responsabilidad civil al que deban quedar sujetos, como prestadores de servicios de la sociedad de la información, sin que se les pueda imputar responsabilidad alguna por las expresiones vertidas por los usuarios, dado que ni se ha acreditado que hubieran tenido conocimiento efectivo de que estos comentarios fueran atentatorios al honor del Sr. Juan Luis ni que tras haberse puesto en contacto la Unidad Orgánica de la Policía Judicial con uno de los creadores de la web, no los hubieran retirado una vez tomaron conocimiento del alcance de aquellas afirmaciones.

correspondiente resolución. Pero ello no impide a juicio de esta Sala que el conocimiento de la ilicitud pueda probarse de alguna otra forma, pues no estamos ante ninguna numeración taxativa, sino una presunción *ad ex emplum*, y que a *sensu contrario* no impediría probar el conocimiento efectivo por cualquier otro medio. Pues bien, en el caso concreto sometido a la consideración de esta alzada no se estima que se tuviese tal conocimiento de ilicitud. Aun reconociendo que los creadores de un foro, deben moderarlo, como así ocurre en la práctica diaria, se comparte con la sentencia apelada que no puede darse por probado que los demandados tuvieran certeza efectiva, y no meras sospechas, de que los comentarios de los usuarios resultaron atentatorios contra el honor del demandante” (FJ2).

Es importante, por tanto, diferenciar, como apunta Miguel Ángel Mata²⁹⁴, la eventual responsabilidad de los distintos sujetos que se ven involucrados en la infracción o delito por los comentarios vertidos en la red:

- El autor del hecho delictivo: Será siempre el primer responsable de la infracción o delito, al tratarse del autor del comentario que ha provocado la denuncia.
- El proveedor del *hosting* o alojamiento web: se verá exento de responsabilidad, siempre que no tenga conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.
- El moderador de un foro o wiki: en el caso de que tuviese la capacidad de control de la información, por lo que no se descarta que pudiera ser responsable, según el caso concreto.

En relación con el derecho al olvido, el problema surge a la hora de saber cómo lograr que se olviden esos contenidos en los foros y blogs y quién tiene la responsabilidad de hacer que dichos contenidos se olviden. El TEDH en el caso *Delfi AS v. Estonia*²⁹⁵, de

²⁹⁴ Contenido extraído del artículo *Libertad de expresión en Internet* (2009). Disponible en: <http://www.miguelangelmata.com/page/3/>

²⁹⁵ Delfi es un portal de noticias muy popular en Estonia. En el momento de la demanda, la web publicaba unos 330 artículos diarios, en los que se permitía a los lectores escribir comentarios al final de cada artículo, para lo cual no se exigía identificación. El número de comentarios publicados diariamente era de unos diez mil. Se publicaban en la web de modo inmediato, sin una previa moderación, pero existía un

16 de junio de 2015, abordó, por primera vez, la responsabilidad de un portal web de noticias por los comentarios de sus usuarios, no habiendo adoptado las medidas necesarias y exigibles para retirar los comentarios injuriosos y violentos.

El Tribunal estableció que “es preciso señalar que Delfi no puede decirse que haya totalmente descuidado su deber de evitar causar daños a terceros. Sin embargo, y lo más importante, el filtro basado en palabras automáticas utilizado por la empresa solicitante para no publicar expresiones de odio o que inciten a la violencia por parte de los lectores, limita su capacidad para eliminar con rapidez los comentarios ofensivos. El Tribunal recuerda que la mayoría de las palabras y expresiones en este caso no contenían metáforas sofisticadas ni amenazas sutiles, eran expresiones manifiestas de odio y amenazas abiertas a la integridad física del director de la compañía. Por lo tanto, incluso si el filtro automático basado en palabras, puede haber sido útil en algunos casos, los hechos del presente caso demuestran que era insuficiente para la detección de los comentarios cuyo contenido no constituye la expresión protegida por el artículo 10 de la Convención. El TEDH observó que como consecuencia de este fracaso del mecanismo de filtrado, tales comentarios claramente ilegales permanecieron en línea durante seis semanas” (Puntos 155-156). En definitiva, la sentencia concluyó que “la decisión de los tribunales domésticos de declarar responsable al portal de noticias por los comentarios violentos y de odio redactados por sus usuarios se basa en motivos pertinentes y suficientes y es una restricción justificada y proporcionada del derecho a la libertad de expresión de dicho portal y que no ha habido por tanto una violación del artículo 10 del Convenio” (Punto 162).

filtro que eliminaba automáticamente los mensajes que contenían palabras inapropiadas. El portal había dispuesto además un sistema de notificación y retirada de mensajes ofensivos. Cualquier lector de la web podía marcar un mensaje como ofensivo y este era inmediatamente retirado. Asimismo, el ofendido por un mensaje difamatorio podía también dirigirse directamente a Delfi, quien de modo inmediato retiraba el comentario (Puntos 10-14). El 24 de enero de 2006 el portal publicó un artículo sobre la destrucción accidental de una carretera de hielo que une el continente con algunas islas en invierno. El accidente había sido causado por SLK, una empresa de ferris que cubre el mismo trayecto. Sin la carretera transitable, el modo de transporte habitual es el ferry, que resulta mucho más caro. Entre los días 24 y 25, el artículo recibió 185 comentarios, de los cuales unos veinte resultaban ofensivos contra el director de la compañía. El 9 de marzo de 2006, el agraviado pidió a Delfi que retirara los comentarios insultantes y que le abonara el equivalente a 32.000 euros por daños morales. El portal retiró los comentarios el mismo día, pero se negó al pago de la indemnización (Puntos 16-18).

Podemos concluir, por tanto, que, a partir de esta sentencia, las páginas web tendrán que controlar los comentarios vertidos por sus usuarios en sus páginas, ya que, éstos podrán insultar libremente y dar opiniones injuriosas, saliendo impunes de dichos comentarios debido a que la responsabilidad, como fijó el TEDH, recaería sobre la página web. Esto podría llegar a suponer un problema y obligar a las web a no permitir que sus usuarios hagan comentarios sobre sus artículos o noticias.

5.5.3. La intimidad vs. Derecho al olvido

Tradicionalmente, como señala Lucena, se ha formulado la intimidad “en términos de autonomía, secreto, libertad, desarrollo de la personalidad, sustrato inviolable de la dignidad personal...En la actualidad, se reivindica como derecho del control de la información personal, demandando la protección de la información personal frente al potencial invasivo de las nuevas tecnologías, su almacenamiento, procesamiento, difusión y utilización en el ámbito telemático”. Cabe resaltar que una regulación estatal “no tendría capacidad de garantizar la información de sus ciudadanos ya que no existen fronteras en el ciberespacio donde se almacena, analiza y difunde mucha de esta información”²⁹⁶.

El uso de los datos privados tiene que ser abordado en cada caso, ya que algunos usos “pueden ser prohibidos por completo o pueden requerir protecciones extraordinarias y, otros, tal vez la mayoría, requerirán una evaluación de riesgos específica del contexto y el empleo de las herramientas apropiadas. “El principio de uso reconoce que la elección individual puede ser una de esas herramientas. Además, cuando se requiera notificación y consentimiento deben proporcionarse verdaderas opciones al usuario, que irán acompañadas de la información pertinente, comprensible sobre la elección y sus consecuencias”. Por otro lado, el principio de la participación individual se limita a situaciones en las que se “están utilizando datos personales que de ninguna manera afectan a la educación, el empleo, la salud física o mental, la situación financiera, o los derechos protegidos por la ley de un individuo”. En estas situaciones, los individuos

²⁹⁶ LUCENA CID, I. V., (2014). *El concepto de la intimidad en los nuevos contextos tecnológicos*, págs. 31-33; en GALÁN MUÑOZ, A. (coord.) (2014). *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*. Tirant lo Blanch. Valencia.

tienen derecho a “conocer los datos personales que se están utilizando, pudiendo obtener fácilmente información sobre el uso previsto; acceder a ellos y tener la posibilidad de impugnar el procesamiento y la exactitud de dichos datos. Si el acceso o la corrección no se proporcionase o el procesamiento no se detuviese, habría que dar al usuario la oportunidad de recurrir judicialmente”. El administrador tiene la obligación de “corregir los datos inexactos o dar razones legítimas por su incapacidad para hacerlo, teniendo que estar definidas por una ley aplicable, pudiendo incluir factores tales como errores que no representan riesgo de perjuicio a los afectados, especialmente si esos errores son caros o excesivamente gravosos de corregir”²⁹⁷.

5.5.3.1. Los antecedentes penales, ¿forman parte de la intimidad y han de ser olvidados?

El TC se ha pronunciado al respecto en la sentencia 144/1999, de 22 de julio, en la que reconoce que “la información relativa a un aspecto tan sensible de la vida de un individuo, como son sus antecedentes penales, que indudablemente afectan a su integridad moral, debe estar a recaudo de una publicidad indebida y no consentida por el afectado, y, aun en el caso de que una norma de rango legal autorice a determinados sujetos el acceso a la misma, con o sin el consentimiento del afectado, ese acceso sólo está justificado si responde a alguna de las finalidades que explican la existencia del archivo o registro en el que estén contenidas; fines que deberán coincidir con alguna de las limitaciones constitucionalmente impuestas a la esfera íntima del individuo y su familia. Así pues, si el acceso no se realiza con estricta observancia de las normas que lo regulan, se vulnera el derecho a la intimidad. Y se vulnera ese derecho en la medida en que aquel archivo o registro se puede convertir en una fuente de información sobre la vida de una persona o su familia, menoscabando la confidencialidad de esa información, y que debe garantizarse mediante el establecimiento de las oportunas precauciones sobre la accesibilidad de la misma, pues el hecho mismo de la existencia de estos archivos y registros, conteniendo información sensible relativa a un individuo, puesta a disposición del poder público, entraña de suyo un grave riesgo para la intimidad individual” (FJ8).

²⁹⁷ CATE, F.H., MAYER-SCHÖNBERGER, V. y CULLEN, P. (2014). *Data Protection Principles for the 21st Century. Revising the 1980 OECD Guidelines*. Universidad de Oxford, pág. 18.

Por esta razón, “la existencia de ese archivo o registro, la información que en él puede almacenarse y su accesibilidad al conocimiento de otros poderes públicos o particulares debe estar sometida al estricto escrutinio del fin que lo legitime, que no puede ser otro que la realización efectiva de los límites constitucionales al derecho a la intimidad del art. 18.1 CE. De otro lado, el derecho a la intimidad impone a los poderes públicos la obligación de adoptar cuantas medidas fuesen necesarias para hacer efectivo aquel poder de disposición, y preservar de potenciales agresiones a ese ámbito reservado de la vida personal y familiar, no accesible a los demás; en especial, cuando la protección de otros derechos fundamentales o bienes constitucionalmente protegidos pueden justificar que ciertas informaciones relativas a una persona o su familia sean registradas y archivadas por un poder público, como es el caso del Registro Central de Penados y Rebeldes²⁹⁸” (FJ8).

Esta sentencia fue pionera en su momento y planteó una percepción del derecho a la intimidad distinta hasta el momento por el TC, pero no generó un *leading case*, y no fue seguida por su jurisprudencia. Como recogen Jacobs y Larrauri, si bien la anterior sentencia afirmó que “los antecedentes penales están protegidos por el derecho a la intimidad, en otras sentencias el propio TC (STC 223/1992, de 14 de diciembre) afirma que una sanción administrativa no puede ser considerada un dato privado comprendido

²⁹⁸ El Registro Central de Penados tiene por objeto, como recoge en su artículo 2.3.a) el real Decreto 95/2009, de 6 de febrero, por el que se regula el Sistema de registros administrativos de apoyo a la Administración de Justicia, “la inscripción de las resoluciones firmes por la comisión de un delito o falta que impongan penas o medidas de seguridad, dictadas por los Juzgados o Tribunales del orden jurisdiccional penal”. En su artículo 5 se reconoce que: “1. El Ministerio de Justicia autorizará, estableciendo las medidas de seguridad oportunas, el acceso directo a la información contenida en los Registros Centrales integrados en el Sistema, a: a) Los órganos judiciales, a través del personal de cada oficina judicial autorizado por el Secretario Judicial, a los efectos de su utilización en los procedimientos y actuaciones de los que están conociendo en el ámbito de sus respectivas competencias, conforme a las disposiciones legales vigentes. b) El Ministerio Fiscal, a través del personal de cada Fiscalía autorizado por el Fiscal Jefe, cuando ello resulte necesario para el cumplimiento de las funciones atribuidas al mismo por la Ley de Enjuiciamiento Criminal aprobada por real decreto de 14 de septiembre de 1882, la Ley Orgánica 5/2000, de 12 de enero, reguladora de la responsabilidad Penal de los menores y la Ley 50/1981, de 30 de diciembre, reguladora del Estatuto Orgánico del Ministerio Fiscal. 2. En cualquier caso, los interesados, acreditando su identidad, tendrán derecho a solicitar el acceso, mediante exhibición, únicamente a los datos relativos a su persona contenidos en cualquiera de los Registros a los que se refiere este real decreto”.

en el art.7.4 de la LO 1/1982²⁹⁹”. No obstante el TC admite su publicación “en un periódico siempre y cuando esta publicidad esté amparada por la libertad de información. Aun cuando se concluyese que una condena penal es un dato privado, un periódico podría publicarla sin incurrir en responsabilidad penal o civil si su divulgación está amparada por la libertad de información, es decir, la información es veraz, de relevancia pública y necesaria”³⁰⁰, añaden.

En opinión de Ignacio Villaverde, lo más acertado sería “hablar de concepto formal o material de intimidad”. El TC hasta su sentencia 134/1999, de 15 de julio “parecía haber mantenido un concepto material de intimidad según el cual lo es todo lo que razonablemente puede considerarse íntimo o privado”. Dicha sentencia introdujo un concepto diverso al tratar de dar respuesta a las siguientes cuestiones: “¿qué norma apodera al legislador o al juez, en particular al Constitucional, para decidir caso a caso qué sea íntimo y qué no? y ¿no debe ser el propio titular del derecho quien así lo haga? Ni siquiera en el caso de la intimidad territorial hay norma que atribuya al legislador o los jueces y tribunales la competencia para decidir qué espacios son íntimos. Es al titular del derecho fundamental a la intimidad quien tiene atribuida por él la competencia para determinar qué espacios o qué información son íntimos; en fin, qué de la vida de uno mismo, por banal que sea, debe estar oculto al conocimiento de terceros. Mucho más contundente fue en su FJ8³⁰¹ la STC 144/1999”³⁰².

²⁹⁹ Artículo 7.4: “Tendrán la consideración de intromisiones ilegítimas en el ámbito de protección delimitado por el artículo 2 de esta ley: la revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela”.

³⁰⁰ JACOBS, J. B. y LARRAURI, E. (2010). ¿Son las sentencias públicas? ¿Son los antecedentes penales privados? Una comparación de la cultura jurídica de Estados Unidos y España. *Revista InDret*. Barcelona, pág. 26.

³⁰¹ FJ8: “El art.18.1 CE no garantiza sin más la intimidad, sino el derecho a poseerla, a tener vida privada disponiendo de un poder de control sobre la publicidad de la información relativa a nuestra persona y familia, sea cual sea el contenido de aquello que se desea mantener al abrigo del conocimiento público. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías, y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información”.

³⁰² VILLAVERDE MENÉNDEZ, I. (2013). La intimidad, ese “terrible derecho... *ob. cit.*, pág. 63.

Con el paso de los años, en la jurisprudencia del TC se ha impuesto el concepto formal de identidad que señalaba Villaverde. Y esto concepto se ve claramente reflejado en la sentencia TC 173/2011³⁰³, de 7 de noviembre, ya que “su piedra angular es el consentimiento sobre el acceso a la información inicialmente considerada íntima. La intromisión contraria al artículo 18.1 CE del tercero privado en el derecho a la intimidad se produce cuando no media consentimiento de su titular porque le está imponiendo el deber unilateral de soportar el acceso a aquello que ha querido sustraer al conocimiento ajeno”³⁰⁴. En dicha sentencia se establece que “el derecho a la intimidad personal, en cuanto derivación de la dignidad de la persona (art. 10.1 CE), implica la existencia de un ámbito propio y reservado frente a la acción y el conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de la vida humana (SSTC 207/1996, de 16 de diciembre, FJ3; 186/2000, de 10 de julio, FJ5; 196/2004, de 15 de noviembre, FJ2; 206/2007, de 24 de septiembre, FJ 4; y 159/2009, de 29 de junio, FJ 3). De forma que «lo que el art. 18.1 garantiza es un derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuales sean los lindes de nuestra vida privada, pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio» (SSTC 127/2003, de 30 de junio, FJ 7 y 89/2006, de 27 de marzo, FJ 5). Del precepto constitucional citado se deduce que el derecho a la intimidad confiere a la persona el poder jurídico de imponer a terceros el deber de abstenerse de toda intromisión en la esfera íntima y la prohibición de hacer uso de lo así conocido (SSTC 196/2004, de 15 de noviembre, FJ 2; 206/2007, de 24 de septiembre, FJ 5; y 70/2009, de 23 de marzo, FJ 2). No obstante lo anterior, hemos afirmado que el consentimiento eficaz del sujeto particular permitirá la inmisión en su derecho a la intimidad, pues corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno (SSTC 83/2002, de 22 de abril, FJ 5 y 196/2006, de 3 de julio, FJ 5), aunque este

³⁰³ El recurrente fue condenado como autor de un delito de corrupción de menores en su modalidad de distribución de pornografía infantil, presentando su demanda de amparo por considerar que se había fundado la condena en prueba de cargo obtenida con vulneración del derecho a la intimidad, al haber accedido tanto el denunciante de los hechos, como después la policía, a determinados archivos del ordenador del demandante de amparo sin su consentimiento y sin autorización judicial.

³⁰⁴ VILLAVERDE MENÉNDEZ, I. (2013). La intimidad, ese “terrible derecho... *ob. cit.*, pág. 65.

consentimiento puede ser revocado en cualquier momento (STC 159/2009, de 29 de junio, FJ 3)” (FJ2).

El TC descartó que la actuación del denunciante vulnerara el derecho a la intimidad del recurrente, ya que “se aprecia claramente en el recurrente una declaración expresiva de su voluntad de hacer entrega a dicho encargado de su portátil, poniéndolo a su disposición, para que éste procediera a su reparación (en concreto, para cambiar la grabadora que no funcionaba). Para ello le informa, incluso, como hemos visto, de que no precisa de contraseña alguna de acceso. Las razones que hayan podido llevar al recurrente a adoptar esta actitud, ya sean debidas a negligencia, descuido o desconocimiento del carácter ilícito de los referidos archivos escapan, evidentemente, al análisis que debe realizarse en este TC. Así las cosas, durante el desempeño de la función encomendada, el responsable del establecimiento informático descubrió casualmente el material pedófilo, en particular cuando, una vez reparado el ordenador, procedía a comprobar su correcto funcionamiento. A tal fin, escogió al azar diversos archivos para llevar a cabo su grabación y posterior reproducción, lo que le permitiría conocer el correcto funcionamiento de las piezas sustituidas, práctica que, según se acreditó durante el juicio, constituye el protocolo habitual en estos casos. De lo expuesto, se deduce que dicho responsable no se extralimitó del mandato recibido estando amparado su proceder, que ha llevado al descubrimiento del material ilícito, por la propia autorización expresa del ahora demandante. Una vez producido el hallazgo, aquél se limitó a cumplir con la obligación que le viene legalmente impuesta a todo ciudadano consistente en denunciar ante las autoridades competentes la posible perpetración de un delito público del que ha tenido conocimiento” (FJ5).

En cuanto a la actuación de la Policía, el TC considera que “la conducta adoptada por la policía perseguía un fin legítimo, por cuanto se enmarcaba dentro de las investigaciones que ésta realizaba dirigidas al esclarecimiento de un delito de pornografía infantil. Al propio tiempo existe la habilitación legal necesaria para la realización, por parte de los agentes intervinientes, de este tipo de pesquisas, pues, como hemos visto, se encuentran entre sus funciones las de practicar las diligencias necesarias para comprobar los delitos, descubrir sus autores y recoger los efectos, instrumentos o pruebas, pudiendo efectuar un primer análisis de los efectos intervenidos. Finalmente, si bien la intervención policial desplegada no contó con la previa autorización judicial, circunstancia ésta que

ha llevado a considerar, tanto al recurrente como al Fiscal, que se había producido en este caso una vulneración del derecho a la intimidad personal, podemos afirmar que nos encontramos ante uno de los supuestos excepcionados de la regla general, que permite nuestra jurisprudencia, pues existen y pueden constatarse razones para entender que la actuación de la policía era necesaria, resultando, además, la medida de investigación adoptada razonable en términos de proporcionalidad” (FJ7).

En contraposición al concepto formal o material de intimidad que señala Villaverde, Javier Mieres opta por hablar de intimidad territorial e intimidad informacional. En el caso de la intimidad territorial, “se protegen espacios o zonas de aislamiento frente a la intrusión de extraños. Estos ámbitos propios y reservados protegidos por el derecho fundamental abarcan realidades diversas: desde las zonas íntimas del propio cuerpo a la denominada propia esfera de desenvolvimiento del individuo, noción potencialmente amplísima, pero que el TC ha ceñido a espacios vitales que presentan una vinculación fuerte y directa con los principios de dignidad humana y libre desarrollo de la personalidad”. En cuanto a la intimidad informacional, apunta que “tiene por objeto las informaciones relativas a la vida privada de las personas. La noción de información constitucionalmente protegida desde el punto de vista del derecho a la intimidad y respecto de la cual son legítimos la reserva y el silencio impuesto a terceros, se debate en nuestra jurisprudencia constitucional entre una definición objetiva (información considerada objetivamente íntima y conforme a estándares sociales dominantes en la medida en que se proyecta sobre los más básicos aspectos de la autodeterminación como persona) y subjetiva (información subjetivamente reservada, a voluntad del titular del derecho, y con independencia de su contenido)”³⁰⁵.

Es evidente que todos tenemos un pasado y que las personas pueden tomar decisiones erróneas, pero eso no quita que una vez superadas pueda rehacer su vida sin tener que estar dando continuamente explicaciones, ya que una condena en el pasado no le hace más o menos capaz para desempeñar un puesto de trabajo, aunque si la persona encargada de contratarle cuenta con esa información ya va a estar sugestionado a la hora de hacerlo.

³⁰⁵ MIERES MIERES, L. J. (2002). *Intimidad personal y familiar. Prontuario de Jurisprudencia Constitucional*. Editorial Aranzadi. Navarra, pág. 25.

El ordenamiento jurídico español, al contrario que otros países como Estados Unidos, reconoce la cancelación de los antecedentes penales a: “los condenados que hayan extinguido su responsabilidad penal y que tienen derecho a obtener del Ministerio de Justicia, de oficio o a instancia de parte, la cancelación de sus antecedentes penales, cuando hayan transcurrido sin haber vuelto a delinquir los siguientes plazos: a) Seis meses para las penas leves. b) Dos años para las penas que no excedan de doce meses y las impuestas por delitos imprudentes. c) Tres años para las restantes penas menos graves inferiores a tres años. d) Cinco años para las restantes penas menos graves iguales o superiores a tres años. e) Diez años para las penas graves”³⁰⁶. Además, preserva el anonimato en las sentencias o utiliza nombres ficticios. Por lo tanto, sin darse cuenta, el ordenamiento jurídico español reconoce un derecho al olvido a los delincuentes que ya hayan cumplido su condena con el fin de que puedan reintegrarse, con más facilidad y sin prejuicios, en la sociedad. Algo parecido sucede en Francia, en el que el derecho a la prescripción de los antecedentes penales se encuentra ya recogido en su ordenamiento jurídico a través del artículo 35 de la *Loi sur la liberté de la presse*, de 29 de julio de 1881³⁰⁷.

En los Estados Unidos, no se protege el derecho al olvido en estos casos, al considerar “inevitable y tal vez deseable que la condena penal avergüence a la persona condenada, porque además de servir a la prevención, la publicidad de la condena también promueve el objetivo resocializador pues la vergüenza puede contribuir a la rehabilitación si provoca arrepentimiento”. Por ese motivo, “la amplia difusión de las condenas mejora, sin duda, la seguridad pública. Si los miembros de la sociedad saben por ejemplo, que

³⁰⁶ Artículo 136.1 de la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

³⁰⁷ Artículo 35 de la *Loi sur la liberté de la presse*, de 29 de julio de 1881, modificada por la Loi n°98-468, de 17 de junio de 1998: “La verdad de un hecho difamatorio cuando es relativo a las funciones, podrá establecerse por vías ordinarias en el caso de imputaciones contra órganos constitucionales, ejército de tierra, mar o aire, administraciones públicas y contra cualquiera de las personas enumeradas en el artículo 31. La verdad de las imputaciones difamatorias o injuriosas podrá establecerse igualmente contra los directores o administradores de cualquier empresa industrial, comercial o financiera que cotice en bolsa. La verdad de los hechos difamatorios puede probarse siempre, salvo: a) Que la imputación concierna a la vida privada de la persona. b) Que la imputación se refiera a hechos ocurridos hace más de diez años. c) Que la imputación se refiera a un hecho que constituya un delito por el que se haya concedido amnistía o que haya prescrito o que haya dado lugar a una condena que haya sido rehabilitada o revisada”.

alguien es un estafador, pueden protegerse a sí mismos no invirtiendo dinero con él”³⁰⁸. Contemplamos así la gran diferencia que existe a la hora de abordar el olvido de los antecedentes penales entre el sistema *common law* (Estados Unidos) y el civilista (España y Francia).

Esto se debe a que la privacidad en los Estados Unidos, se basa, como apunta Emerson, “en premisas del individualismo y en la existencia de la sociedad para promover el valor y la dignidad del individuo. El derecho a la vida privada es esencialmente el derecho a no participar en la vida colectiva. En este contexto la necesidad urgente de un derecho de privacidad en el sistema de los derechos individuales es manifiesta. El alcance cada vez mayor de la intervención gubernamental en la mayoría de ámbitos de la vida nacional, el desarrollo de la tecnología moderna para sonsacar y el seguimiento de los asuntos de todo el mundo desde el vientre a la tumba, el cierre de espacio físico y psíquico para la persona promedio, todos hacen la necesidad de crear de una ley de la privacidad adecuada imperativo para la salud futura de nuestra sociedad. Es esencial, por tanto, conciliar esta nueva área de los derechos individuales con los principios establecidos de la libertad de prensa. Los peligros se manifiestan, debido a la interferencia gubernamental en la libertad de expresión en cualquier forma, inevitablemente, supone una amenaza para el sistema de derechos individuales”³⁰⁹. Por su parte, Solove considera que “la privacidad ha sido durante mucho tiempo una selva conceptual que ha enredado derecho y política”, y, por eso, propone una nueva forma de conceptualizar la privacidad, entendiendo la privacidad como “un conjunto de protecciones contra una pluralidad de problemas distintos pero relacionados. Estos problemas no están relacionados por un denominador común o elemento central. En cambio, cada problema tiene elementos en común con otro, pero no necesariamente el mismo elemento. Denominamos a todo el conjunto como privacidad, pero este término es útil primordialmente como una forma abreviada de describir el conjunto”³¹⁰.

Pero, ¿todos los antecedentes penales han de tener el mismo tratamiento? En nuestra opinión, hay sectores laborales que tendrían que tener un marco normativo especial y para los que sería necesario conocer los antecedentes penales de los candidatos. En el

³⁰⁸ JACOBS, J. B. y LARRAURI, E. (2010). ¿Son las sentencias públicas?... *ob. cit.*, pág. 25.

³⁰⁹ EMERSON, T. (1979). *The Right of Privacy and Freedom of the Press*. Yale Law School, pág. 331.

³¹⁰ SOLOVE, D. J. (2009). *Understanding Privacy...* *ob. cit.*, págs. 171-172.

caso de aquellas personas que fuesen condenadas por un delito contra los menores, no sería ético ni moral que desempeñase una función de profesor o monitor, trabajando con niños, esa información sí resultaría de interés para los contratantes. Así lo ha entendido el Gobierno que en la Ley 26/2015, de 28 de julio, de modificación del sistema de protección a la infancia y a la adolescencia, que modifica la Ley Orgánica 1/1996, de 15 de enero, de protección jurídica del menor, de modificación del Código Civil y de la Ley de Enjuiciamiento Civil, considera que “será requisito para el acceso y ejercicio a las profesiones, oficios y actividades que impliquen contacto habitual con menores, el no haber sido condenado por sentencia firme por algún delito contra la libertad e indemnidad sexual, que incluye la agresión y abuso sexual, acoso sexual, exhibicionismo y provocación sexual, prostitución y explotación sexual y corrupción de menores, así como por trata de seres humanos. A tal efecto, quien pretenda el acceso a tales profesiones, oficios o actividades deberá acreditar esta circunstancia mediante la aportación de una certificación negativa del Registro Central de delincuentes sexuales”³¹¹.

El Registro Central de delincuentes sexuales constituye “un sistema de información, de carácter no público y gratuito, relativo a la identidad, perfil genético (ADN), penas y medidas de seguridad impuestas a aquellas personas condenadas en sentencia firme por cualquier delito contra la libertad e indemnidad sexuales o por trata de seres humanos con fines de explotación sexual, incluyendo la pornografía con independencia de la edad de la víctima. Esta información se referirá a las condenas dictadas tanto en España como en otros países, en particular los Estados miembros de la Unión Europea y del Consejo de Europa. La finalidad del Registro es contribuir a la protección de los menores contra la explotación y el abuso sexual, con independencia de quién sea el autor del delito, mediante el establecimiento de un mecanismo de prevención que permita conocer si quienes pretenden el acceso y ejercicio de profesiones, oficios y actividades que impliquen el contacto habitual con menores, carecen o no de condenas penales por los delitos a los que se refiere el apartado anterior. Asimismo, el Registro tiene como fin facilitar la investigación y persecución de los delitos a que se refiere el presente real decreto con objeto de proteger a las víctimas menores de edad de la delincuencia sexual, introduciendo medidas eficaces que contribuyan a la identificación de sus autores y de

³¹¹ Artículo 13.5.

cooperación con las autoridades judiciales y policiales de otros países, en particular con los Estados miembros de la Unión Europea y del Consejo de Europa”³¹². Dicho Registro, como se recoge en el artículo 5, no incluirá “los datos de identidad de la víctima, salvo, en su caso, su condición de menor de edad”.

5.5.3.2. Las sanciones administrativas también prescriben

Tiene sentido que las infracciones administrativas prescriban, ya que el Estado ha de tener unos plazos para poder sancionar a las personas, no dejándoles en la incertidumbre de que, en cualquier momento de su vida, se les pueda exigir una responsabilidad administrativa por hechos acaecidos en el pasado. La prescripción de estas viene recogida, tanto para las infracciones cometidas como para las sanciones impuestas, en el artículo 30 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público establece que “1. Las infracciones y sanciones prescribirán según lo dispuesto en las leyes que las establezcan. Si éstas no fijan plazos de prescripción, las infracciones muy graves prescribirán a los tres años, las graves a los dos años y las leves a los seis meses; las sanciones impuestas por faltas muy graves prescribirán a los tres años, las impuestas por faltas graves a los dos años y las impuestas por faltas leves al año. 2. El plazo de prescripción de las infracciones comenzará a contarse desde el día en que la infracción se hubiera cometido. En el caso de infracciones continuadas o permanentes, el plazo comenzará a correr desde que finalizó la conducta infractora. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, de un procedimiento administrativo de naturaleza sancionadora, reiniciándose el plazo de prescripción si el expediente sancionador estuviera paralizado durante más de un mes por causa no imputable al presunto responsable. 3. El plazo de prescripción de las sanciones comenzará a contarse desde el día siguiente a aquel en que sea ejecutable la resolución por la que se impone la sanción o haya transcurrido el plazo para recurrirla. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si aquél está paralizado durante más de un mes por causa no imputable al infractor. En el caso de desestimación presunta del recurso de alzada interpuesto contra la resolución por la que se impone la sanción, el plazo de prescripción de la sanción comenzará a contarse desde el día

³¹² Artículo 3 del Real Decreto 1110/2015, de 11 de diciembre, por el que se regula el Registro Central de Delincuentes Sexuales.

siguiente a aquel en que finalice el plazo legalmente previsto para la resolución de dicho recurso”.

Es importante distinguir, como señala Such, entre prescripción y caducidad, ya que “decimos que una acción está prescrita cuando ha transcurrido un espacio temporal contemplado en la norma que impide el inicio del procedimiento bajo el amparo de la legalidad”, mientras que, cuando se habla de caducidad, “no estamos refiriendo al espacio temporal máximo que puede durar un procedimiento... cuando se inicia un procedimiento sancionador necesariamente debe quedar finalizado dentro de esos márgenes temporales que para cada supuesto establece la norma ya que, si tal espacio temporal se sobrepasa o se excede sin justificación, indefectiblemente debe ponerse fin al procedimiento en el estado en que se encuentre, declarándose caducado y debiéndose comenzar de nuevo desde la casilla de salida; claro está, siempre que para entonces la infracción no hubiera prescrito”³¹³.

5.5.4. Interés público vs. Interés privado en la privacidad

El TC ha definido el derecho fundamental a la propia imagen como “un derecho constitucional autónomo que dispone de un ámbito específico de protección frente a reproducciones de la imagen que, afectando a la esfera personal de su titular, no lesionan su buen nombre ni dan a conocer su vida íntima, pretendiendo la salvaguarda de un ámbito propio y reservado, aunque no íntimo, frente a la acción y conocimiento de los demás. Por ello atribuye a su titular la facultad para evitar la difusión incondicionada de su aspecto físico, ya que constituye el primer elemento configurador de la esfera personal de todo individuo, en cuanto instrumento básico de identificación y

³¹³ SUCH MARTÍNEZ, J. (2016). La prescripción y la caducidad en derecho administrativo. Dos instituciones vinculadas al espacio temporal del comienzo y finalización del procedimiento. *Economist & Jurist*. Vol. 24, nº199, págs. 20-29. En este sentido, la caducidad en el derecho público a diferencia del derecho privado es “un mecanismo extintivo que tiene por objeto garantizar la correcta satisfacción del interés general. Es decir, la caducidad es una vía de canalización de las relaciones jurídicas por cuanto, en virtud del interés general el ordenamiento jurídico, impone que tanto en el derecho público como en el derecho privado las acciones y recursos sean ejercidos dentro de un plazo concreto, que los procedimientos no queden estancados indefinidamente, y que los derechos otorgados en términos favorables sean realmente aprovechados por sus titulares”. CABALLERO SÁNCHEZ, R. (1999). *Prescripción y caducidad en el ordenamiento administrativo*. McGraw-Hill. Madrid, pág. 92.

proyección exterior y factor imprescindible para su propio reconocimiento como sujeto individual” (SSTC 231/1988, de 2 de diciembre FJ3; 99/1994, de 11 de abril, FJ5).

El derecho a la propia imagen, definido, según Touriño, como “la representación gráfica de la figura humana, que incluye el nombre y la voz, es un derecho fundamental reconocido en la CE”. Esta teoría, según añade, estaba configurada para “un mundo en el que no existía Internet, pero es plenamente aplicable a Internet y sus novedosos modelos de negocios. Piénsese si no en cualquier red social o plataforma en la que se suban miles de fotografías, dichas fotografías podrán ser meras reproducciones de paisajes u objetos, que en nada afectan al derecho a la propia imagen. Pero podrán ser también fotos en las que aparecen personas, que, según lo establecido por la legislación vigente, tienen su derecho a la propia imagen. Es decir, cualquier persona que vea su imagen reproducida en Internet estaría, en principio facultado para requerir a quien la haya publicado para que proceda su retirada”³¹⁴.

La captación, reproducción y publicación no consentida de imágenes de personas anónimas desnudas o semidesnudas tomando el sol en una playa con el único objetivo de difundirlas constituye una intromisión ilegítima. El TS en su sentencia 3818/2002, de 28 de mayo. Sala de lo Civil (número de recurso: 3761/1996), señaló que “todo ciudadano puede establecer diferentes ámbitos o espacios físicos para desenvolver su vida íntima, los cuales, en principio han de ser respetados. Así sucede respecto a la llamada intimidad en soledad, pero también es protegible una intimidad sin aislamiento, cuando la misma se circunscribe a un ámbito familiar o a otro círculo personal restringido. No puede pensarse, en cambio, en reclamar intimidad en ámbitos o espacios públicos, pues los actos públicos y los lugares abiertos al público no son compatibles con la idea de privacidad. En dicho supuesto, el sr. Luis Antonio, en el momento de ser fotografiado, no se hallaba, evidentemente en su morada, sino en una playa. Aun cuando estos parajes se hallan legalmente considerados como bienes de dominio público por estar destinados al uso público, (artículo 339.1º del Código Civil) no puede olvidarse que dentro del pluralismo y del derecho al libre desarrollo de la personalidad que caracterizan a un Estado democrático de Derecho, ha ido surgiendo una aceptación

³¹⁴ TOURIÑO, A. (2014). *El derecho al olvido y a la intimidad en Internet*. Los Libros de la Catarata. Madrid, págs. 85-86.

social del hecho de que determinadas zonas de espacios destinados al uso público o común puedan ser utilizadas por los ciudadanos que consideran que conviene al ejercicio de ciertas actividades físicas el máximo contacto con la naturaleza, despojándose de los obstáculos que al efecto puedan significar no solo las ropas de uso cotidiano, sino incluso aquellas otras más ligeras, que para la práctica de los deportes utiliza un sector realmente mayoritario de la población. A través de esa común aceptación de la conveniencia de la restricción de uso de zonas como las playas nudistas, los grupos a que nos referimos pueden proceder al ejercicio de una libertad que les reconoce el artículo 9.2 de la Constitución sin molestar a los ciudadanos que no aprueban sus pautas de comportamiento, ni ser inquietados por ellos” (FJ4).

Internet ha hecho que la proliferación de imágenes no autorizadas de personas en lugares públicos, captadas, en su mayoría, por teléfonos móviles y difundidas a través de las redes sociales haya crecido exponencialmente. En este sentido, también los medios de comunicación se ven afectados, ya que, en algunas ocasiones, los intereses privados de las personas físicas se encuentran enfrentados con el derecho a la información en dichos medios, teniendo que ceder y permitir que prime el derecho a la propia imagen frente al derecho a la información.

La divulgación, como apunta Mieres, afecta al derecho a la intimidad “en la medida en que se hacen públicos para los demás determinados datos de la vida privada de una persona que el particular pretende mantener reservados. Y es que el carácter reservado de los datos sobre la propia vida es siempre relativo, una misma información se puede compartir con algunos y negar a otros. Nuestras vidas son relativamente opacas y relativamente transparentes, a nuestra elección. La divulgación de un dato no conocido por aquellos con quienes mantenemos una relación y que hemos querido mantener reservado, lesiona el derecho. Y es que la intimidad no sólo se lesiona en el caso de los famosos”³¹⁵. Ahora bien, para Carrillo, en una sociedad como la actual “donde la imagen es un valor añadido al comportamiento social, no puede hacerse una abstracción de las enormes posibilidades de que la imagen de una persona pueda ser difundida sin

³¹⁵ MIERES MIERES, L. J. (2002). *Intimidad personal y familiar...ob. cit.*, págs. 64-65.

que forzosamente o, en todo caso, tal circunstancia conlleve una exigencia de responsabilidad”³¹⁶.

Como indica el artículo 8.2.a) de la LO 1/1982: “cualquier persona física, profesional o medio de comunicación se encuentra legitimado para captar, reproducir o difundir en cualquier plataforma digital o tradicional, la imagen de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se hubiera captado durante un acto público o en lugares abiertos al público”. Por lo tanto, la Ley no impide la captación, reproducción y publicación de estas imágenes siempre que se realicen en un lugar público, no siendo necesario que éstas den su consentimiento para que su imagen pueda ser recogida en los medios de comunicación o en cualquier otro espacio digital, aunque sólo cuando se emplee con fines informativos³¹⁷. La información

³¹⁶ CARRILLO LÓPEZ, M. (2003). *El derecho a no ser molestado... ob. cit.*, pág. 88.

³¹⁷ En cuanto a lo que es objeto principal de la noticia o reportaje gráfico, el TC en su sentencia 72/2007, de 16 de abril, denegó el recurso de amparo de una sargento de la Policía Municipal de Madrid que demandó a la sociedad editora del periódico Diario 16, su director y un fotógrafo, por una presunta intromisión en su derecho a la imagen, a consecuencia de la publicación en la portada del periódico el día 2 de octubre de 1992, de una fotografía tomada durante una actuación profesional de auxilio a una comisión judicial para el desalojo de determinadas viviendas, fotografía que identificaba plenamente y en primer plano a la demandante, e ilustrada con el titular «Desalojo violento». Más tarde, en la información aparecida sobre el mismo desalojo en la página 27 del periódico correspondiente al día 9 de octubre de 1992, se incluyó una fotografía de los afectados por el desalojo en actitud de protesta, en la que se observa la utilización de la fotografía de la demandante que apareció en la portada del periódico del día 2 de octubre de 1992. El TC consideró que “el derecho de los periodistas a difundir libremente información veraz prevalece en este caso sobre el derecho a la propia imagen de la demandante, toda vez que la controvertida fotografía de ésta fue captada en un lugar público, con ocasión de un acto público y en el ejercicio por la demandante de su cargo y profesión, que constituyen cargo público y profesión de proyección pública, por lo que resulta aplicable lo dispuesto en el art. 8.2 a) de la LO 1/1982, de 5 de mayo. Además, la reproducción fotográfica tiene carácter accesorio respecto de la información escrita, la cual es veraz y con evidente trascendencia o interés público, siendo incuestionable la relación que guarda la fotografía con la información escrita, pues resulta ilustrativa de lo que se pretendía comunicar, esto es, la resistencia de unos vecinos a desalojar unas viviendas, a pesar de existir una orden judicial, por lo que fue necesario el auxilio de la policía municipal a la comisión judicial encargada del desalojo” (FJ4). La sentencia reconoce que “no se discute que la fotografía controvertida publicada en la portada del periódico reproduce de forma nítida el rostro de la demandante –aunque no aparece identificada por su nombre y apellidos– ni que la publicación de la imagen se produjo sin el consentimiento de la demandante. Ahora bien, el derecho a la propia imagen no es absoluto o incondicionado, de suerte que

gráfica destinada a otros fines, como los publicitarios y comerciales, requiere siempre un consentimiento expreso previo a través de un contrato de cesión de imagen. Cuando se trata de personas sin proyección pública, la captación, reproducción o publicación de su imagen es “una intromisión ilegítima”, salvo que haya prestado el debido consentimiento expreso. La STS 769/2006, de 22 de febrero. Sala de lo Civil (número de recurso: 2926/2001) reconoce que “el consentimiento presunto no elimina la intromisión; además, este consentimiento no puede ser general, sino que habrá de referirse a cada concreto acto de intromisión, según se desprende de los artículos 2.2 y 8.1 LO 1/1982, lo que deriva del carácter irrenunciable que tiene este derecho, según lo dispuesto en el artículo 1.3 LO 1/1982” (FJ4).

En este sentido ha de tenerse presente que el examen de la fotografía y del texto que la acompaña pone de manifiesto que estamos ante un documento que reproduce la imagen de una persona en el ejercicio de un cargo público y así lo recoge la STS 1750/2003, de 14 de marzo. Sala de lo civil (nº de recurso: 2313/1997), en la que la propia demandante de amparo admite expresamente que por su condición de Sargento de la policía municipal de Madrid desempeña un cargo público y que la fotografía en cuestión fue captada con motivo de un acto público (un desalojo por orden judicial, que para ser llevado a cabo precisó del auxilio de los agentes de la policía municipal, ante la resistencia violenta de los afectados), en un lugar público (una calle de un barrio madrileño), por lo que en modo alguno resulta irrazonable concluir, como se razona en la Sentencia impugnada, que concurre el supuesto previsto en el art. 8.2 a) de la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad

existen circunstancias que pueden determinar que la regla general conforme a la cual es al titular de este derecho a quien, en principio, corresponde decidir si permite o no la captación y difusión de su imagen por un tercero, ceda a favor de otros derechos o intereses constitucionalmente legítimos, lo que ocurrirá en los casos en los que exista un interés público en la captación o difusión de la imagen y este interés público se considere constitucionalmente prevalente al interés de la persona en evitar la captación o difusión de su imagen. Por ello, cuando el derecho a la propia imagen entre en colisión con otros bienes o derechos constitucionalmente protegidos, particularmente las libertades de expresión e información, deberán ponderarse los distintos intereses enfrentados y, atendiendo a las circunstancias concretas de cada caso, decidir qué interés merece mayor protección, si el interés del titular del derecho a la imagen en que sus rasgos físicos no se capten o difundan sin su consentimiento o el interés público en la captación o difusión de su imagen (STC 156/2001, de 2 de julio, FJ6)” (FJ5).

personal y familiar y a la propia imagen. Por otra parte, resulta asimismo incuestionable que la información que se transmite por el periódico es veraz y tiene evidente trascendencia pública. Además, la fotografía en cuestión (y pese a lo que se alega en la demanda de amparo) tiene carácter accesorio respecto de la información publicada y no refleja a la demandante realizando cosa distinta que no sea el estricto cumplimiento de su deber, como igualmente se explica en la Sentencia impugnada, por lo que tampoco resulta irrazonable concluir que concurre el supuesto previsto en el primer inciso del art. 8.2 c) de la Ley Orgánica 1/1982, de 5 de mayo. En fin, aunque es cierto que la utilización de cualquier técnica de distorsión u ocultamiento del rostro de la demandante habría posibilitado que la noticia del desalojo violento hubiera llegado a los lectores de igual manera y sin merma alguna, como se sostiene en la demanda de amparo, no lo es menos que, tal como se afirma en la Sentencia recurrida en amparo, no estamos ante un caso concreto que exija el anonimato, sin perjuicio de que en otros pudiera exigirlo [último inciso del art. 8.2 c) de la Ley Orgánica 1/1982, de 5 de mayo]. En efecto, en contra de lo que se aduce por la demandante de amparo, no cabe apreciar que, en las circunstancias de este caso, existan razones de seguridad para ocultar el rostro de un funcionario policial por el mero hecho de intervenir, en el legítimo ejercicio de sus funciones profesionales, en una actuación de auxilio a una comisión judicial encargada de ejecutar una orden de desalojo, ante la decidida resistencia de los ciudadanos afectados.

El TC extendió en su sentencia 139/2001, de 18 de junio³¹⁸, el alcance del derecho fundamental a la propia imagen a los personajes públicos al considerar que las fotografías publicadas “se insertan en el ámbito propio y reservado de lo que es la esfera personal de los afectados. Su pertenencia ha dicho ámbito personal y privado queda además acreditado por las propias circunstancias de hecho que han rodeado a las

³¹⁸ “La revista Diez Minutos publicó un reportaje titulado “Las fotos más esperadas de Marta Chávarri y Alberto Cortina”, que incluía cinco fotografías en las que aparecía el demandante, y que fueron obtenidas por un pariente del señor Cortina de Alcocer en una reserva de caza en Kenia durante un viaje privado que aquéllos realizaron junto a familiares y amigos el año anterior a la publicación del reportaje en cuestión. Las referidas fotografías llegaron a poder de don Luis Gozalo, titular de la agencia España Reportajes y autor del citado reportaje, quien lo vendió por ocho millones de pesetas a Gráficas Espejo, S.A., entidad editora de la revista. El Sr. Gozalo se amparó en el secreto profesional para no desvelar el nombre de la persona que le facilitó las fotos, si bien confesó que no le fueron transferidas por quienes aparecen en ellas ni por el autor de las mismas, admitiendo la ilicitud de su procedencia” (FJ5).

fotografías cuestionadas: su obtención por un pariente del ahora recurrente, con la cámara de éste, en el contexto de un viaje privado de familiares y amigos y con destino a un recuerdo íntimo. En el contexto que acaba de expresarse queda evidenciado dicho carácter personal, privado y reservado de las expresadas fotografías, cualesquiera que fueran las personas a las que reproducían y el lugar en que se hubieran hecho. Por otra parte, no deja de ser revelador a tal efecto el hecho de que dichas fotografías hayan salido a la luz pública sin el consentimiento del interesado y mediante una operación de terceros ajena a su voluntad” (FJ5).

La sentencia reconoce también que, aunque “no puede deducirse del art. 18 CE que el derecho a la propia imagen, en cuanto límite del obrar ajeno, comprenda el derecho incondicionado y sin reservas a permanecer en el anonimato. Pero tampoco el anonimato, como expresión de un ámbito de reserva especialmente amplio, es un valor absolutamente irrelevante, de modo que quede desprotegido el interés de una persona a salvaguardarlo impidiendo que su imagen se capte y se difunda. Lo que se pretende con este derecho, en su dimensión constitucional, es que los individuos puedan decidir qué aspectos de su persona desean preservar de la difusión pública, a fin de garantizar un ámbito privativo para el desarrollo de la propia personalidad ajeno a injerencias externas (STC 81/2001, de 26 de marzo, FJ2)”. En definitiva, atendiendo a las circunstancias expuestas, “la publicación por parte de la revista Diez Minutos de las fotografías privadas del recurrente, sin su consentimiento, constituyó una intromisión ilegítima en su derecho a la propia imagen (art. 18.1 CE) que, en este caso, no puede encontrar protección en el derecho a comunicar libremente información veraz (art. 20.1.d CE), el cual se encuentra constitucionalmente limitado de forma expresa por aquel derecho (art. 20.4 CE)” (FJ5).

En términos similares se pronuncia la sentencia TC 83/2002, de 22 de abril³¹⁹, al afirmar que “el recurrente es, desde luego, una persona con notoriedad pública por

³¹⁹ “La revista Diez Minutos publicó unas fotografías de Alberto Alcocer junto con Margarita Hernández, en las que aparecen ambos tumbados en una playa, en situación de afectividad, y que fueron tomadas con la cámara fotográfica de Alcocer por un amigo suyo, quien se la devolvió al señor Alcocer, procediendo posteriormente éste a su revelado. Dichas fotografías, sin quedar determinado a través de qué medio, llegaron a poder de don Luis Gonzalo, quien las vendió por cuatro millones de pesetas a la mercantil Editorial Gráficas Espejo, S.A., la cual sin recabar el consentimiento de los que aparecen en ellas,

diversas razones, entre ellas su frecuente presencia en los medios de comunicación exponiendo al conocimiento de terceros su actividad profesional, por lo que cabe incluirla en el grupo de aquellos sujetos que, junto con quienes tienen atribuidas la administración del poder público, por su actividad asumen un mayor riesgo frente a informaciones que les conciernen. No obstante si bien los personajes con notoriedad pública inevitablemente ven reducida su esfera de intimidad, no es menos cierto que, más allá de ese ámbito abierto al conocimiento de los demás su intimidad permanece y, por tanto, el derecho constitucional que la protege no se ve minorado en el ámbito que el sujeto se ha reservado y su eficacia como límite al derecho de información es igual a la de quien carece de toda notoriedad (SSTC 115/2000, de 10 de mayo, FJ5; y 134/1999, de 15 de julio, FJ7). De otro lado, no toda información que se refiere a una persona con notoriedad pública goza de esa especial protección, sino que para ello es exigible, junto a ese elemento subjetivo del carácter público de la persona afectada, el elemento objetivo de que los hechos constitutivos de la información, por su relevancia pública, no afecten a la intimidad, por restringida que ésta sea (STC 197/1991, FJ 4). Pues bien, la notoriedad pública del recurrente en el ámbito de su actividad profesional, y en concreto su proyección pública en el campo de las finanzas, no le priva de mantener, más allá de esta esfera abierta al conocimiento de los demás, un ámbito reservado de su vida como es el que atañe a sus relaciones afectivas, sin que su conducta en aquellas actividades profesionales elimine el derecho a la intimidad de su vida amorosa, si por propia voluntad decide, como en este caso, mantenerla alejada del público conocimiento ya que corresponde a cada persona acotar el ámbito de intimidad personal y familiar que reserva al conocimiento ajeno. De nuevo, las circunstancias en que las fotografías fueron captadas, difundidas y presentadas ponen de relieve que, en este caso, no se justifica el descenso de las barreras de reserva impuestas por el propio recurrente; a tal efecto es irrelevante el sólo dato de que las imágenes fueran captadas en una playa, como lugar abierto al uso público, pues ello no elimina la relevante circunstancia de que aquéllas fueron obtenidas en el círculo íntimo de las personas afectadas, sin que éstas, atendidas todas las circunstancias concurrentes, descuidasen su

procedió a su publicación en la portada de la citada revista, en su número de 22 de febrero de 1991, con el titular: «Tras el escándalo Alberto Cortina-Marta Chávarri, ahora gran exclusiva: las fotos definitivas de Alberto Alcocer y Margarita Hernández». Las controvertidas fotografías sirvieron también para confeccionar un cartel publicitario de la revista, distribuido en los puestos de venta, y una de ellas, como se ha dicho, fue nuevamente publicada en un número posterior” (FJ3).

intimidad personal y familiar, abriéndola al público conocimiento”. La sentencia concluye que “es claro que la revelación de las relaciones afectivas del recurrente, propósito inequívoco del reportaje en el que se incluyen las controvertidas fotografías, carece en absoluto de cualquier trascendencia para la comunidad porque no afecta al conjunto de los ciudadanos ni a la vida económica o política del país, al margen de la mera curiosidad generada por la propia revista en este caso al atribuir un valor noticioso a la publicación de las repetidas imágenes, el cual no debe ser confundido con un interés público digno de protección constitucional” (FJ5).

Frente a esta línea jurisprudencial del TC, el Supremo, como señala De la Iglesia, “se viene mostrando mucho más restrictivo con el alcance de la reserva del derecho a la intimidad y del derecho a la propia imagen de los personajes populares y, en general, entiende que «en el caso de una persona de proyección pública (como puede ser, entre otros casos, una actriz de cine y televisión) su derecho al honor disminuye, su derecho a la intimidad se diluye y su derecho a la imagen se excluye, y este último se excluye en aplicación de lo dispuesto en el artículo 8.2.a) de la Ley de 5 de mayo de 1982 que no considera intromisión la publicación de imagen de persona de proyección pública en lugar público» {SSTS 7765/1997³²⁰, de 17 de diciembre de 1997. Sala de lo Civil

³²⁰ El demandante (Alberto Alcocer) se encontraba en una playa, en compañía de unos amigos y entregó su cámara fotográfica a uno de ellos con el fin de que realizara unas instantáneas del mismo junto con su pareja, realizándose dichas imágenes en las que los protagonistas aparecen tumbados uno al lado del otro en la playa en una de las fotos y en la otra dándose un beso; realizadas las fotografías se devolvió la cámara fotográfica al demandante, que procedió a su revelado posteriormente. Sin que se haya acreditado su procedencia, las fotografías fueron publicadas por la revista Diez Minutos (FJ1). Sin embargo, en esta sentencia, el TS dio la razón a la revista al considerar que: “en primer lugar, el demandante es persona de proyección pública, en su faceta de su trascendencia económica. Es hecho notorio la profusión de noticias e imágenes que sobre él han divulgado los medios de comunicación. Esto lo reconocen las sentencias de instancia, pero añaden un matiz que no puede ser compartido, dice la sentencia de la Audiencia que «cierta notoriedad pública, ésta le viene por su carácter de financiero y hombre de empresa y no por su particular vida privada, que en todo momento ha mantenido al margen de su actividad profesional pública, por lo que si bien no podría ejercitar acciones en defensa de su imagen cuando ésta se refiera a su actividad bancaria o empresarial, sí puede ejercitarlas al referirse a aspectos de su vida íntima, cuando de sus propios actos no se desprende que haya favorecido, divulgado o amparado la publicidad o divulgación de su privacidad». La Sala, en efecto, no acepta esta limitación y entiende que la persona de proyección pública no tiene estas escisiones de su personalidad, en el sentido de que para un ámbito es público y para otro es privado”. El segundo punto habla sobre el interés general que “no se halla en la importancia o

(número de recurso: 30/1994), FJ4; y STS 3424/2000³²¹, de 24 de abril de 2000. Sala de lo Civil (número de recurso: 432/2000), FJ1}, Puede decirse sin matices que la última jurisprudencia de los dos tribunales a propósito del derecho a la intimidad y a la propia imagen de los personajes públicos muestra una divergencia severa en la forma de apreciar cómo la popularidad afecta al alcance de la reserva de estos derechos o a la legitimidad de las intromisiones. Asistimos así a una situación curiosa, donde el Tribunal Constitucional se erige en adalid de los derechos que antes fueran patrimonio de la jurisdicción civil y con una proyección de contenido patrimonial innegable, frente a un Tribunal Supremo más restrictivo con el alcance de estos derechos en el caso de los personajes públicos y en defensa de una interpretación pro libertad de información del art. 20.1 .d) CE³²².

trascendencia del reportaje, sino en que se trata de unos actos privados en que la persona, por los usos sociales y por el ámbito que mantiene reservado (artículo 2.1 de la Ley de 5 de mayo de 1982), le ha convertido en punto de atención de los medios de comunicación, y lo son, no sólo por el interés en los detalles de la vida de los demás, sino por constituir en casos semejantes, muy semejantes, motivo para importantes cambios financieros”. Y por último, la playa es, como reconoce el TS, “indudablemente, un lugar abierto al público, no sólo por ley sino por la realidad. Esta Sala no comparte la consideración que hace la sentencia de instancia de que dentro de una playa no haya lugares apartados que permitan la intimidad, con lo cual confunde la intimidad con imagen y su exclusión de la intromisión, según el artículo 8.2.a) y tampoco declara probado esta situación aislada o recóndita de un lugar de la playa, sino que lo deduce de que no se ven otras personas en la fotografía (en el caso de la sentencia de 29 de marzo de 1988 sí se estimó probado el lugar de la playa poco concurrido y alejado de los núcleos de población)” (FJ5).

³²¹ Lydia Bosch asistió a la boda de su hermana, en la que se tomaron una serie de fotografías realizadas por un estudio contratado, en las que posaban tanto Lydia como su hermana en el domicilio de los padres como en la iglesia donde se contrajo el matrimonio. La intromisión ilegítima en el derecho a propia imagen debe ser estimada, ya que la obtención de las fotografías fue voluntariamente no ya aceptado sino encargado al estudio fotográfico; pero no hubo consentimiento expreso para su publicación en una revista, ni de ningún modo puede deducirse del hecho de tratarse de una boda con asistencia de invitados. Ciertamente, Lydia Bosch es persona de proyección pública, pero no así su hermana que ni siquiera se ha planteado que lo fuera. También es cierto que una iglesia, lugar de culto, es lugar abierto al público, pero el domicilio de los padres de las demandantes en ningún caso puede tenerse como lugar público. Así, la revista publicó unas fotografías en que, por lo menos alguna o algunas de ellas, aparece personas privadas carentes de proyección pública y en un lugar (un domicilio privado) que no es abierto al público (FJ1 y FJ2).

³²² DE LA IGLESIA CHAMARRO, A. (2003). El derecho a la propia imagen de los personajes públicos. *Revista Española de Derecho Constitucional* nº67, pág. 287.

El TC, en la sentencia 292/2000, de 30 de noviembre, tuvo ocasión de abordar la función del derecho fundamental de la intimidad, cuya finalidad es “la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. En fin, el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, por esta razón, y así lo ha dicho este Tribunal (SSTC 134/1999, de 15 de julio, FJ 5; 144/1999, FJ 8; 98/2000, de 10 de abril, FJ 5; 115/2000, de 10 de mayo, FJ 4), es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebida de dicha información. Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin” (FJ6).

Por su parte, Carbonell considera que la intimidad protegida es “todo conocimiento reservado, que el sujeto no conozca, o no esté seguro de conocer, y que el sujeto pasivo no quiera que se conozca”³²³. Además, también existe un supuesto agravado³²⁴ para los casos en que el acceso a dichas comunicaciones afecte a “datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual”, de lo que resultaría sencillo concluir que no puede restringirse el ámbito típico del artículo 197.1 del Código Penal, que comprende: “el apoderamiento de papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales; la interceptación de telecomunicaciones; o la utilización de artificios de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación; con la finalidad de descubrir los secretos o vulnerar la intimidad de otro”. Por tanto, lo que se protege, más que la intimidad personal, es el derecho

³²³ CARBONELL MATEU, J. C. y GONZÁLEZ CUSSAC, J. L. (1999). *Derecho penal. Parte especial*. Tirant lo Blanch. Valencia, pág. 287.

³²⁴ CP. Artículo 197.5.

fundamental a la inviolabilidad de las comunicaciones como parte del derecho a la intimidad del individuo, pero eso no evita que la idea de secreto de dicho artículo vaya asociada al de intimidad.

Sin embargo, este punto de vista no parece ser defendido en las resoluciones del TS, señalando que “el contenido debe ir referido a aspectos propios de la intimidad personal y no a informaciones de carácter trivial”³²⁵ {STS 1105/1999, de 18 de febrero. Sala de lo Penal (nº de recurso: 3256/1998)}. Por lo tanto, la acción del autor estará encaminada a conocer la información reservada de otro sin su consentimiento, invadiendo el ámbito de su intimidad personal. Al respecto, la STS 7601/2000, de 23 de octubre. Sala de lo Penal (nº de recurso: 465/1999), reconoce que para la comisión del delito del artículo 197 CP “queda fuera del ámbito de la presunción de inocencia los propósitos, las intenciones, los saberes o la voluntad de la persona por ser todos ellos elementos propios del ámbito interno del sujeto, y no hechos en sentido estricto susceptibles de ser aprehendidos por los sentidos; con independencia de ello, decimos, la conducta desarrollada por la acusada al utilizar la carta en la forma antes referida, pone de manifiesto de manera palmaria no sólo el dolo genérico de saber lo que se hace y la voluntad de hacerlo, sino también el dolo específico requerido por esta figura delictiva, caracterizado por el ánimo tendencial de invadir la esfera de privacidad e intimidad que representa la correspondencia privada de las personas que, en el caso presente tratándose de un matrimonio separado y con malas relaciones al punto de no dirigirse la palabra, no puede ser puesto en duda a la vista de la actividad de la acusada”³²⁶ (FJ2). Según lo visto, al tener que ser necesaria una acción voluntaria del sujeto para obtener los datos, quedan excluidos de delito aquellos casos de lecturas ocasionales producidas

³²⁵ En el FJ2 se añade que “no es fácil, a priori y en abstracto, determinar cuando el desvelamiento de un dato personal o familiar produce ese perjuicio. Baste decir que lo produce siempre que se trata de un dato que se considera sensible por ser inherente al ámbito de su intimidad más estricta. Dicho de otro modo, un dato perteneciente al reducto de los que se pretenden que no trasciendan fuera de la esfera en que se desenvuelve la privacidad de las personas y su núcleo familiar”.

³²⁶ En los mismos términos se expresa la STS 4149/2006, de 19 de junio. Sala de lo Penal (nº de recurso: 1392/2005). FJ4: “no cabe afirmar que los acusados hubieran pretendido vulnerar la intimidad del titular y usuario de la cuenta de correo electrónico, pues no era previsible que fuese a manifestarse a través de esa forma de comunicación. Por ello, hay que decir que comunicaciones del género de las interferidas en este caso no están destinadas a ser el cauce de contenidos de carácter íntimo, y lo cierto es que no lo fueron aquí, según consta”.

por descuido del titular o casualidad³²⁷. También se excluyen aquellos casos en los que se accede a sitios en que existe información reservada como mero reto personal, sin que sea objeto de interés el contenido de la información. Así lo recoge el Auto del Juzgado de Instrucción núm. 2 de Lorca, 29 de enero de 2002, al decir que “las conductas de *hacking*³²⁸ de mero acceso a los sistemas informáticos con la única finalidad de acceder al password o contraseña, no son actualmente constitutivos de delito, pues carecen del elemento subjetivo del injusto”.

Por otro lado, no hay que olvidar que el artículo 197 se encuentra inserto en el título del artículo primero del capítulo X del Código Penal, concebido para dar protección a los bienes jurídicos fundamentales consagrados en el artículo 18.1 de la CE, entre ellos, la intimidad. Por este motivo, la idea de secreto expresada en dicho artículo resultaría conceptualmente indisociable de la intimidad, al tratarse de un ámbito especial propio, restringido y reservado frente al conocimiento de los demás.

En los casos que exista la protección penal de la intimidad, tendrá ésta preferente aplicación, por ser sin duda la de más fuerte efectividad, si bien la responsabilidad civil derivada del delito se deberá fijar de acuerdo con los criterios que esta establece la Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Por tanto, el Código Penal no agota el derecho a la intimidad, también existe una visión civil de dicho derecho. La protección civil del honor, de la intimidad y de la propia imagen “quedará delimitada por las leyes y por los usos sociales atendiendo al ámbito que, por sus propios actos, mantenga cada persona reservado para sí misma o su familia”. Además, “no se apreciará la existencia de intromisión ilegítima en el ámbito protegido cuando estuviere expresamente autorizada por Ley o cuando el titular del derecho hubiere otorgado al efecto su consentimiento expreso, o, por imperativo del artículo 71 de la Constitución, cuando se trate de opiniones manifestadas por Diputados o Senadores en el ejercicio de sus funciones. Iniciado un proceso civil en aplicación de la presente Ley, no podrá seguirse contra un Diputado o Senador sin la previa autorización del Congreso de los

³²⁷ MATA y MARTÍN, R. (2006). La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías. *Revista Penal* nº18, julio, pág. 225.

³²⁸ Técnicas y procedimientos utilizados por un *hacker*, definido por la Real Academia Española (RAE) como “pirata informático”.

Diputados o del Senado”³²⁹. Por otro lado, dicha ley también establece aquellas situaciones que son consideradas como intromisiones ilegítimas en el ámbito de protección de estos derechos³³⁰.

El TEDH, en aplicación del artículo 8 del CEDH³³¹, en la STEDH, de 24 de junio de 2004, caso *Von Hannover c. Alemania*. Sección 3ª, consideró que los tribunales alemanes no protegieron adecuadamente los derechos de la demandante, en esta caso Carolina de Mónaco, al considerar que las imágenes, que fueron tomadas en diversas escenas de su vida diaria (haciendo deporte, de compras, caminando...), son de un carácter absolutamente privado, por lo que, según señala, “ha de hacerse una distinción entre narrar hechos, incluso controvertidos, que contribuyan a un debate en una

³²⁹ Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Artículo 2.

³³⁰ Ley Orgánica 1/1982, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Artículo 7: “1. El emplazamiento en cualquier lugar de aparatos de escucha, de filmación, de dispositivos ópticos o de cualquier otro medio apto para grabar o reproducir la vida íntima de las personas. 2. La utilización de aparatos de escucha, dispositivos ópticos, o de cualquier otro medio para el conocimiento de la vida íntima de las personas o de manifestaciones o cartas privadas no destinadas a quien haga uso de tales medios, así como su grabación, registro o reproducción. 3. La divulgación de hechos relativos a la vida privada de una persona o familia que afecten a su reputación y buen nombre, así como la revelación o publicación del contenido de cartas, memorias u otros escritos personales de carácter íntimo. 4. La revelación de datos privados de una persona o familia conocidos a través de la actividad profesional u oficial de quien los revela. 5. La captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo 8.2. 6. La utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga. 7. La imputación de hechos o la manifestación de juicios de valor a través de acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación. 8. La utilización del delito por el condenado en sentencia penal firme para conseguir notoriedad pública u obtener provecho económico, o la divulgación de datos falsos sobre los hechos delictivos, cuando ello suponga el menoscabo de la dignidad de las víctimas”.

³³¹ Artículo 8: “1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. “No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho salvo cuando esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de terceros”.

sociedad democrática, y narrar hechos de la vida privada de un individuo que, como en este caso, no ejerce funciones oficiales”.

Por otro lado, el TEDH opina que la publicación de los artículos y fotos de la princesa de Mónaco “tenía como único propósito satisfacer la curiosidad de un cierto tipo de lectores y sin contribuir a ningún debate de interés general, a pesar de que la demandante es una persona pública”. Además, para su publicación hay que tener también en consideración el contexto en que las imágenes fueron tomadas, “sin consentimiento de la demandante”, y con el añadido del “acoso sufrido por la misma” que no puede ser descartado al enjuiciar el caso. En definitiva, el factor decisivo de ponderación entre la protección de la vida privada y la libertad de expresión debe recaer en que lo publicado contribuya a un debate de interés general, lo que no se da en este caso.

En la jurisprudencia del Tribunal Europeo ha primado el reconocimiento del derecho a la intimidad como valor esencial, que debe protegerse aún más si cabe como consecuencia del continuo avance tecnológico y sus repercusiones. En este sentido, uno de los casos más conocidos y en el que se produjo una amenaza contra el derecho a la intimidad fue el caso *Éditions Plon c. Francia*, con la publicación en Internet del libro “*Le grand secret*”³³², sobre la historia médica y política del que fue presidente de la República Francesa, François Mitterrand. El libro estuvo disponible en Internet sólo unos días, después de que a los diez días hubiese una prohibición temporal de distribución y nueve meses después, el *Tribunal de Grande Instance* de París obligó a “indemnizar a la familia por la publicación y mantuvo de forma indefinida la prohibición de su difusión”.

El TEDH consideró en su sentencia que la prohibición de la distribución del libro desde octubre de 1996 fue “incongruente y desproporcionado”³³³, debido a que antes de la

³³² El libro fue escrito por doctor Gubler, médico personal de François Mitterrand, y publicado en enero de 1996, a los diez días de la muerte del ex presidente de la República Francesa.

³³³ Lo considera así, porque ya habían transcurrido nueve meses desde la muerte y el daño a sus familiares ya no era el mismo. En todo caso, señala que “a más tiempo transcurrido, más prevalece el interés general y relevancia de la muerte del presidente sobre los derechos individuales y la confidencialidad médica”.

prohibición, el libro se difundió durante diez días. Además, había sido difundido en Internet, con acceso libre y generando un debate público. Por lo tanto, el TEDH considera que la información que contenía el libro “ya no era confidencial, por lo que la preservación de la confidencialidad médica no era un argumento ya de entidad, ni podía considerarse una necesidad social importante para mantener la prohibición” (STEDH, de 18 de mayo de 2004, caso *Éditions Plon c. Francia*. Sección.2ª).

De este modo, el TEDH no comparte la opinión del tribunal francés, al señalar que “el hecho de que el libro fuera difundido en la red no afecta a la ilegalidad de la información que contiene”. Su difusión, como reconocieron, “sólo fue posible por haber estado una vez a la venta, y porque la mayoría de los servidores de Internet que lo difundieron estaban fuera del ámbito de actuación de las autoridades francesas”. Este argumento juega en contra de las pretensiones de la parte demandante, ya que a la hora de valorar el daño producido por la prohibición de la publicación, no se concede indemnización alguna³³⁴.

5.6. LA PROTECCIÓN DE DATOS COMO LIBERTAD INFORMÁTICA

Las sentencias del TC 290/2000 y 292/2000, de 30 de noviembre, son las primeras en España que se pronuncian en materia de protección de datos en relación con la CE. El TC reconoce que “si el derecho a la autodeterminación informativa es un derecho activo de control sobre el conjunto de informaciones relativas a una persona, cuando el art. 18.4 CE establece que la Ley limitará el uso de la informática para garantizar los derechos del art. 18.1 no puede significar más que el otorgamiento a los ciudadanos de una posibilidad de actuación con el propósito de, por un lado, impedir o prohibir cualquier intromisión ilegítima en su intimidad a través del uso de la informática, y, de otro lado, garantizar el ejercicio de las facultades de conocimiento y acceso a las informaciones incorporadas a una base de datos, o corregir o suprimir los datos, así como disponer sobre su transmisión y divulgación”³³⁵. El derecho a la

Recalca también que una vez “la confidencialidad se había roto, con una respuesta penal y disciplinaria, el paso del tiempo abre la puerta al interés público”.

³³⁴ Esto ocurre porque el *Tribunal de Grande Instance* de París consideró que es “muy relativo el interés por comprar el libro nueve meses después del evento, especialmente estando disponible en Internet”.

³³⁵ STC 290/2000, de 30 de noviembre.

autodeterminación informativa, como señala Quilez Agreda, “se prevé no sólo para garantizar el derecho a la intimidad, al honor o a la propia imagen, ni sólo para los datos de carácter íntimo sino que quiere garantizar el libre y pleno ejercicio de cualquier otro derecho mediante la protección de cualquier dato personal”³³⁶.

El magistrado Jiménez de Parga y Cabrera dictó un voto particular a la STC 290/2000 en la que, aunque comparte el fallo de la sentencia “debió afirmarse de modo explícito, en la argumentación, que nuestro Tribunal reconoce y protege ahora un derecho fundamental, el derecho de libertad informática³³⁷, que no figura en la Tabla del texto de 1978”. Para Jiménez de Parga y Cabrera, “la libertad informática, en cuanto derecho fundamental no recogido expresamente en el texto de 1978, debe tener como eje vertebrador el art. 10.1 CE, ya que es un derecho inherente a la dignidad de la persona. Tal vinculación a la dignidad de la persona proporciona a la libertad informática la debida consistencia constitucional. También son preceptos que facilitan la configuración

³³⁶ QUILEZ AGREDA, E. (2000). *El Derecho a la protección de datos en la jurisprudencia constitucional*. III Jornadas sobre informática y sociedad. Facultad de Derecho Comillas, pág. 188.

³³⁷ La STC 254/1993, de 20 de julio, mencionó por primera vez en la jurisprudencia española la libertad informática como un derecho fundamental. FJ7: “A partir de aquí se plantea el problema de cuál deba ser ese contenido mínimo, provisional, en relación con este derecho o libertad que el ciudadano debe encontrar garantizado, aun en ausencia de desarrollo legislativo del mismo. Un primer elemento, el más «elemental», de ese contenido, es, sin duda, negativo, respondiendo al enunciado literal del derecho: El uso de la informática encuentra un límite en el respeto al honor y la intimidad de las personas y en el pleno ejercicio de sus derechos. Ahora bien, la efectividad de ese derecho puede requerir inexcusablemente de alguna garantía complementaria, y es aquí donde pueden venir en auxilio interpretativo los tratados y convenios internacionales sobre esta materia suscritos por España. Pues, como señala el Ministerio Fiscal, la garantía de la intimidad adopta hoy un contenido positivo en forma de derecho de control sobre los datos relativos a la propia persona. La llamada «libertad informática» es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data). En este sentido, las pautas interpretativas que nacen del Convenio de protección de datos personales de 1981 conducen a una respuesta inequívocamente favorable a las tesis del demandante de amparo. El derecho fundamental a la intimidad puede justificar en determinados casos que un ciudadano se niegue a suministrar a las autoridades determinados datos personales, no se ve la razón por la que no podría justificar igualmente que ese mismo ciudadano se oponga a que esos mismos datos sean conservados una vez satisfecho o desaparecido el legítimo fin que justificó su obtención por parte de la Administración, o a que sean utilizados o difundidos para fines distintos, y aun ilegales o fraudulentos, o incluso a que esos datos personales que tiene derecho a negar a la Administración sean suministrados por terceros no autorizados para ello”.

de la libertad informática los contenidos en los arts. 18.1 (derecho al honor, a la intimidad personal y familiar y a la propia imagen) y 20.1 (libertad de expresión y de información), entre otros, así como los Tratados y Acuerdos internacionales, en cuanto son guías de interpretación constitucional (art. 10.2 CE): fundamentalmente, el Convenio Europeo para la protección de los Derechos Humanos y las Libertades Fundamentales (1950), art. 8; el Convenio del Consejo de Europa para la Protección de las personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (1981), arts. 5, 6, 8 y 9; Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la libre Circulación de estos datos, art. 13”. Lo que no sorprende al magistrado es que en 1978 no se tutelase la libertad informática, ya que “veintidós años atrás la revolución de la técnica en este campo apenas comenzaba y apenas se percibía. No hemos de extrañarnos tampoco por la omisión de esta materia en los Estatutos de Autonomía de las Comunidades españolas. El entorno es ahora distinto del que fue nuestro mundo en 1978. La informática no ofrecía las actuales posibilidades para el quehacer vital, tanto positivas como negativas, con la adecuada protección de la dignidad de la persona. Muy significativo al respecto es que en la recentísima Carta de Derechos Fundamentales de la Unión Europea se haya incluido como una de las primeras libertades (art. 8) la resultante de la protección de datos de carácter personal. En suma, los cimientos constitucionales para levantar sobre ellos el derecho de libertad informática son más amplios que los que proporciona el art. 18.4 CE”³³⁸.

El Reglamento (UE) 2016/679, que se basa en el artículo 16 del TFUE³³⁹, viene a sustituir la Directiva 95/46/CE, debido a que la “rápida evolución tecnológica ha

³³⁸ STC 290/2000, de 30 de noviembre. Voto particular.

³³⁹ TFUE, revisado el 1 de enero de 2013. Artículo 16: “1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 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. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea”.

supuesto nuevos retos para la protección de los datos personales³⁴⁰. Se ha incrementado enormemente la magnitud del intercambio y la recogida de datos. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de desarrollar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. Generar confianza en el entorno en línea es esencial para el desarrollo económico. La falta de confianza hace que los consumidores vacilen a la hora de adquirir productos en línea y adoptar nuevos servicios, con lo que se corre el riesgo de que se ralentice el desarrollo de usos innovadores de las nuevas tecnologías”³⁴¹. Dicho Reglamento también recoge en su artículo 5, los principios relativos a la protección de datos personales³⁴².

El panorama actual excluye “cualquier solución legislativa duradera y válida para regular esta situación, por las características de Internet, que salta fronteras y legislaciones, por lo que se hace imprescindible el consenso internacional para regular este fenómeno. A partir de ese consenso se podrá abordar la regulación jurídica de la

³⁴⁰ Artículo 4.2. Definición de dato personal: “toda información relativa a un interesado”.

³⁴¹ Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. Contexto de la propuesta, pág. 1.

³⁴² Artículo 5: “Los datos personales deberán ser: a) tratados de manera lícita, leal y transparente en relación con el interesado; b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines; c) adecuados, pertinentes y limitados al mínimo necesario en relación a los fines para los que se traten; solo se tratarán si y siempre que estos fines no pudieran alcanzarse mediante el tratamiento de información que no implique datos personales; d) exactos y se mantendrán actualizados; se habrán de adoptar todas las medidas razonables para que se supriman o rectifiquen sin demora los datos personales que sean inexactos con respecto a los fines para los que se tratan; e) conservados en una forma que permita identificar al interesado durante un período no superior al necesario para lo fines para los que se someten a tratamiento; los datos personales podrán ser conservados durante períodos más largos, siempre que se traten exclusivamente para fines de investigación histórica, estadística o científica, con arreglo a las normas y condiciones establecidas en el artículo 83 y si se lleva a cabo una revisión periódica para evaluar la necesidad de seguir conservándolos; f) tratados bajo la responsabilidad del responsable del tratamiento, que, para cada operación de tratamiento, garantizará y demostrará el cumplimiento de las disposiciones del presente Reglamento”.

red”³⁴³. Pero, ni las conferencias anuales de las Autoridades Nacionales de Protección de Datos ni el Comité consultivo del Convenio 108³⁴⁴, como señala Castillo, no han aspirado a convertirse en una autoridad supranacional.

5.7. EL TRATAMIENTO DE LOS DATOS PERSONALES EN LA RED

Es obvio que la inmediatez con la que circulan las informaciones y los datos personales a través de Internet puede intensificar el daño y provocar una vulneración de los derechos fundamentales. Si la información publicada por un medio de comunicación o en una red social no ha sido contrastada y resulta, finalmente, que no es cierta, crea un perjuicio a la persona citada, ya que la difusión que ha podido tener en un principio ya no será la misma que pudiese tener la rectificación si se llegase a realizar. Un ejemplo claro fue el caso de Diego Pastrana³⁴⁵, que fue señalado social y mediáticamente por el asesinato y violación de una niña de 3 años, cuya muerte se comprobó que había sido accidental. A las pocas horas de conocerse la muerte de la menor, su foto, capturada de su red social y sin su consentimiento, fue difundida por todos los medios de comunicación, vulnerando la Ley de Protección de Datos y el derecho a la propia imagen.

Las sentencias y su publicidad es otro problema que afecta a los ciudadanos y que se encuentra estrechamente relacionado con la protección de datos personales. En este sentido, debe precisarse si las resoluciones judiciales son o no fuentes accesibles al

³⁴³ CASTILLO JIMÉNEZ, C. (2001). *Protección del Derecho a la Intimidad y uso de las nuevas tecnologías de la información*, pág. 46; en *Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*. Vol. 1. Universidad de Huelva.

³⁴⁴ El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

³⁴⁵ Presunto agresor sexual, maltratador y asesino de una niña de 3 años, que una vez conocida la autopsia, revelaba que la menor no fue violada y que las heridas que le causaron la muerte se las produjo por la caída desde un columpio. Los hechos ocurrieron en noviembre de 2009 en el municipio tinerfeño de Arona.

público. El artículo 7³⁴⁶ de la Ley Orgánica 15/1999, desarrollado por el Real Decreto 1720/2007, de 21 de diciembre por el que se aprueba el Reglamento de desarrollo de la Ley; indica cuáles son las fuentes accesibles al público, dando a entender, al no aparecer reflejadas, que las resoluciones judiciales no tienen dicha consideración. Pero, por otro lado, hay que tener en cuenta el alcance de la difusión de las sentencias, regulada por la Ley Orgánica 6/1985³⁴⁷, de 1 de julio, del Poder Judicial. El Acuerdo del Pleno del Consejo General del Poder Judicial, de 15 de septiembre de 2005, por el que se aprueba el Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales, dispone que dispone que “en el tratamiento y difusión de las resoluciones judiciales se cumplirá lo dispuesto en la legislación en materia de protección de datos personales y en los artículos 234 y 266 de la LOPJ. Salvo lo dispuesto en los artículos 234 y 266 de la LOPJ, no se facilitarán por los órganos jurisdiccionales copias de las resoluciones judiciales a los fines de difusión pública regulados en el presente artículo, sin perjuicio del derecho a acceder en las condiciones que se establezcan, a la información jurídica de que disponga el Centro de Documentación Judicial del Consejo General del Poder Judicial. Todo ello sin perjuicio de las competencias atribuidas a los Gabinetes de

³⁴⁶ En el artículo 7 se señala que: 1. “A efectos del artículo 3, párrafo j de la Ley Orgánica 15/1999, se entenderá que sólo tendrán el carácter de fuentes accesibles al público: a.) El censo promocional, regulado conforme a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre. b.) Las guías de servicios de comunicaciones electrónicas, en los términos previstos por su normativa específica. c.) Las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección profesional e indicación de su pertenencia al grupo. La dirección profesional podrá incluir los datos del domicilio postal completo, número telefónico, número de fax y dirección electrónica. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional. d.) Los diarios y boletines oficiales. e.) Los medios de comunicación social. 2. En todo caso, para que los supuestos enumerados en el apartado anterior puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación”.

³⁴⁷ En su artículo 266 dice que: 1. “Las sentencias, una vez extendidas y firmadas por el juez o por todos los Magistrados que las hubieren dictado, serán depositadas en la Oficina judicial y se permitirá a cualquier interesado el acceso al texto de las mismas. El acceso al texto de las sentencias, o a determinados extremos de las mismas, podrá quedar restringido cuando el mismo pudiera afectar al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados, cuando proceda, así como, con carácter general, para evitar que las sentencias puedan ser usadas con fines contrarios a las leyes”.

Comunicación del Tribunal Supremo, Audiencia Nacional y Tribunales Superiores de Justicia, previstas en el Reglamento de los Órganos de Gobierno de Tribunales”³⁴⁸. Anteriormente, ya en el Acuerdo del Pleno del Consejo General del Poder Judicial, de 18 de junio de 1997, por el que se modifica el Reglamento número 5/1995, de los aspectos accesorios de las actuaciones judiciales, en su artículo 5.3 bis se señalaba que “en el tratamiento y difusión de las resoluciones judiciales se procurará la supresión de los datos de identificación para asegurar en todo momento la protección del honor e intimidad personal y familiar”.

La CE, como apunta Gómez Loeches, establece que “las actuaciones judiciales serán públicas con las excepciones que prevean las leyes. En la modulación del acceso a las actuaciones judiciales, es capital el papel desempeñado por el Juez o Presidente y por el Secretario Judicial del órgano jurisdiccional, a la hora de resolver y, en su caso, materializar el acceso solicitado. Estos, a la luz del proceso en cuestión, han de considerar circunstancias como: la fase en la que se encuentra, si no ha concluido aún, la legitimación del interés del peticionario, el alcance objetivo de la consulta, o la finalidad del tratamiento, previo a la ponderación de los valores en conflicto, buscando el necesario equilibrio entre el derecho a un proceso público con todas las garantías, la tutela de los derechos fundamentales inherentes a las personas cuyos datos personales constan incorporados a la documentación judicial y otros valores constitucionalmente protegidos, como el derecho, también fundamental, a recibir y comunicar información”³⁴⁹. Este principio de publicidad de las actuaciones judiciales puede abordarse desde el principio derecho a un proceso público proclamado en el artículo 24.2 de la CE³⁵⁰. Además, el artículo 6.2 de la LOPD³⁵¹ recoge aquellas situaciones en

³⁴⁸ Acuerdo del Pleno del Consejo General del Poder Judicial. Artículo 7.

³⁴⁹ GÓMEZ LOECHES, L. (1998). *El acceso a la documentación de las actuaciones judiciales*. VI Jornadas Españolas de Documentación. FESABID.

³⁵⁰ CE. Artículo 24.2: “Todos tienen derecho al Juez ordinario predeterminado por la ley, a la defensa y a la asistencia de letrado, a ser informados de la acusación formulada contra ellos, a un proceso público sin dilaciones indebidas y con todas las garantías, a utilizar los medios de prueba pertinentes para su defensa, a no declarar contra sí mismos, a no confesarse culpables y a la presunción de inocencia. La ley regulará los casos en que, por razón de parentesco o de secreto profesional, no se estará obligado a declarar sobre hechos presuntamente delictivos”.

³⁵¹ LOPD. Artículo 6.2: “no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus

las que no es necesario el consentimiento del ciudadano para el uso de sus datos personales.

Relacionado con todo lo anterior, la Agencia Española de Protección de Datos en su R/01239/2007³⁵² ha determinado que hay que entender que “las sentencias no son públicas ni se publican para su general conocimiento, aunque en virtud del derecho de información existan noticias relacionadas con el denunciante y los hechos” (R/01239/2007, de 24 de abril de 2008. FJ3). Por lo tanto, la difusión de las sentencias no puede utilizarse para llevar a cabo actividades que puedan vulnerar otros derechos fundamentales, como es el derecho a la protección de datos personales.

En otra resolución, la AEPD rechazó las alegaciones del Boletín Oficial del Estado (BOE) y dictó una resolución en la que instaba al BOE a que “adopte las medidas necesarias para evitar la indexación de los datos personales de la reclamante en sus páginas, con objeto de que en el futuro los motores de búsqueda de internet no puedan asociarlas a la reclamante” (R/02568/2010, de 21 de diciembre de 2010). La reclamante había exigido que su nombre y apellidos que aparecían vinculados a un indulto por estafa informática no fuesen accesibles para los buscadores. La opción planteada por la AEPD es que se incluyesen los datos de la demandante en un fichero “robots.txt”,³⁵³

competencias; cuando se refieran a las partes de un contrato o precontrato de una relación laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado”.

³⁵² Un Policía Local denunció a la Consejería de Seguridad Ciudadana de la Ciudad Autónoma de por haber vulnerado la normativa de protección de datos al haber publicado, en el BOEM, una sentencia de la Audiencia Provincial de Málaga, en la que el denunciante fue absuelto de delito de agresión sexual, y se le condenó por uno de abuso sexual con prevalimiento, a la pena de dos años de prisión e inhabilitación para la profesión de Policía, así como a indemnizar a la perjudicada en la suma de tres millones de pesetas, de las que se declaró responsable subsidiaria la ciudad de Melilla, añadiendo después que al denunciante le fue remitida la pena.

³⁵³ “Se trata de un archivo que se encuentra en la raíz de un sitio e indica a qué partes no quieres que accedan los rastreadores de los motores de búsqueda. El archivo utiliza un protocolo con un pequeño conjunto de comandos que se puede utilizar para indicar el acceso al sitio web por sección y por tipos

para que esa información no fuese captada por los motores de búsqueda de internet. El BOE alegó que el fichero “robots.txt” no se actualiza desde el año 2010 y que, por tanto, no procedía a añadir a nadie más allí, reconociendo que es suficiente con eliminar la información de su propio buscador. La AEPD, en la citada resolución entiende que “la adopción del protocolo de la industria denominado «robots.txt» es un método válido para atender las solicitudes de los ciudadanos que han ejercitado su derecho de oposición o supresión ante un Boletín o Diario Oficial, al considerar que existen motivos que justifican la cesación del tratamiento consistente en permitir la indexación de sus datos publicados en una determinada edición”³⁵⁴. Por tanto, la AEPD entiende que la utilización del protocolo “robots.txt” ha de ser considerada como la medida que garantiza con mayor eficacia el ejercicio del derecho de oposición a la indexación de los datos por los responsables de los motores de búsqueda, ya que es respetado por ellos.

Esta resolución sale al paso de un caso puntual y pone de manifiesto ante situaciones continuadas que deberían tener una regulación equiparada en el ordenamiento jurídico español para que en el caso de que un ciudadano quiera preservar su intimidad ante los boletines oficiales, pueda seguir un cauce establecido de antemano que le permita encontrar respuestas similares ya sea en el Boletín Oficial del Estado como en los relativos a las distintas provincias, ya que hay algunas que no admiten la indexación, mientras que otras, como la Comunidad de Madrid, convierte los textos en imágenes para impedir su indexación en los buscadores.

Verónica Alarcón, abogada del gabinete ePrivacidad y que llevó la defensa de la demandante, considera que “ningún ciudadano puede oponerse al mantenimiento en un Boletín Oficial de sus datos de carácter personal siempre que ese tratamiento se encuentre amparado en una Ley que haya ordenado esa publicación. Igualmente tampoco cabe satisfacer su derecho de supresión si el mismo fuese ejercitado, pues ese derecho no alcanza a lo publicado, ya sea en edición impresa o electrónica, al no ser posible la eliminación de los datos por esa obligación de publicidad derivada

específicos de rastreadores web. Para las páginas web, el archivo robots.txt solo debe usarse para controlar el tráfico de rastreo. Normalmente, esto sirve para evitar que el rastreador de Google sobrecargue el servidor o para no rastrear páginas que sean muy parecidas”. Información extraída del soporte de ayuda de Google (<https://support.google.com/webmasters/answer/6062608?hl=es>).

³⁵⁴ De acuerdo con lo previsto en el Capítulo IV del Título III del Reglamento de desarrollo de la LOPD.

normativamente”. Lo que sí podrá ese ciudadano es “oponerse a que sus datos sean tratados previniendo su captación por los motores de búsqueda de internet siempre que tenga un motivo legítimo y fundado en el sentido que prevé la normativa de protección de datos”³⁵⁵.

Relacionado con el artículo 6.2 de la LOPD, se encuentra el procedimiento sancionador PS/00629/2008, instruido por AEPD a la entidad SABERLOTOTO Internet, S.L., tras las denuncias particulares presentadas a diferentes entidades financieras³⁵⁶. Los ficheros de SABERLOTOTO son accesibles para aquellas empresas que tienen un contrato de suministro de información. En este caso como declara la sentencia, se registraron en los ficheros, “los datos de los denunciantes, sin que se hubiese acreditado que contaba con sus consentimientos y sin que concurriera ninguna de las circunstancias previstas en el artículo 6.2 de la LOPD”, citado anteriormente. La empresa lo justificó diciendo que habían sido obtenidos a través del censo electoral. Al respecto, la AEPD explicó que “el censo electoral y el padrón municipal no son una fuente de acceso público, de modo que la utilización y cesión de estos datos provenientes del censo o del padrón municipal no se ajusta a la LOPD”. La AEPD impuso a SABERLOTOTO Internet, S.L., una multa de 60.101,21 € por una infracción del artículo 6.1³⁵⁷ de la LOPD, tipificada como grave en el artículo 44.3.d.)³⁵⁸. Por otro lado, se le impone otra multa de 300.506,05 € por una

³⁵⁵ ALARCÓN SEVILLA, V. (2011). *El BOE deberá seguir utilizando el fichero "robots.txt"*. Legal Today. Disponible en: <http://www.legaltoday.com/blogs/nuevas-tecnologias/blog-privacidad-en-internet/el-boe-debera-seguir-utilizando-el-fichero-robotstxt#>

³⁵⁶ Las denuncias se produjeron por haber utilizado las entidades financieras sus datos de carácter personal para requerirles el pago de una deuda, mediante cartas dirigidas a sus domicilios, sin que les hubiesen facilitado sus datos. Por su parte, las empresas denunciadas realizaron una búsqueda de nuevos datos relativos a sus clientes, obteniéndolos a través del sitio web www.saberlotodo.com, que les permitió la realización de nuevas actuaciones de intento de cobro.

³⁵⁷ En el que se expone que: “El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa”.

³⁵⁸ Se establece que será sanción grave: “Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave”.

infracción del artículo 11.1³⁵⁹ de la LOPD, tipificada como muy grave en el artículo 44.4.b.)³⁶⁰.

El TJUE ha pronunciado dos sentencias, basadas en la interpretación de la Directiva 95/46/CE, y relacionadas con el tratamiento de datos personales a través de páginas de Internet. Las sentencias vinculan el tratamiento de datos personales con la libertad de expresión e información y el derecho a la intimidad; por un lado, se encuentra la sentencia del TJUE C-101/01, de 6 de noviembre de 2003, caso *Lindqvist*³⁶¹. En la sentencia se establece que la referencia a datos personales entre los contenidos de una página web constituye un “tratamiento total o parcialmente automatizado de datos personales”³⁶². La sentencia también concluye que la difusión de datos personales en una página web los hace accesibles a cualquier persona que se conecte a Internet, incluidas aquellas que se encuentren en terceros países, aunque esto no constituye una “transferencia internacional de datos” según el artículo 25³⁶³ de la Directiva 95/46/CE.

³⁵⁹ En este artículo se señala que: “Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado”.

³⁶⁰ Se recoge como sanción muy grave: “La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas”.

³⁶¹ A finales de 1998, la señora *Lindqvist* diseñó varias páginas web con el fin de que los feligreses de la parroquia que se preparaban para la confirmación pudieran obtener fácilmente la información que necesitaban. Las páginas web contenían información sobre dieciocho de sus compañeros de la parroquia, incluido su nombre completo y una descripción de las funciones que desempeñaban, así como sus aficiones. En algunos casos, se mencionaba también la situación familiar, el número de teléfono e información adicional. Además, señaló que uno de sus compañeras se había lesionado un pie y se encontraba en situación de baja temporal por enfermedad. La señora *Lindqvist* no había informado a sus compañeros de la existencia de estas páginas web, ni había solicitado su consentimiento.

³⁶² Artículo 3.1 de la Directiva 95/46/CE, que no está comprendido en ninguna de las excepciones del artículo 3.2, y que, al incluir la información de que una persona se ha lesionado un pie y está en situación de baja parcial, comprende un dato personal relativo a la salud (artículo 8, apartado 1).

³⁶³ En el que se expone que: 1. “Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado. 2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en

No obstante, el TJUE destaca que “corresponde a las autoridades y a los órganos jurisdiccionales de los Estados miembros no sólo interpretar su Derecho nacional de conformidad con la Directiva, sino también procurar que la interpretación de ésta que tomen como base no entre en conflicto con los derechos fundamentales tutelados por el ordenamiento jurídico comunitario o con los otros principios generales del Derecho comunitario como el principio de proporcionalidad” (Punto 87).

El TJUE no dio respuesta a la cuestión de si la protección de datos es una barrera a la libertad de expresión en Internet, aunque afirmó que las disposiciones de la Directiva 95/46/CE “no entrañan, por sí mismas, una restricción contraria al principio general de la libertad de expresión (...) Incumbe a las autoridades y a los órganos jurisdiccionales nacionales garantizar el justo equilibrio entre los derechos e intereses en juego, incluidos los derechos fundamentales tutelados por el ordenamiento jurídico comunitario”³⁶⁴.

La segunda de las sentencias relacionada con el tratamiento de datos personales a través de páginas de Internet es la STJUE C-465/00, de 20 de mayo de 2003, caso

particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países. 3. Los Estados miembros y la Comisión se informarán recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2. 4. Cuando la Comisión compruebe, con arreglo al procedimiento establecido en el apartado 2 del artículo 31, que un tercer país no garantiza un nivel de protección adecuado con arreglo al apartado 2 del presente artículo, los Estado miembros adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate. 5. La Comisión iniciará en el momento oportuno las negociaciones destinadas a remediar la situación que se produzca cuando se compruebe este hecho en aplicación del apartado 4. 6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas”.

³⁶⁴ Punto 90.

*Österreichischer Rundfunk*³⁶⁵. El TJUE tuvo que abordar la compatibilidad de la Directiva 95/46/CE con las leyes vigentes en Austria sobre el acceso a datos personales por parte de las Administraciones Públicas. El TJUE estableció que los artículos 6.1.c), 7.c) y e)³⁶⁶ de la citada Directiva, no se oponen a una normativa nacional “siempre que se demuestre que la amplia divulgación de todos esos datos es necesaria y apropiada para lograr el objetivo de buena gestión de los recursos públicos”. Por ello, el TJUE manifiesta que “las disposiciones de la Directiva, en la medida en que regulan el tratamiento de datos personales que pueden atentar contra las libertades fundamentales y, en particular, contra el derecho a la intimidad, deben ser interpretados a la luz de los derechos fundamentales que, según una reiterada jurisprudencia, forman parte de los principios generales del Derecho cuyo respeto garantiza el Tribunal de Justicia” (Punto 68).

En cuanto a la recogida de datos sobre los ingresos profesionales de una persona para trasladarlos a terceros, el TJUE expresa que está comprendida en el ámbito de aplicación del artículo 8 del CEDH, con base en la jurisprudencia del TEDH, que ha declarado que “ninguna razón de principio permite excluir las actividades profesionales del concepto de vida privada”. La sentencia del caso *Österreichischer Rundfunk* afirma que ciertos artículos de la Directiva 95/46/CE son “directamente aplicables, en el sentido de que un particular puede invocarlos ante los órganos jurisdiccionales nacionales para evitar la aplicación de normas de Derecho interno contrarias a dichas disposiciones” (Punto 101).

³⁶⁵ El TJUE tuvo que pronunciarse sobre las cuestiones prejudiciales planteadas por *Verfassungsgerichtshof* y por el *Oberster Gerichtshof* austriacos, relativas a las obligaciones de las entidades sujetas a control del Tribunal de Cuentas (*Rechnungshof*) de proporcionar a éste, información sobre las retribuciones y pensiones superiores a un nivel determinado que tales entidades abonan a sus empleados y pensionistas, así como el nombre de los beneficiarios, con objeto de elaborar un informe anual para el Parlamento y ponerlo a disposición del público en general.

³⁶⁶ El artículo 6.1.c) señala que: “Los Estados miembros dispondrán que los datos personales sean adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente”. El artículo 7 expone que: “Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: c.) “(...) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento. e.) (...) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos”.

5.7.1. El principio de reconocibilidad de la imagen

Con asiduidad, en las redes sociales se publican imágenes de terceros en su vida diaria sin su consentimiento. Partiremos del principio de reconocibilidad que fue reconocido por el TS al afirmar que “la captación, reproducción o publicación de la imagen de una persona no requiere, de manera esencial e ineludible que la persona aparezca identificable y reconocible con total claridad en cuanto a los rasgos y características que configuran la integridad de su fisonomía, sino, únicamente, en la medida que permita su reconocimiento. Por ello, el hecho de que la misma resulte un tanto borrosa no obsta para que pueda existir intromisión si la reproducción permitió, atendiendo a los hechos acreditados, la perfecta identificación de la persona cuya imagen fue fotografiada” {STS 4851/1998, de 18 de julio. Sala de lo Civil (nº de recurso: 1319/1994). FJ4}. Un principio esencial que determina si existe o no derecho a reclamar el derecho a la propia imagen.

La intromisión ilegítima en el derecho a la propia imagen viene recogida en la Ley Orgánica 1/1982 al afirmar que tendrán la consideración de intromisiones ilegítimas en el ámbito de protección: “la captación, reproducción o publicación por fotografía, filme o cualquier otro procedimiento, de la imagen de una persona en lugares o momentos de su vida privada o fuera de ellos, salvo los casos previstos en el artículo 8.2³⁶⁷ y la utilización del nombre, de la voz o de la imagen de una persona para fines publicitarios, comerciales o de naturaleza análoga”³⁶⁸.

Centrándonos en las imágenes publicadas en las redes sociales de terceros sin su consentimiento, tenemos que diferenciar aquellas que implican situaciones cotidianas de aquellas que pueden resultar dañinas para la persona fotografiada, que, en este caso,

³⁶⁷ Ley Orgánica 1/1982, de 15 de mayo. Artículo 8.2: “El derecho a la propia imagen no impedirá: a) Su captación, reproducción o publicación por cualquier medio, cuando se trate de personas que ejerzan un cargo público o una profesión de notoriedad o proyección pública y la imagen se capte durante un acto público o en lugares abiertos al público. b) La utilización de la caricatura de dichas personas, de acuerdo con el uso social. c) La información gráfica sobre un suceso o acaecimiento público cuando la imagen de una persona determinada aparezca como meramente accesorio.

Las excepciones contempladas en los párrafos a) y b) no serán de aplicación respecto de las autoridades o personas que desempeñen funciones que por su naturaleza necesiten el anonimato de la persona que las ejerza”.

³⁶⁸ Artículos 7.5 y 7.6.

podría vulnerar, además del derecho a la propia imagen, los derechos al honor y a la intimidad. Respecto del primer caso, la AP de Madrid se pronunció al respecto en el auto 11574/2011, de 21 de julio. Sección 11ª (nº de recurso: 129/2011), desestimando el recurso del demandante³⁶⁹ al considerar que “no se ha discutido ni desvirtuado por el apelante el hecho fundamental en el que se asienta el auto dictado: su consentimiento para que las fotografías incluidas en la red, puedan ser utilizadas por los integrantes de la misma, como consta expresamente y así se ha reseñado en la Declaración de Derechos y Responsabilidades de la red social Facebook³⁷⁰. Sentada por tanto esta premisa esencial del sometimiento voluntario del actor a los criterios no sólo contractuales sino a la práctica ordinaria de intercambio de comunicación, información, y contenidos, constituye conducta contraria a los propios actos y proscrita por nuestro ordenamiento –artículo 7 del CC–, negar a ahora a los demandados el uso que se hizo de la propia fotografía «colgada» por el demandante”. En cuanto a la cuestión del carácter injurioso o ánimo de ridiculizar, “tampoco se encuentra fundamento en la solicitud, pues, en primer término, el propio uso social del lenguaje, expresiones, y contenidos de la red, en cuanto a la falta de rigor y seriedad, que incluye aspectos gramaticales y semánticos, entendiéndose por la ausencia de ésta, el tono distendido y crítico que informan las intervenciones y comentarios vertidos, consustancial a la red social. En segundo lugar, del examen de las frases y comentarios incluidos, no se desprende el ánimo invocado de injuriar, ridiculizar, ni menos aún imputar determinadas conductas atinentes a orientación sexual, ya que hacen alusión directa y exclusiva a la tenencia de la foto, lo que es legítimo” (FJ2).

³⁶⁹ El demandante solicitaba el cierre del grupo de Facebook "Salvemos al Padre Abel", alegando que el grupo citado atentaba contra sus derechos al honor, a la propia imagen y a la intimidad, dado que en él se utiliza una foto personal suya, obtenida sin autorización, con ánimo de ridiculizarle e insinuar una determinada orientación sexual. Este propósito de escarnio se encontraría igualmente en la categorización del grupo en los dedicados a "animales y mascotas", así como en los comentarios vertidos en el grupo.

³⁷⁰ En su apartado 2.1, prevé, respecto de los derechos de privacidad y propiedad intelectual, que “la licencia exclusiva y transferible, con posibilidad, incluso, de transmitirse, de todas aquellas imágenes procedentes de vídeos y fotografías publicadas en la red o en conexión con la misma, exentas de cualquier tipo de remuneración o royalties; asimismo, en caso de eliminación por el interesado, quedan al margen los derechos adquiridos por terceros que las hubiesen incorporado a sus propios grupos, y no las hubieran eliminado”.

Para Martínez Otero, la argumentación de la AP es “abusiva” por dos motivos. En primer lugar, “la Audiencia da por sentado que las cláusulas de Facebook habilitan a la red social y a sus usuarios a copiar y utilizar sin permiso imágenes de terceras personas, extremo que no resulta evidente tras una lectura detenida de las cláusulas de Facebook. Además, en el caso de que las cláusulas permitiesen dicha conducta, cabría cuestionarse si no se trataría de una cláusula contraria al ordenamiento jurídico español –según la legislación y jurisprudencia reiterada del TC el derecho a la propia imagen es un derecho indisponible y cabe la revocación del consentimiento– y, por lo tanto, habría de reputarse como cláusula contractual nula”. En segundo lugar, “la Audiencia presume como un uso social comúnmente admitido el acceso a perfiles ajenos, la copia de imágenes de terceros, y la publicación de dichas imágenes en nuevos perfiles o grupos, aun contra la voluntad del interesado. Dicha presunción es errónea, ya que la conducta descrita no ha alcanzado a día de hoy la categoría de uso social, ni es de esperar que lo alcance pronto”³⁷¹.

Por su parte, la AEPD dictó la resolución R/00617/2008, en la que expone que “la grabación y posterior difusión de las imágenes en un portal como *Youtube* sin el consentimiento del afectado vulnera la normativa de protección de datos de carácter personal”. En esta ocasión, la Agencia Española de Protección de Datos entró a investigar de oficio tras la aparición de noticias en los medios de comunicación donde se hacían eco de la aparición de videos en *Youtube*³⁷², grabados por vecinos de la calle Montera (Madrid) donde se ejercía la prostitución. La AEPD deja claro en la resolución que se trata de un tratamiento de datos, como se recoge en el artículo 3.c)³⁷³ de la

³⁷¹ MARTÍNEZ OTERO, J. M. (2016). Derechos fundamentales y publicación de imágenes ajenas en las redes sociales sin consentimiento. *Revista Española de Derecho Constitucional* nº106, págs. 131-132.

³⁷² En el caso analizado, se constató que aparecían publicados en *Youtube* veintidós vídeos con imágenes captadas en la calle. De éstos, en su mayoría aparecen las imágenes de personas distorsionadas, no permitiendo su identificación. Pero en dos de ellos se comprobó que aparecen con nitidez varios transeúntes. Respecto a estas imágenes, que permiten identificar a las personas, deben ser consideradas datos de carácter personal, conforme al artículo 3.a.) de la LOPD, en el que se describen los datos de carácter personal como “cualquier información concerniente a personas físicas identificadas o identificables”; y tales imágenes constituyen, en sí mismas consideradas, un tratamiento de datos en los términos de la LOPD.

³⁷³ En el que se define el tratamiento de datos como: “operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación,

LOPD, y recalca que “aunque la imagen no esté asociada a datos personales del interesado, al ser posible su identificación cruzándolo con terceras bases de datos esas imágenes se pueden considerar como datos de carácter personal”. Por otro lado, como se refleja en la sentencia, “la captación y reproducción de imágenes de los transeúntes en la calle, que constituyen datos de carácter personal, y su publicación en *Youtube*, accesible para cualquier usuario de Internet, se encuentra sometida al consentimiento de sus titulares, de conformidad con lo dispuesto en el artículo 6.1 de la LOPD”. La AEPD sancionó al autor de las imágenes con una multa de 601,01 €, con una disminución de la cuantía al distorsionar la práctica totalidad de las imágenes y la ausencia de beneficios obtenidos.

5.7.1.1. Las imágenes de menores en las redes

La AEPD ha analizado la aplicación de la LOPD en aquellos casos en los que los padres publican fotos de sus hijos menores en blogs o redes sociales. El primer análisis que hay que realizar consiste en determinar si estas imágenes se pueden considerar como datos de carácter personal, definidos de la Ley 15/1999 como “cualquier información concerniente a personas físicas identificadas o identificables”³⁷⁴. Por lo tanto, las imágenes de los menores serán consideradas datos de carácter personal cuando se permita la identificación de los niños que en ellas aparecen, no encontrándose amparadas por la LOPD en caso contrario.

Cuando el tratamiento de las imágenes del menor se efectúa por parte de los propios padres, la ley no sería de aplicación si “los ficheros son mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas”³⁷⁵. La Sentencia de la Audiencia Nacional, de 15 de junio de 2006, intenta aclarar qué se entiende por ámbito personal o doméstico³⁷⁶. Se considerará ámbito personal cuando “los datos tratados afecten a la esfera más íntima de la persona, a sus relaciones familiares y de

bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias”.

³⁷⁴ LOPD. Artículo 3.a).

³⁷⁵ LOPD. Artículo 2.2.a).

³⁷⁶ La sentencia refleja que “Lo relevante para la sujeción al régimen de protección de datos no será por tanto que haya existido tratamiento, sino si dicho tratamiento se ha desarrollado en un ámbito que no sea exclusivamente personal o doméstico”.

amistad y que la finalidad del tratamiento no sea otra que surtir efectos en esos ámbitos”, como se refleja en el artículo 4 del Reglamento de Protección de Datos³⁷⁷. Por lo tanto, la aplicación de la LOPD no tendrá efecto cuando la publicación de la imagen quede limitada al ámbito personal o familiar. Mientras que, por el contrario, dicha norma será aplicable cuando se excede ese ámbito, debiendo solicitarse el consentimiento³⁷⁸ de los padres o de los propios menores cuando estos tengan capacidad para prestarlo, tanto para la obtención de la imagen como para su publicación. Así, la difusión de las imágenes de los menores a través de blogs o redes sociales conlleva que ya no se encuentre dentro del ámbito de la vida familiar, ya que tiene una proyección más allá del ámbito privado.

Por último, la AEPD señalaba que deben extremarse las precauciones en Internet e indicaba que “no es aconsejable publicar fotos que identifiquen a un niño, situándole en el contexto de un colegio o actividad determinados”³⁷⁹. El objetivo es evitar que se ponga en riesgo a un menor mediante la publicación de imágenes que pueden ser utilizadas por terceros “para finalidades no deseadas”.

³⁷⁷ En dicho artículo se expone que “el régimen de protección de los datos de carácter personal que se establece en el presente reglamento no será de aplicación a los siguientes ficheros y tratamientos: a.) A los realizados o mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas. Sólo se considerarán relacionados con actividades personales o domésticas los tratamientos relativos a las actividades que se inscriben en el marco de la vida privada o familiar de los particulares”.

³⁷⁸ El artículo 3.j.) de la LOPD define la cesión de datos como “toda revelación de datos realizada a una persona distinta del interesado”.

³⁷⁹ Informe 0615/2008 de la Agencia Española de Protección de Datos.

CAPÍTULO 6. EL AUGE DE LAS FAKE NEWS Y EL PROBLEMA DE CÓMO ABORDARLAS

6.1. UN CONCEPTO ACTUAL, PERO NO TAN NOVEDOSO

Desde la llegada de Donald Trump al poder no se ha dejado de especular y escuchar la expresión fake news o noticias falsas, por una razón muy sencilla, el triunfo de Trump, como apunta Esteban Illades, sorprendió por “varios motivos, pero el más importante estaba estrechamente relacionado con la información. Todos los medios de comunicación inundaron la conversación pública con contenidos nunca antes vistos y los votantes podían incluso revisar en tiempo real, lo que iban diciendo los candidatos y conocer cualquier cosa de ellos, sin filtro alguno. Pero ahí es donde se torció el asunto. El torrente de información, no era limpio, mucho de lo que ahí circulaba no había sido verificado, pudiendo leerse textos investigados y documentados sobre los millones de dólares defraudados por Donald Trump, así como la enfermedad terminal de Hillary Clinton que la mataría antes de las elecciones”³⁸⁰. Está claro que cuanto más polarizada se encuentra una sociedad, es más vulnerable y más fácil de utilizar sus debilidades para atacarla a través de noticias falsas que reafirmen su ideario.

Tras su victoria, Trump ha conseguido dar un cambio radical al concepto de “fake news”, incluyendo en este grupo cualquier noticia crítica relacionada con él, con su entorno o su gobierno³⁸¹. Por lo tanto, hay que empezar distinguiendo claramente qué es una noticia falsa. La filósofa Regina Rini, las califica como un fenómeno ideado a conciencia e intencionadamente, que tiene por objetivo engañar, al menos, a una parte de su audiencia general que se la crean y la comparten, pero ¿qué lleva a ciertas

³⁸⁰ ILLADES, E. (2018). *Fake news. La nueva realidad*. Grijalbo, págs. 10-14.

³⁸¹ Como explica Faulkner, “supongamos que uno es un partidario de Trump y por eso cree la falsa hipótesis de las noticias ideada por el presidente. Dada esta hipótesis, la verdad de una noticia general sobre Trump es irrelevante para la posición epistémica de un consumidor de noticias. Incluso si la noticia es verdadera, cuando se trata de noticias relacionadas con Trump, la verdad simplemente no importa. Pero en la medida en que la verdad no importa, realmente no hay distinción entre los medios de comunicación tradicionales y los medios de noticias falsos cuando se trata de noticias relacionadas con Trump. Por lo tanto, hay un sentido en el que la hipótesis de las noticias falsas es epistémicamente autosuficiente”. FAULKNER, P. (2018). Fake Barns, Fake News. *Social Epistemology Review and Reply Collective* 7, nº6, págs. 18-19.

personas a creerse estas historias, a menudo ridículas? Pues muy sencillo, “la gente cree las noticias falsas porque las reciben a través de las redes sociales y estas tienen una serie de características que reducen la disposición de la audiencia a pensar críticamente o verificar los hechos. Este efecto se amplifica cuando el editor y la audiencia comparten una orientación partidista. La afiliación partidista compartida alienta a los destinatarios a otorgar más credibilidad a los declarantes de lo que de otro modo estaría garantizado”³⁸².

Más tajante se muestra Gelfert a la hora de definir un fenómeno que “es novedoso en su dimensión sistémica, con unas características inherentes al diseño de las fuentes y canales a través de los cuales proliferan las noticias falsas, ya que cuando se combinan con las redes sociales en línea, permite la manipulación específica de la audiencia, formando una combinación potente y, en algunos casos, políticamente explosiva”. Considerando desde un punto de vista informativa a las fake news como “la presentación deliberada de afirmaciones falsas o engañosas como noticias, donde los contenidos son engañosos intencionadamente”³⁸³.

La elaboración de este tipo de noticias falsas suele sustentarse en motivaciones económicas o políticas. En el primer caso, son operaciones comerciales que buscan generar tráfico a partir de contenidos falsos y, sobre todo, titulares sensacionalistas para que la gente acceda a una información que no tiene relevancia alguna. En cuanto a las motivaciones políticas, las noticias intentan parecer auténticas para manipular el debate público a favor de determinados intereses políticos. El interés político no excluye al económico y un claro ejemplo es que en el caso de la desinformación alrededor de la campaña presidencial de Estados Unidos que alzó como presidente a Donald Trump, se

³⁸² RINI, R. (2017). Fake news and partisan epistemology. *Kennedy Institute of Ethics Journal*, nº 27. Special Issue: Trump and the 2016 election, pág. 44. Como principio de esta relación entre la psicología, la filosofía y las máquinas apareció en la década de los años cincuenta, la tesis de Miller, que, como expone GLEICK, J. (2011). *La información. Historia y realidad*. Editorial Crítica, pág. 265; “se convirtió en una especie de manifiesto, siendo el principio del movimiento llamado revolución cognitiva, que combinaba la psicología, la ciencia de las computadoras y la filosofía. Retrospectivamente, algunos filósofos han llamado a este momento giro informacional”. En este sentido, Frederick Adams apunta que “los que dan el giro informacional ven la información como el ingrediente básico para construir una mente”. ADAMS, F. (2003). The informational turn in philosophy. *Minds and Machines* nº13, pág. 495.

³⁸³ GELFERT, A. (2018). Fake news: a definition. *Informal Logic*. Vol. 38, nº1, págs. 108-113.

unían ambos factores. A pesar de que a los jóvenes macedonios podía resultarles indiferente quién ganara la elección; pero no a los operativos rusos que también influyeron en ella. En este último caso, los beneficios económicos por cuenta del tráfico y la interacción se sumaban a la agenda política subyacente³⁸⁴.

A partir de entonces, en la celebración de cada proceso electoral hay cada vez más evidencias de que tanto los candidatos como los propios partidos políticos están utilizando las redes sociales para difundir desinformación. Aunque pudiese parecer que este método es ya antiguo, porque se buscan llevar a cabo campañas negativas contra los contrincantes, lo que hace que este fenómeno sea único es el uso deliberado de la propaganda computacional para manipular a los votantes y dar forma al resultado de las elecciones. Sin ir más lejos, en las democracias emergentes y occidentales, se utilizan sofisticados análisis de datos y robots políticos para envenenar el entorno de la información, promover el escepticismo y la desconfianza, polarizar a los votantes y socavar la integridad de los procesos democráticos. En regímenes más autoritarios, los partidos gobernantes aplican las mismas estrategias como parte de sus esfuerzos más amplios para subvertir las elecciones³⁸⁵.

Es tal la repercusión que ha alcanzado el fenómeno de las noticias falsas en internet que el Instituto Tecnológico de Massachusetts (MIT) realizó una investigación sobre la difusión diferencial de todas las historias de noticias verificadas, verdaderas y falsas, distribuidas en Twitter de 2006 a 2017. Los datos aportados comprenden, aproximadamente, 126 000 cascadas –patrón de expansión de rumores que exhibe una cadena de retweets ininterrumpida con un origen singular y común de noticias– tuiteadas por cerca de tres millones de personas, más de cuatro millones de veces.

El estudio publicado por la revista *Science* considera básico comprender cómo se propagan las noticias falsa como primer paso para contenerlas y aborda el problema

³⁸⁴ CORTÉS, C. e ISAZA, L. (2017). Noticias falsas en Internet: la estrategia para combatir la desinformación. *Centro de Estudios en Libertad de Expresión y Acceso a la Información*. Universidad de Palermo, págs. 7-8.

³⁸⁵ BRADSHAW, S. y HOWARD, P. (2018). Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation. *Computational Propaganda Research Project*. University of Oxford, págs. 5-7.

tratando de dar respuesta a dos preguntas muy importantes: ¿cómo se diferencian la verdad y la falsedad? y ¿qué factores relacionados con el juicio humano explican estas diferencias? A la hora de verificar los tweets, las investigaciones fueron llevadas a cabo por seis organizaciones independientes de verificación de hechos: snopes.com; politifact.com; factcheck.org; truthorfction.com; urbanlegends.about.com; y hoax-slayer.com.

Los resultados de la investigación fueron sorprendentes, ya que las noticias falsas tenían un 70% más de probabilidad de ser retuiteadas que las verdaderas, sobre todo, en lo referente a noticias sobre política y leyendas urbanas, que se difundieron más rápidamente y fueron las más virales. Una explicación que encuentra su razón de ser en la teoría de la información y la teoría bayesina de la decisión, ya que la novedad capta más la atención de los usuarios y es más valiosa. Por otro lado, las noticias falsas pueden generar una mala asignación de recursos durante los ataques terroristas y desastres naturales. Además, lejos de lo que pudiese parecer, en el estudio, aunque la inclusión de bots aceleró la propagación de noticias tanto verdaderas como falsas, los resultados fueron prácticamente similares, lo que sugiere que, contrariamente a lo que muchos creen, las noticias falsas se difunden con mayor rapidez, más lejos y a más gente, porque los seres humanos, no los robots, tienen más posibilidades de propagarlas. Con lo cual, implica que las políticas de contención de información falsa deben enfatizar las intervenciones conductuales en lugar de centrarse exclusivamente en restringir los robots³⁸⁶. La conclusión a la que podemos llegar es que aunque los bots aceleran las noticias falsas, también lo hacen con las verdaderas en igual proporción, por lo que son los usuarios los que hacen que unas y no otras sean difundidas a mayor velocidad.

6.1.1. Antecedentes

Estados Unidos siempre ha sido un referente en lo que a fake news se refiere. Para comprobarlo, hay que remontarse al 30 de octubre de 1938. Lo que era un simple programa de radio se convirtió en una histeria colectiva, durante la cual millones de personas pensaron que estaban siendo invadidos por un ejército alienígena. El motivo

³⁸⁶ VOSOUGHI, S.; ROY, D.; y ARAL, S. (2018). The spread of true and false news online. *Science*. Vol. 359, pág. 1148.

no era otro que la representación en forma de noticiero de la obra «La Guerra de los Mundos», de H. G. Wells, a cargo de un joven Orson Welles y la compañía teatral Mercury. A pesar de que la CBS señaló de inicio que se trataba de una adaptación, muchos de los oyentes o bien sintonizaron más tarde la emisión o simplemente no le prestaron atención al aviso. De ahí que cuando se produjo el primer corte en el que se anunciaba: “señoras y señores, interrumpimos nuestro programa de baile para traer un boletín especial de Intercontinental Radio News. Veinte minutos antes de las ocho, el profesor Farrell del Observatorio Mount Jennings, Chicago, Illinois, informa haber observado varias explosiones de gas incandescente que ocurren a intervalos regulares en el planeta Marte. El espectroscopio indica que el gas es hidrógeno y se mueve hacia la tierra con una velocidad enorme. El profesor Pierson del Observatorio de Princeton confirma la observación de Farrell y describe el fenómeno como un chorro de llama azul disparado desde un arma. Ahora volvemos a la música de Ramón Raquello, desde el Meridian Room del Plaza Hotel”³⁸⁷.

Durante la retransmisión, los cortes se sucedían con mayor frecuencia y las informaciones cada vez eran más preocupantes, lo que hizo que los cerca de 12 millones de personas que escuchaban la transmisión empezasen a preocuparse, abandonando sus casas y colapsando las carreteras huyendo de los alienígenas. Una alarma social que no concluyó con la emisión del programa, ya que muchas de las personas ya habían desconectado y huido a pesar de que el propio Welles terminó la entrega señalando que “La Guerra de los Mundos no tiene más importancia que la oferta de entretenimiento que pretendía ser. Aniquilamos el mundo ante sus oídos, y destruimos por completo la CBS, pero le aliviará, espero, saber que no lo decimos en serio y que ambas instituciones todavía están abiertas para los negocios. Así que adiós a todos y recuerden la terrible lección que aprendieron esta noche. Ese invasor globular, sonriente y resplandeciente de tu sala de estar es un habitante de la parcela de calabazas, y si suena el timbre de la puerta y no hay nadie, ese no era un marciano...es Halloween”. Esa fue la forma que tuvo Orson Welles de celebrar su particular Halloween, convirtiendo su retransmisión en un hecho insólito y sin precedentes, creando sin saberlo la primera gran fake news de la historia.

³⁸⁷ Extracto de la transcripción de la obra radiada por Orson Welles y la compañía teatral Mercury, el 30 de octubre de 1938, en la emisora Columbia Broadcasting System (CBS).

Comprender hoy en día los ataques vinculados con las noticias falsas, no podría ser posible sin entender las operaciones de inteligencia desarrolladas durante el siglo XX, principalmente durante la Guerra Fría. Una amenaza para las democracias europeas que tiene un denominador común: Rusia. Todos los focos apuntan al país presidido por Vladimir Putin, que lleva años perfeccionando este método de desinformación para crear confusión y sacar provecho de ella. Para ello, hay que remontarse a principios de los años 80 cuando, en plena Guerra Fría, la KGB impulsó la denominada *Operation Infektion*. ¿Cómo hacer creer que Estados Unidos podía haber creado el virus VIH? En la visión del mundo que se tenía en esos momentos, impulsada por la división, era posible suponer que el SIDA podía ser una nueva arma biológica ideada por los Estados Unidos. Ahora solo faltaba que esta información se propagase y eso fue lo que sucedió cuando el 17 de julio de 1983, un periódico local de la India, “The Patriot”, controlado y financiado por el KGB, publicó una carta, supuestamente escrita por un conocido científico y antropólogo estadounidense, en la que se afirmaba que se creía que «el SIDA es el resultado de los experimentos del Pentágono para desarrollar nuevas y peligrosas armas biológicas». Para darle más interés al asunto, en el texto se decía que Estados Unidos estaba a punto de trasladar estos experimentos a Pakistán, donde representarían una grave amenaza para la vecina India.³⁸⁸

³⁸⁸ US DEPARTMENT OF STATE (1987). *Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986-87*, pág. 34. En el texto, en las páginas siguientes (40-42) se indica que para paliar la desinformación sobre el SIDA, el gobierno de los Estados Unidos trató agresivamente de contrarrestar los falsos cargos soviéticos poniendo a disposición de los medios de comunicación y representantes de gobiernos extranjeros tanta información objetiva sobre la campaña soviética y sobre el SIDA como fue posible. Cuando las acusaciones respecto al SIDA aparecieron por primera vez en la prensa soviética, el embajador de Estados Unidos en Moscú, Arthur Hartman, envió cartas de protesta a los editores de Literaturnaya Gazeta y Sovyetskaya Rossiya, pero sus cartas no fueron publicadas ni recibió respuesta. También un número importante de embajadores de todo el mundo escribieron cartas y se reunieron con los editores de los medios que habían publicado dicha desinformación. En muchos casos, los editores indicaron que no tenían la intención de desacreditar a los Estados Unidos; a menudo decían que no sabían que la desinformación se originaba en los medios comunistas, y en ocasiones admitían que las historias de desinformación habían aparecido en sus publicaciones sin que ellos lo supieran, publicándose, posteriormente, rectificaciones y material fáctico que exponía la campaña de desinformación soviética, incluso por parte de algún periódico comunista, como el diario Al Bayane, de Marruecos.

La noticia al haber aparecido en un pequeño diario no tuvo mucha repercusión, pero, como señala Boghardt, hubo tres eventos en 1985 que podrían haber contribuido a la decisión soviética de reactivar la campaña. Por un lado, un informe del gobierno de los Estados Unidos, publicado en febrero de 1985, en el que se afirmaba que los soviéticos habían violado la Convención de Ginebra al producir armas biológicas. En segundo lugar, un artículo en la revista *Executive Intelligence*, en el que se acusaba a la URSS de obstaculizar la batalla contra el SIDA. Y por último, la rápida expansión de la enfermedad dentro del país³⁸⁹.

Con este panorama, el bulo se fue extendiendo y convirtiéndose en una realidad entre la población. Sin ir más lejos, en 1992, como señala Goertzel, en las comunidades afroamericanas y gay existía la creencia de que la epidemia del SIDA fue una conspiración deliberada por parte de funcionarios del gobierno. Unas creencias que se reafirmaban en la encuesta realizada por miembros de la iglesia afroamericana, pertenecientes al Consejo de Liderazgo Cristiano del Sur en la que el 35% creía que el SIDA era una forma de genocidio. Además, el 34% de los encuestados creía que era un virus creado por el hombre, viendo similitudes entre el SIDA y los muchos experimentos de sífilis de Tuskegee realizados entre 1932 y 1972³⁹⁰.

³⁸⁹ BOGHARDT, T. (2009). Soviet Bloc Intelligence and Its AIDS Disinformation Campaign. *Studies in Intelligence*. Vol. 53. N°4, pág. 5.

³⁹⁰ GOERTZEL, T. (1994). Belief in Conspiracy Theories. *Political Psychology* n° 15, pág. 734. Este estudio clínico se desarrolló en Tuskegee (Alabama) entre 1932 y 1972 y fue realizado por el Servicio Público de Salud de los Estados Unidos. Para el estudio se seleccionaron a 400 varones de raza negra infectados con la enfermedad y otros 200 sanos, como grupo de control. Se estudió la evolución de la enfermedad sin tratar a los enfermos y sin informarles de que tenían sífilis, solo se les dijo que tenían la sangre mala, pero a cambio se les ofreció tratamiento médico gratuito, transporte a la clínica, comidas y un seguro de sepelio en caso de fallecimiento. BRANDT, A. M. (1978). Racism and research: The case of the Tuskegee Syphilis study. *The Hastings Center Report* 8(6), págs. 21-29. El estudio se dio a conocer debido al artículo de HELLER, J. (1972). *Syphilis victims in U.S. study went untreated for 40 years*. New York Times. Disponible en línea en: <https://www.nytimes.com/1972/07/26/archives/syphilis-victims-in-us-study-went-untreated-for-40-years-syphilis.html>. En el año 1947, se descubrió la penicilina como tratamiento a la sífilis, pero no se les suministró a los pacientes, lo que hizo que cuando el estudio salió en prensa en 1972 ya habían fallecido 28 pacientes por sífilis, mientras que otros 100 habían muerto por complicaciones médicas relacionadas. Además, 40 parejas de los enfermos resultaron infectadas y 19 niños contrajeron la enfermedad por transmisión durante el embarazo. A raíz de este estudio, Estados Unidos se planteó la necesidad de regular los ensayos clínicos en humanos, creando el Consejo Nacional

6.1.2. Consecuencias de las fake news

Más allá de los problemas que pueden suscitar las fake news como tal, también pueden generar unas consecuencias devastadoras para la sociedad, debido a la credibilidad que se les puede dar. Uno de los ejemplos más evidentes de la creencia en las noticias falsas fue el que tuvo lugar en Washington el 4 de diciembre de 2016. Un hombre de 28 años, Edgar Welch, entró en la pizzería Comet Ping Pong y disparó tres veces al aire. Su objetivo era liberar a los niños que allí dentro estaban secuestrados y explotados sexualmente por una red de pederastia dirigida por Hillary Clinton y otros miembros del Partido Demócrata.

¿Cómo se llegó hasta esa situación? Todo fue consecuencia de un rumor en Twitter a raíz de la investigación llevada a cabo por el FBI por el mal uso de su correo electrónico cuando era Secretaria de Estado. A partir de ese tuit, la fake news empezó a extenderse por diferentes foros de apoyo a Donald Trump. El siguiente paso fue conectar a los demócratas con la pizzería. Eso fue sencillo, ya que en uno de los correos de Podesta, jefe de campaña de Clinton, se hablaba del Comet Ping Pong para celebrar un evento para recaudar fondos para el partido y se conectaron algunas palabras con el lenguaje usado por los pedófilos, dándole un doble sentido³⁹¹.

En ese caso, no hubo víctimas, todo lo contrario de lo que sucedió en México en noviembre de 2018. Dos hombres fueron apaleados y quemados vivos después de que una multitud asaltase la comisaría para sacarles a la calle y les prendiese fuego en público. ¿Su delito? Haber aparcado su vehículo cerca de un colegio, ya que desde hacía días circulaba el siguiente mensaje por Whatsapp: “Por favor, todos estén alerta porque una plaga de secuestradores de niños entró en el país. Al parecer, estos criminales están involucrados en el tráfico de órganos... En los últimos días, desaparecieron niños de 4, 8 y 14 años, y algunos fueron encontrados muertos y con signos de que se les habían

de Investigaciones con Humanos y se redactó el Informe Belmont, elaborado por la comisión nacional para la protección de los sujetos humanos de investigación biomédica y del comportamiento, con la intención de regular los principios éticos para la protección de los sujetos humanos de investigación. Disponible en línea en: https://videocast.nih.gov/pdf/ohrp_appendix_belmont_report_vol_2.pdf.

³⁹¹ AISCH, G., HUANG, J., y KANG, C. (2016). *Dissecting the #PizzaGate Conspiracy Theories*. New York Times. Disponible en línea en:

<https://www.nytimes.com/interactive/2016/12/10/business/media/pizzagate.html>.

extirpado órganos. Sus abdomenes habían sido abiertos y estaban vacíos”. Los vecinos se alarmaron y llamaron a la policía, pero una vez detenidos, decidieron tomarse la justicia por su mano. Al final, ni ellos eran secuestradores, ni se pudo demostrarse que existiesen dichos secuestradores. Todo era una fake news extendida por Whatsapp³⁹².

España no ha sido ajena a estas noticias falsas. El atentado del Estado Islámico en agosto de 2017 en Barcelona sirvió para la difusión descontrolada de este tipo de noticias. Varios medios como RTVE, TV3 o El Español, entre otros, publicaron informaciones sin contrastar en las que decían que un terrorista se había atrincherado en un restaurante cercano a las Ramblas con rehenes. La noticia se fue propaganda por las redes sociales y por los diferentes medios que cubrían el atentado en directo y los Mossos d’Esquadra tuvieron que desmentir la noticia. Pero, ¿por qué sucede esto? Marc Amorós lo explica señalando que “las fake news no tienen escrúpulos y se apoderan del miedo y del terror, quienes las fabrican lo saben y no tiene ningún escrúpulo en afirmar que tienen amigos, primos o conocidos en la Policía o los servicios de emergencia para hacerlas creíbles”. Además, se aprovechan del desconcierto informativo, “los distintos medios de comunicación buscan datos que ayuden a construir un relato de los hechos, por eso es importante que sigan fuentes oficiales y que se exige al periodismo que contraste todas y cada una de las informaciones que difunda”³⁹³.

6.2. LAS ELECCIONES PRESIDENCIALES ESTADOUNIDENSES DE 2016 COMO PUNTO DE PARTIDA

Después de los resultados de las elecciones presidenciales estadounidenses de 2016, surgió una gran preocupación por las noticias falsas que habían inundado las redes sociales en los meses previos y que, visto los resultados, podían haber sido determinantes en la elección del presidente. El problema partía de que usuarios individuales sin ningún tipo de filtro ni posibilidad de verificar los hechos podían compartir las informaciones a través de las redes y llegar a tantos lectores como

³⁹² OLLERO, D. (2018). *Quemados hasta la muerte entre aplausos por un bulo de Whatsapp que les acusaba de robar órganos a niños*. El Mundo. Disponible en línea en:

<https://www.elmundo.es/tecnologia/2018/11/14/5beb0d74ca474132048b45d9.html?cid=SIN12201>

³⁹³ AMORÓS, M. (2018). *Fake news. La verdad de las noticias falsas*. Plataforma editorial, págs. 129-132.

cualquier medio de comunicación. En este sentido, la rápida difusión de información falsa en línea es uno de los principales peligros para la sociedad. Cuando este tipo de noticias están respaldadas por la automatización, ya sea a través de algoritmos de difusión o a través de bots, que promueven el contenido de manera preprogramada, los actores políticos tienen un conjunto poderoso de herramientas para la propaganda computacional. Por eso, los sitios web de fake news publican deliberadamente información engañosa o incorrecta que pretende ser una noticia real con fines políticos, económicos o culturales. Estos sitios a menudo dependen de las redes sociales para atraer tráfico web e impulsar su compromiso. De ahí que tanto las webs de noticias falsas como los bots políticos son herramientas cruciales en los ataques de propaganda digital que apuntan a influir en las conversaciones, desmovilizar a la oposición y generar apoyo falso³⁹⁴.

6.2.1. ¿Hubo o no un consumo masivo de fake news?

Para analizar realmente el alcance y la repercusión de las noticias falsas en la previa de las elecciones, Allcott y Gentzkow, miembros del *National Bureau of Economic Research* de los Estados Unidos, llevaron a cabo un estudio con el fin de discutir la trascendencia de las noticias falsas y su consumo antes de las elecciones. Lo primero que queda claro en el estudio es que el 62% de los adultos estadounidenses recibe noticias a través de las redes sociales, siendo las noticias falsas más populares, las que más se compartieron. Además, muchas de las personas que leían este tipo de noticias

³⁹⁴ HOWARD, P., KOLLANYI, B., BRADSHAW, S., y NEUDERT, L. M. (2018). *Social Media, News and Political Information during the US Election: Was Polarizing Content Concentrated in Swing States?* Project on Computational Propaganda. University of Oxford. Estos mismos autores en el estudio titulado: *Junk News and Bots during the U.S. Election: What Were Michigan Voters Sharing Over Twitter?* (2017) University of Oxford; recopilaron datos sobre las noticias no deseadas generadas mediante hashtags relacionados con la política en el estado de Michigan antes de las elecciones presidenciales de 2016, concluyendo que “los usuarios de las redes sociales compartieron muchos enlaces a noticias e información política, pero las noticias basura, caracterizadas por el extremismo ideológico, la desinformación y la intención de persuadir a los lectores a que respeten u odien a un candidato o una política basada en apelaciones emocionales, fue así, si no más, prevalente que la cantidad de información producida por las organizaciones de noticias profesionales. Esta propaganda computacional no solo superó a las noticias reales en Michigan antes de la elección presidencial, sino que la proporción de contenido de noticias profesionales que se compartió alcanzó su punto más bajo el día anterior a la votación”.

falsas reconocían que las creían. Por último, corroboraron que las noticias falsas fueron ampliamente compartidas y fuertemente inclinadas a favor de Trump³⁹⁵.

Este hecho hizo que muchos analistas sugiriesen que Donald Trump no habría sido elegido presidente si no fuera por la influencia de noticias falsas, pero aunque es cierto que hubo una mayor exposición por parte de los votantes a noticias falsas a favor de Trump, es difícil cuantificar en qué grado afectó a su intención de voto. Como punto de referencia para saber el nivel de efectividad de las fake news, Allcott y Gentzkow se basan en el trabajo de Spenkuch y Toniatti, en el que afirmaban que “exponer a los votantes a un anuncio de campaña televisiva adicional cambia las acciones de voto en aproximadamente 0.02 puntos porcentuales”. Lo que les lleva a la conclusión de que “si un artículo de noticias falsas fuera tan persuasivo como un anuncio de una campaña televisiva, las noticias falsas en nuestra base de datos habrían cambiado las cuotas de voto en una cantidad del orden de centésimas de punto porcentual. Esto es mucho más pequeño que el margen de victoria de Trump en los estados centrales de los que dependía el resultado”³⁹⁶. Eso sí, no se puede saber a ciencia cierta la incidencia que cada noticia haya podido tener en sus lectores. Por eso, puede haber casos en los que una noticia falsa, por su importancia y contenido, haya sido mucho más efectiva. Por ejemplo, el hecho de que el Papa Francisco apoyase a Trump podía haber repercutido en los votantes y considerar su decisión final de voto.

En la campaña electoral de 2016, como apunta Rid, destacan tres tipos diferentes de agentes involuntarios. En primer lugar, se encontraría Wikileaks, creado para anonimizar –expresar un dato relativo a entidades o personas eliminando la referencia de su identidad– las fugas de información. El segundo agente sería Twitter, los bots, así como las cuentas semiautomáticas de spam y trolling, constituyen una parte importante de la base de usuarios activos de esta red social, que podría generar fácilmente estadísticas sobre cuántas cuentas son bots o semiautomáticas para amplificar la

³⁹⁵ ALLCOTT, H. y GENTZKOW, M. (2017). *Social Media and Fake News in the 2016 Election*. NBER Working Paper n°23089. Según los datos recopilados en la investigación realizada por Allcott y Gentzkow, encontraron 115 historias falsas pro-Trump, que fueron compartidas en Facebook un total de 30 millones de veces, mientras que las noticias falsas a favor de Clinton, ascendían a 41 y solo fueron compartidas 7.6 millones de veces.

³⁹⁶ ALLCOTT, Hunt y GENTZKOW, Matthew. *Social Media and Fake... ob. cit.*, pág. 20.

desinformación y las noticias falsas con el fin de rebajar la credibilidad de los oponentes. La conclusión es que no le interesa porque “tiene un incentivo comercial para ocultar estas cifras, ya que, con eso, inflan los números de usuarios activos, convirtiéndose en una plataforma de fácil explotación y alto impacto”. Por último, el tercer grupo involuntario sería el formado por aquellos periodistas que cubrieron las filtraciones políticas sin investigar su procedencia³⁹⁷.

Pero no todos los estudios realizados apuestan por un consumo masivo de noticias falsas durante las elecciones presidenciales, el elaborado por Guess, Nagler y Tucker, en el que se cotejaron las noticias compartidas por más de 1300 usuarios de Facebook durante dicho periodo reveló que tan solo el 8,5% difundieron noticias falsas a través de la red social, siendo las personas mayores de 65 años los que más las compartieron en el 11% de los casos, independientemente de su ideología. En el lado opuesto, están los jóvenes entre 18 y 29 años, que solo las compartieron en el 3% de los casos. Por lo tanto, el estudio llegó a la conclusión de que ninguna otra característica demográfica resultó tan relevante como la edad, siendo las personas mayores de 65 años los más proclives a compartir este tipo de noticias falsas, incluso cuando se analizan otros factores como la educación, ideología o partidismo³⁹⁸.

No han sido pocos los trabajos que se han realizado en los últimos años para abordar el fenómeno de las “fake news”. En el realizado por la Facultad de Derecho de Yale y el instituto Floyd Abrams para la libertad de expresión se llegó a una conclusión general: “el restablecimiento de la confianza en las instituciones básicas de una sociedad

³⁹⁷ RID, T. (2017). *Disinformation. A primer in russian active measures and influence campaigns*. Texto presentado durante el 115º Congreso del Comité de Inteligencia del Senado de los Estados Unidos, celebrado el 30 de marzo. En este sentido, Torres, señala “la predisposición de Wikileaks de publicar cualquier dato perjudicial para el Gobierno americano, sin cuestionar excesivamente su procedencia, lo que llevó a algunos analistas a considerar que la plataforma se había convertido en la perfecta «máquina de blanquear las filtraciones rusas», atribuyendo un halo de credibilidad y relevancia a informaciones obtenidas de manera ilegítima por actores que persiguen objetivos muy distintos a los de la democratización del conocimiento”. TORRES SORIANO, M. (2017). Hackeando la democracia: operaciones de influencia en el ciberespacio. *Revista Instituto Español de Estudios Estratégicos (IEEE)*, junio.

³⁹⁸ GUESS, A., NAGLER, J., y TUCKER, J. (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*. Vol. 5, nº1, enero.

democrática es fundamental para combatir los esfuerzos sistemáticos que se realizan para devaluar la verdad”, reconociendo que para pensar cómo combatir las noticias falsas, se debe pensar ampliamente cómo reforzar el respeto por los hechos y contar con una ciudadanía informada con pensamiento crítico. Por otro lado, no hay duda de que hay un movimiento real que quiere “deslegitimar a las instituciones, socavar el discurso racional y promover el tribalismo al servicio del caos y la consolidación del poder. Mientras tanto, los seres humanos son “susceptibles de noticias falsas que confirman sus deseos y creencias, y si bien eso siempre ha sido cierto, las nuevas tecnologías atienden estos rasgos y crean cámaras de eco que finalmente destruyen el discurso informado del que depende una democracia funcional. Desafortunadamente, no existe una solución rápida, permanente o fácil para los problemas asociados con los diversos tipos de noticias falsas”³⁹⁹.

La afirmación: “¡Son solo noticias falsas!”, como señala Dentith, es un problema, ya que este tipo de afirmaciones en el discurso público se hacen falsamente (el agente está mintiendo), o son el resultado de la indiferencia hacia la verdad (al agente no le importa si la acusación es verdadera o falsa). Etiquetar algo como noticias falsas no significa necesariamente que las personas lo consideren falso. Sin embargo, alegar que algo es una noticia falsa es un problema porque se ha convertido en una estratagema retórica, utilizada principalmente por aquellos que ostentan el poder para crear una controversia. Esta perspectiva puede convertirse en una posición política intolerable, ya que cambia el centro del debate político. Si las posiciones que deben considerarse no controvertidas se presentan como meras diferencias de opinión o como falsas, entonces esta licencia, al menos para algunos, es motivo de debate sobre temas que no lo necesitan.

Otra consecuencia preocupante es que al afirmar que los medios de comunicación pueden estar publicando noticias falsas, ya sea de forma explícita o inconscientemente, además de que puedan perder su credibilidad, lo que se consigue es que se equiparen a los medios sensacionalistas, provocando muchas dudas a los lectores que tomarán por ciertas, noticias que pueden no serlo. Pero lo que no se puede usar es el pretexto de noticias falsas cuando algún medio de comunicación vierta alguna opinión o posición

³⁹⁹ *Fighting Fake*. Workshop report. The Information Society Project at Yale Law School and the Floyd Abrams Institute for Freedom of Expression. Marzo 2017, págs. 3-11.

contraria con la que algún personaje público no esté de acuerdo, intentando desacreditarlas y poniendo en peligro la esencia del periodismo. En este sentido, el espectro de noticias falsas, independientemente de su historia, es preocupante simplemente porque habla de cierta indiferencia o falta de sinceridad entre los agentes en el debate político contemporáneo. Después de todo, afirmar que algo es una noticia falsa es una abrogación del deber de confrontar opiniones, optando por la vía de cuestionarlas, en vez de enfrentarse a ellas⁴⁰⁰.

El peligro de las noticias falsas es que “crean una sociedad que no es capaz de ponerse de acuerdo sobre hechos básicos, lo que impide construir una democracia funcional. La desinformación afecta directamente a los fundamentos de las sociedades democráticas que se construyen sobre la presunción de que sus ciudadanos toman decisiones informadas en el momento de acudir a votar, pero este objetivo puede verse truncado si la información es falsa o engañosa. Solo la información veraz sirve como mecanismo de control democrático y puede gozar, por tanto, de protección jurídica”⁴⁰¹.

6.3. EL PROBLEMA DE LA INMEDIATEZ DE LAS REDES SOCIALES

Internet si por algo se caracteriza es por su instantaneidad, por eso es el elemento perfecto para que las mentiras y rumores se difundan con rapidez y sin ningún tipo de control. Todo tipo de información tiene cabida en la red y el contenido se puede transmitir si ningún tipo de filtros ni verificación de hechos a gran velocidad, pero los medios de comunicación no pueden ceder ante esta celeridad y tienen que ser los periodistas los que analicen la información y vean si es relevante o no y, sobre todo, consultar las fuentes para hacerla noticiable. Lo que es un hecho es que hoy en día la noticia no acaba cuando se publica, sino que sigue activa a través de los comentarios y las redes sociales, que pueden poner de actualidad una noticia de hace años que había pasado inadvertida en su momento, imperando lo llamativo frente a lo importante.

⁴⁰⁰ DENTITH, Matthew (2017). The problem of fake news. *Public Reason* 8 (1-2), págs. 65-79.

⁴⁰¹ PAUNER, C. (2018). Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la red. *Teoría y Realidad Constitucional* n°41. UNED, pág 298.

Por tanto, “la crisis actual de los medios de comunicación no es sólo económica, sino también de credibilidad. Los medios ya no son los únicos capaces de transmitir y generar información, ya que los antiguos receptores son ahora emisores potenciales. Estos nuevos emisores, sin embargo, no están sujetos a las obligaciones epistemológicas y deontológicas que deberían regir a los medios, sino que responden a la ley fundamental de la actual Economía de la Atención: generar relatos que triunfen en la constante lucha por el tiempo y el interés de las audiencias. Los medios, al ver que están perdiendo esta batalla, han rendido su autoridad epistemológica y se han puesto a luchar en una guerra que no es la suya. Porque la identidad y la autoridad de los medios informativos (y de forma aún más acusada en las agencias de noticias) residen en saber discernir qué fuentes son creíbles y qué información merece ser transmitida por el bien de sus lectores o espectadores. Si dejan de hacer este trabajo y sus motivaciones son otras, pierden credibilidad y esta pasa a otros emisores, con otros intereses”⁴⁰². La cuestión está en saber si la credibilidad de los medios de comunicación puede restablecerse o viviremos en una sociedad que, o bien va a cuestionarlo todo, o, por el contrario, va a aceptar toda la información que le llegue, sin importarle la fuente, ya que ya no es sinónimo de garantías.

Por ese motivo, en la actualidad, los medios de comunicación tradicionales se encuentran ante la gran tesitura de cómo actuar, haciendo frente a un fenómeno social para el que no están preparados todavía, porque aunque “han tratado de adaptarse, han obviado su función primordial de instrumento social para promover el diálogo, la tolerancia y el pluralismo. La instantaneidad informativa ha adquirido un rol central en el ejercicio diario del periodista, de manera que la noticia ya no es un producto acabado fruto de una elaboración profesional independiente, sino un proceso público en constante mutación que debe convivir con una multitud de discursos no profesionales difundidos por distintos cauces y plataformas. Los medios de comunicación convencionales se enfrentan al dilema de, o bien seguir la fulminante estela que marcan redes sociales como Twitter, o bien erigirse como filtros y analistas de una actualidad retransmitida al minuto. Y todo ello en permanente retroalimentación con una

⁴⁰² GÓMEZ BACEIREDO, B., MARTÍNEZ RODRÍGUEZ, L., y TORRADO MORALES, S. (2012). *¿Compartimos mentiras? El periodismo, la credibilidad y el “efecto bola de nieve” en Internet*, págs. 86-106; en FERNÁNDEZ TOLEDO, M. P. y FERRERAS RODRÍGUEZ, J. G. (coord.). *Del yo al nosotros. Los discursos y la comunicación en la colectividad digital*. Editorial Académica Española.

ciudadanía más activa que demanda una participación real en los discursos informativos”⁴⁰³. Este fenómeno se ha ido acrecentado con la aparición de otros mecanismos de comunicación como las redes sociales, blogs o páginas web, que producen una mayor oferta de contenidos. El problema, además de tener que distinguir la veracidad de dichos contenidos, es que las noticias que se publican a través de estos nuevos cauces alcanzan gran impacto y viralidad porque cuenta con las redes sociales para difundirse globalmente. Por eso, “con el advenimiento del entorno digital y la necesidad de una información permanentemente actualizada se ha quebrado la precisión que requiere la elaboración de las noticias, una de las condiciones básicas para ofrecer información de calidad y sin errores”⁴⁰⁴.

6.3.1. Un periodismo lento como solución

Para acabar con las dudas que está generando el periodismo actual en lo relativo a la veracidad de sus informaciones, hay autores que abogan por un “periodismo lento” (slow journalism), entendiendo lento para referirse a mucho más que la temporalidad en la producción. La primera persona en usar este término fue Susan Greenberg quien argumentó que “debería haber un mercado creciente para ensayos, reportajes y otros escritos de no ficción que se tome su tiempo para descubrir cosas, notar historias que otros extrañan y comunicarlo todo a los más altos estándares: periodismo lento, con el que acabar con el predominio de nuestra cultura de noticias rápidas”⁴⁰⁵.

El periodismo lento mostraría al lector la procedencia de la información y abogaría por la transparencia, un periodismo a la antigua usanza para acabar con la rapidez de las redes sociales y su incertidumbre. En ese sentido, podríamos indicar que “el periodismo lento evita el sensacionalismo y es ético en el tratamiento de la información y de los sujetos que la conforman. Hasta el momento, estas características no son inusuales en periodismo de larga duración o de calidad. El enfoque lento añadiría que las fuentes fuesen verificables y rastreables por los consumidores mediante métodos de

⁴⁰³ SUÁREZ VILLEGAS, J. C. y CRUZ ÁLVAREZ, J. (2013). *Problemas éticos de la instantaneidad informativa en el entorno digital*. I Congreso Internacional de Comunicación y Sociedad Digital. Logroño, pág. 11.

⁴⁰⁴ PAUNER, Cristina (2018). Noticias falsas y libertad de expresión e información... *ob. cit.*, pág. 299.

⁴⁰⁵ GREENBERG, S. (2007). Why doesn't Britain have a culture of serious non-fiction journalism like the US? *Revista Prospect*, febrero.

transparencia (ya sea vinculando o incluyendo la procedencia de la información y el método en el propio texto). Esto significa que dicho periodismo debe producirse en un espacio independiente o alternativo, probablemente a pequeña escala, donde se puedan ejecutar dichos valores. La periodicidad de su entrega también se ralentiza, lo que aumenta los placeres en la producción y el consumo. Este periodismo no requiere una lista de verificación de características claves para calificar como lento. El término, al igual que el movimiento lento en sí, es más una orientación crítica a los efectos de la velocidad práctica del periodismo actual, y una experimentación con publicaciones más lentas a pequeña escala que abordan esos efectos”⁴⁰⁶.

6.4. LA GRAN AMENAZA DE LAS DEMOCRACIAS ACTUALES

Suponiendo, como hemos apuntado, que las noticias falsas son un problema para las democracias, Balkin propone cómo debería regularse. Para él, la forma menos eficiente es que “los estados persigan a las personas y organizaciones que producen las noticias falsas, ya que la mayoría de estas personas son anónimas o están fuera del país, y muchas de ellas emplean ejércitos de bots”. Sin embargo, la solución gubernamental podría estar “probablemente en una nueva forma de regulación del discurso que aliente a las compañías de medios sociales a desarrollar nuevas formas de gobierno privado, estando dirigidas a identificar y vigilar a los elaboradores de noticias falsas, bloqueando los enlaces y los sitios que contengan este tipo de noticias, u obligarles a que las complementen con material de aclaración y las contraste”⁴⁰⁷.

1.4.1. Los países, obligados a actuar

Algunos países, viendo la repercusión social y los problemas que están ocasionando, han empezado a actuar, tratando de regular este fenómeno a través de leyes. La preocupación es máxima y así lo manifestó Emmanuel Macron al afirmar que “la democracia tiene que ver con elecciones verdaderas y decisiones racionales. La

⁴⁰⁶ LE MASURIER, M. (2015). What is slow journalism? *Journalism Practice*. Vol. 9, págs. 142-143.

⁴⁰⁷ BALKIN, J. (2017). Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *UC Davis Law Review*. Vol. 51, pág. 1151-1209.

corrupción de la información es un intento de corroer el espíritu de nuestras democracias”⁴⁰⁸.

6.4.1.1. Alemania, primera ley europea contra las fake news

En Europa, el primer país en aprobar una ley para tratar de combatir las fake news ha sido Alemania, después del intento fallido de los franceses. Con la Ley Netzdurchsetzungsgesetz, más conocida como NetzDG, que entró en vigor el 1 de enero de 2018, el estado germano obliga a las grandes plataformas como Google, Instagram, Facebook o Twitter a que sean ellas las que las eliminen al contar con la tecnología suficiente como para detectar noticias falsas que se repiten y determinar su origen, matizando que aquellas plataformas que ofrecen contenido periodístico o editorial, cuya responsabilidad recae sobre el propio proveedor de servicios, no serán consideradas como redes sociales por dicha Ley. Además, también estarán exentos de ciertas obligaciones, aquellos proveedores cuya red social tenga menos de dos millones de usuarios registrados en Alemania.

Por otro lado, los proveedores de redes sociales que reciban más de 100 quejas al año sobre contenido ilegal estarán obligados a presentar informes semestrales en alemán sobre el tratamiento que se está haciendo sobre dicho contenido ilegal en sus plataformas y estarán obligados a publicar estos informes en la Gaceta Federal y en su propio sitio web a más tardar un mes después de que haya finalizado el semestre correspondiente. Los informes⁴⁰⁹ publicados en su propio sitio web serán fácilmente reconocibles, de acceso directo y estarán disponibles de forma permanente.

⁴⁰⁸ Comparecencia de Emmanuel Macron, presidente de la República Francesa, en el Congreso de los Estados Unidos. 26 de abril de 2018.

⁴⁰⁹ Los informes han de cubrir los siguientes puntos: **1.** Observaciones generales que resaltan los esfuerzos realizados por el proveedor de la red social para eliminar la actividad punible criminalmente en la plataforma. **2.** Descripción de los mecanismos para presentar quejas sobre contenido ilegal y los criterios aplicados para decidir si eliminar o bloquear el contenido ilegal. **3.** El número de quejas recibidas sobre contenido ilegal en el período del informe, desglosado en función de si las quejas fueron presentadas por los organismos de quejas o por usuarios, y según el motivo de la denuncia. **4.** Organización, recursos de personal, experiencia especializada y lingüística en las unidades responsables de procesar las quejas, así como capacitación y apoyo de las personas responsables de procesar las quejas. **5.** Pertenencia a asociaciones de la industria con una indicación de si estas asociaciones de la industria tienen un servicio de quejas. **6.** Número de quejas respecto de las cuales se consultó a un organismo

Al igual que sucedía con los informes, la Ley germana establece que el “proveedor ha de proporcionar a los usuarios un procedimiento fácilmente reconocible, de acceso directo y disponible de forma permanente para presentar quejas sobre el contenido ilegal, tomando nota inmediatamente de la queja y comprobando si el contenido del que se ha informado en la queja es ilegal y está sujeto a eliminación o si el acceso al contenido debe ser bloqueado”. Para ello, eliminará o bloqueará el acceso a todo el contenido ilegal, dentro de los siete posteriores a recibir la queja, pero ese tiempo puede ser excedido si “la decisión sobre la ilegalidad del contenido depende de la falsedad de una alegación de hecho o es claramente dependiente de otras circunstancias de hecho; en tales casos, la red social puede dar al usuario la oportunidad de responder a la queja antes de que se tome la decisión; o si la red social remite la decisión con respecto a la ilegalidad a una institución autorregulada dentro de los 7 días posteriores a haber recibido la queja y admite aceptar la decisión de esa institución”. Por otro lado, la NetzDG establece que las infracciones pueden ser sancionados con multas de entre 500.000 euros y 50 millones de euros. Las sanciones tienen el carácter de infracciones administrativas por lo que permite que se puedan aplicar a personas jurídicas, en este caso, a los proveedores de las redes sociales.

Esta ley presenta varios aspectos polémicos. El principal, que dicha ley externaliza la justicia, ya que no sería la Justicia quien dictamina qué es la verdad sino que se le otorga ese poder a las empresas para que decidan qué contenidos son legales y cuáles no. En este sentido, el abogado alemán Felix Hilgert, especializado en tecnologías de la información, señalaba que “algunas de las disposiciones del Código Penal que esta ley cubre son tan indefinidas por sí mismas que puede ser muy difícil determinar si el contenido los viola o no. Por ejemplo, hay una provisión contra la glorificación de la

externo para adoptar la decisión. **7.** Número de quejas en el período de notificación que dio lugar a la eliminación o bloqueo del contenido en cuestión, desglosado según si las quejas fueron presentadas por los organismos de quejas o por los usuarios; según el motivo de la queja; y según si el caso correspondió a la sección 3, subsección (2), número (3), letra (a) y, de ser así, si la reclamación se envió al usuario y si el asunto se remitió a una institución autorregulada reconocida de conformidad con la subsección de la sección 3 (2) número (3) letra (b). **8.** El tiempo entre la recepción de las quejas por parte de la red social y la eliminación o el bloqueo del contenido ilegal, desglosado según si las quejas fueron presentadas por los organismos de quejas o por los usuarios; según el motivo de la queja, y en qué periodo: "dentro de 24 horas", "dentro de 48 horas", "dentro de una semana" o "en algún momento posterior". **9.** Medidas para informar a la persona que presentó la queja y al usuario acerca de la decisión sobre la queja.

violencia, pero eso no significa que cualquier contenido violento esté prohibido. A no ser que las personas destinadas en estas unidades de bloqueo sean abogados y estén especializados en el tema, y aun así sería muy complicado, es muy posible que las decisiones que tomen sean equivocadas en muchos casos”⁴¹⁰.

Lógicamente la ley NetzDG tiene detractores que la ven como un mecanismo de censura que coarta la libertad de prensa y la libertad expresión. Por tanto, lo normal es que las personas responsables de decidir sobre dicho contenido deberían tener formación legal en derecho alemán, para garantizar que pueden tomar decisiones efectivas que respetan dicha ley, por lo que, por ejemplo, en los casos de calumnias “ya no sería la Justicia quien dictamine qué es la verdad sino que queda en manos de empresas extranjeras que tienen un enorme poder para decidirlo”⁴¹¹. Pero también se puede dar el caso contrario y es que ante la posibilidad de ser sancionadas, las redes sociales decidan bloquear, ante cualquier mínima duda, contenidos denunciados por los usuarios a pesar de que no constituyan ningún delito.

Es un hecho que la ley alemana asienta las bases para poder acabar con las fake news, sobre todo, en los referente a los plazos fijados para retirar las informaciones aunque, en algunos casos y teniendo en cuenta la rápida difusión en redes sociales, parecen excesivos. El problema es que la ley solo se centra en las redes sociales, sin entrar a valorar otro tipo de empresas del sector que también divulgan informaciones y a las que han excluido, perdiendo así la oportunidad de crear una normativa común y homogénea, equiparable a la creada para las redes sociales.

Por su parte, la Comisión Europea ha publicado el informe *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation* en el que participaron académicos, periodistas, organizaciones de la sociedad civil y representantes de la industria como Google, Twitter y Facebook. En dicho informe recogen que la principal amenaza es la desinformación, no las noticias falsas, definiendo dicha desinformación como

⁴¹⁰ *La polémica ley alemana para las redes sociales: ¿censura o lucha contra el odio?* Revista El Salto nº9. Enero 2018.

⁴¹¹ MONTANO, P. (2018). Fake news y libertad de expresión. *Revista Hacer Empresa*, junio, págs. 88-89. Montevideo.

“información falsa, inexacta o engañosa diseñada, presentada y promocionada para causar daños públicos o con fines intencional. El riesgo de daño incluye amenazas a los valores y procesos políticos democráticos, que pueden dirigirse específicamente a una variedad de sectores, como salud, ciencia, educación, finanzas...”⁴¹². Además, consideran que el término noticias falsas es engañoso, ya que algunos políticos y sus partidarios se lo han apropiado, demostrándose que hay ciudadanos que asocian dicho término con el debate político partidista y el periodismo pobre en general.

Como conclusiones del informe, el Consejo se basa en cinco pilares consistentes en acciones destinadas a “mejorar la transparencia del ecosistema de información digital; promover y agudizar el uso de los medios de comunicación y la alfabetización de la información para contrarrestar la desinformación y ayudar a los usuarios a navegar por nuestro entorno de información digital; desarrollar herramientas para capacitar a los usuarios y periodistas y fomentar un compromiso positivo con las tecnologías de la información en rápida evolución; salvaguardar la diversidad y la sostenibilidad del ecosistema de los medios de comunicación europeos; y calibrar la efectividad de las respuestas a través de la investigación continua sobre el impacto de la desinformación en Europa y un proceso de participación que incluye pasos predefinidos y con plazos combinados con requisitos de monitoreo e informes”.

6.4.1.2. Sudamérica apuesta por regular Internet

Si nos centramos en Sudamérica, desde 2011, se ve un incremento en el desarrollo de normas para tratar de regular Internet, pero no es hasta 2013, cuando comienzan a fraguarse diferentes proyectos de ley enfocados a regular los contenidos en Internet, precedidos de procesos o decisiones judiciales que evidenciaban la existencia de vacíos legales o la dificultad de abordar la nueva realidad digital. A diferencia de lo que sucede en Estados Unidos y en Europa, con la ley alemana NetzDG, muy pocos países han adoptado un régimen de responsabilidad de intermediarios. En ninguno de los cuatro países analizados (Argentina, Ecuador, México y Perú) en el estudio realizado por el Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) existe

⁴¹² EUROPEAN COMMISSION (2018). *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*. Communications Networks, Content and Technology. Marzo, págs. 10-11.

“aún regulación específica en materia de responsabilidad de intermediarios, por lo que es posible encontrar dificultades al momento de determinar la responsabilidad de los distintos tipos de proveedores y plataformas en internet por infracciones y daños. En Argentina, los primeros proyectos datan de mediados del 2000 y a pesar de ello, todavía no existe legislación al respecto. En Ecuador se está debatiendo el proyecto presentado en 2017 pero aún sin claridad en cuanto a su destino⁴¹³. En Perú, por ejemplo, es frecuente encontrar iniciativas legislativas que plantean el agravamiento de penas en caso de que las acciones se realicen en el ámbito de internet. Esto también ocurre en México y Argentina aunque en menor medida, incluso habiendo estándares internacionales que desalientan este tipo de regulaciones”⁴¹⁴.

En Brasil, la Ley Federal 12 965, del 23 de abril 2014, sobre los principios, garantías, derechos y deberes para el uso de Internet fue una de las primeras en aprobarse, teniendo como particularidades, el principio de neutralidad de la red, así como que los proveedores de Internet tienen como obligación transmitir todos los datos desde su origen hasta su destino sin interferencias y en el caso de que existan, deben hacerlo con transparencia y siempre informando a los usuarios afectados. Así se recoge en el artículo 9 en el que se señala que “en el supuesto de discriminación o degradación del tráfico prevista, el responsable mencionado debe: abstenerse de causar daño a los usuarios, en la forma del art. 927 de la Ley 10.406, de 10 de enero de 2002; actuar con proporcionalidad, transparencia e isonomía; informar previamente de modo transparente, claro y suficientemente descriptivo a sus usuarios sobre las prácticas de

⁴¹³ El proyecto de Ley, que fue presentado por el ex Presidente Rafael Correa días antes de terminar su mandato y regula los Actos de Odio y Discriminación en Redes Sociales e Internet a través de diez artículos, está pendiente de aprobación. El documento argumenta que “Internet podría ser utilizada como medio para la realización de actos discriminatorios y la comisión de delitos de odio, así como la difamación. Por lo que tales actos no deben estar exentos de intervención administrativa y penal”. Entre los puntos más significativos, contempla en su artículo 5, la gestión de contenidos ilícitos, obligando a “los proveedores a establecer un procedimiento eficaz para solventar los reclamos de contenido ilegal, teniendo que remover los contenidos manifiestamente ilegales en el plazo de 24 horas desde la recepción del reporte”. Además, “los proveedores de servicios de redes sociales elaborarán un informe trimestral con los reclamos o reportes sobre contenido ilegal que presenten los usuarios” (artículo 3).

⁴¹⁴ DEL CAMPO, A. (2018). La regulación de Internet y su impacto en la libertad de expresión en América Latina. *Centro de Estudios en Libertad de Expresión y Acceso a la Información* (CELE). Universidad de Palermo, marzo, págs. 10-11.

gestión y mitigación de tráfico adoptadas, incluidas las relacionadas con la seguridad de la red; y ofrecer servicios en condiciones comerciales no discriminatorias y abstenerse de practicar conductas anticompetitivas”. Además, en “la provisión de conexión a internet, onerosa o gratuita, así como en la transmisión, conmutación o enrutamiento, es vedado bloquear, monitorear, filtrar o analizar el contenido de los paquetes de datos, respetando lo dispuesto en este artículo”. La ley brasileña en su artículo 15 establece que “el proveedor de Internet constituido en forma de persona jurídica y que ejerza esa actividad de forma organizada, profesionalmente y con fines económicos deberá mantener los respectivos registros de acceso a aplicaciones de Internet, bajo secreto, en ambiente controlado y durante un plazo de seis meses”.

El acceso a Internet es esencial para el ejercicio de la ciudadanía y así lo recoge la Ley Federal 12 965 en su artículo 7, garantizando a los usuarios los siguientes derechos: “I. Inviolabilidad de la intimidad y de la vida privada, su protección e indemnización por el daño material o moral resultante de su violación; II. Inviolabilidad y sigilo del flujo de sus comunicaciones por internet, salvo por orden judicial, en la forma de la ley; III. Inviolabilidad y secreto de sus comunicaciones privadas almacenadas, salvo por orden judicial; IV. No suspensión de la conexión a internet, salvo por débito directamente derivado de su utilización; V. Mantenimiento de la calidad contratada de la conexión a Internet; VI. Informaciones claras y completas contenidas en los contratos de prestación de servicios, con detalle sobre el régimen de protección a los registros de conexión y los registros de acceso a aplicaciones de Internet, así como sobre prácticas de gestión de la red que puedan afectar su calidad; VII. No suministrar a terceros de sus datos personales, incluyendo registros de conexión, y de acceso a aplicaciones de Internet, salvo mediante consentimiento libre, expreso e informado o en las hipótesis previstas por ley; VIII. Informaciones claras y completas sobre recolección, uso, almacenamiento, tratamiento y protección de sus datos personales, que sólo podrán ser utilizados para fines que: a) justifiquen su recolección; b) no estén vedadas por la legislación; y c) estén especificadas en los contratos de servicios o en términos de uso de aplicaciones de Internet; IX. Consentimiento expreso sobre recolección, uso, almacenamiento y tratamiento de datos personales, que deberá ocurrir de forma destacada de las demás cláusulas contractuales; X. Exclusión definitiva de los datos personales que haya proporcionado a determinada aplicación de Internet, a su solicitud, al término de la relación entre las partes, con las excepciones a las hipótesis de guardia obligatoria de

registros previstos en esta Ley. XI. Publicidad y claridad de eventuales políticas de uso de los proveedores de conexión a Internet y de aplicaciones de internet; XII. Accesibilidad, consideradas las características físico-motoras, perceptivas, sensoriales, intelectuales y mentales del usuario, en los términos de la ley; y XIII. Aplicación de las normas de protección y defensa del consumidor en las relaciones de consumo realizadas en Internet”.

En los últimos años han sido varios los países que han tratado de regular el uso y contenido de las redes sociales. Al caso de Ecuador, ya citado anteriormente, hay que sumar el de Honduras, que aprobó en febrero de 2018 la Ley que regula los Actos de Odio y Discriminación en Redes Sociales e Internet, cuyo objetivo viene a ser similar a las ya aprobadas en otros países, con la clara intención de que los proveedores de servicios, plataformas y administradores de sitios web adopten medidas para evaluar y bloquear información y contenidos que puedan constituir actos de discriminación, de odio, injurias, amenazas o incitación a la violencia, realizando “un informe trimestral relacionado a la gestión de los reclamos o reportes sobre contenido ilegal que presenten los usuarios” (artículo 3). Además, el proceso, según se recoge en el artículo 5, deberá garantizar los siguiente preceptos: “Registrar inmediatamente el reclamo o reporte, y examinar si el contenido sujeto a reclamo o reporte de la red social es ilegal, verificado lo cual se deberá eliminar, o inhabilitar su acceso; remover o bloquear el acceso al contenido manifiestamente ilegal, en el plazo de veinticuatro horas contado desde recepción del reclamo o reporte, excepto si la institución estatal apropiada ha acordado un periodo más largo para la eliminación o el bloqueo de los contenidos ilícitos; eliminar o bloquear el acceso a cualquier contenido ilegal dentro de las setenta y dos horas siguientes a la recepción del reclamo o reporte; en caso de supresión del contenido, este será asegurado con fines probatorios, debiendo ponerlos a disponibilidad de las autoridades hondureñas cuando sea requerido; notificar a los usuarios cualquier decisión con inmediatez, la misma que deberá encontrarse apropiadamente motivada; así también, de inmediato remover o bloquear todas las copias del material ilícito que se encuentren en su plataforma; y disponer medidas efectivas para prevenir el re-almacenamiento de contenido ilegal”.

El problema de esta ley es que no establece los parámetros para determinar qué contenidos tienen que ser objeto de bloqueo, por lo que los más críticos, encabezados

por la asociación *Access Now*, señalan que la ley “pone en mano de empresas privadas, a menudo extranjeras, el poder de evaluar qué contenido es ilegal y la obligación de tomar decisiones de censura. Estas son facultades que, en un país democrático, corresponden a los tribunales de justicia. Un procedimiento de este tipo, sin legitimidad legal ni controles democráticos es una restricción desproporcionada e innecesaria de la libertad de expresión; e incumple con estándares mínimos de Derechos Humanos, limitando la crítica al Gobierno e impidiendo que la sociedad exija la transparencia y la lucha contra la corrupción”⁴¹⁵.

Por su parte, la Asamblea Nacional Constituyente venezolana aprobó el 8 de noviembre de 2017 la Ley Constitucional contra el Odio, por la Convivencia Pacífica y la Tolerancia, que tiene por objeto “contribuir a generar las condiciones necesarias para promover y garantizar el reconocimiento de la diversidad, la tolerancia y el respeto recíproco, así como para prevenir y erradicar toda forma de odio, desprecio, hostigamiento, discriminación y violencia, a los fines de asegurar la efectiva vigencia de los derechos humanos, favorecer el desarrollo individual y colectivo de la persona, preservar la paz y la tranquilidad pública y proteger a la Nación”. Dicha Ley habla tanto de la responsabilidad de los medios de comunicación⁴¹⁶ como de las redes sociales para la convivencia pacífica y la tolerancia. En el caso de las redes, en su artículo 14 establece que “la difusión de mensajes a través de las redes sociales y medios electrónicos que promuevan la guerra o inciten al odio nacional, racial, étnico, religioso, político, social, ideológico, de género, orientación sexual, identidad de género,

⁴¹⁵ *Por la no aprobación de la ley que regula los actos de odio y discriminación en Internet de Honduras*. Comunicado elaborado por Access Now el 8 de febrero de 2018 y suscrito por más de medio centenar de organizaciones de derechos humanos y digitales de latinoamericana para retirar este proyecto de ley y abrir un verdadero debate, multiparticipativo para encarar los desafíos que presenta la seguridad en línea. Disponible en línea en: <https://nocomun.org/la-no-aprobacion-la-ley-regula-los-actos-odio-discriminacion-internet-honduras/>.

⁴¹⁶ **Artículo 12.** “Los prestadores de servicio de radio, televisión, por suscripción y medios impresos, públicos, privados y comunitarios, están obligados a difundir mensajes dirigidos promoción de la paz, la tolerancia, la igualdad, el respeto y la diversidad. A tal efecto, el Estado podrá ordenarle a los prestadores de estos servicios la difusión de estos mensajes por un tiempo de treinta minutos semanales. En la difusión de estos mensajes se otorgará prioridad a aquellos producidos por productores nacionales independientes y organizaciones y movimientos sociales del Poder Popular”.

expresión de género y de cualquier otra naturaleza que constituya incitación a la discriminación, la intolerancia o la violencia a través se encuentra prohibida. Las personas jurídicas que administran las redes sociales y medios electrónicos se encuentran obligadas a cumplir estrictamente lo dispuesto en esta disposición y adoptarán las medidas adecuadas para prevenir la difusión de estos mensajes. A tal efecto, deberán retirar inmediatamente de su difusión cualquier propaganda o mensaje que la contravenga”.

La intención de la Ley es crear la Comisión para la Promoción y Garantía de la Convivencia Pacífica, “como espacio interinstitucional encargado de diagnosticar, organizar y formular las directrices de la política pública destinada a promover y garantizar la dignidad humana, el reconocimiento de la diversidad, la tolerancia y el respeto recíproco, así como para prevenir y erradicar toda forma de violencia, odio e intolerancia política, social y de cualquier otro tipo”. Al contrario de lo que sucede con las otras leyes citadas, las sanciones son mucho más restrictivas en este caso y no se limitan solo a multas económicas sino que pueden conllevar hasta penas de prisión. Y así lo establece la ley, que expone que “quien públicamente o mediante cualquier medio apto para su difusión pública fomente, promueva o incite al odio, la discriminación o la violencia contra una persona o conjunto de personas, en razón de su pertenencia real o presunta a determinado grupo social, étnico, religioso, político, de orientación sexual, de identidad de género, de expresión de género o cualquier otro motivo discriminatorio será sancionado con prisión de diez a veinte años, sin perjuicio de la responsabilidad civil y disciplinaria por los daños causados” (artículo 20).

Además, expone que será considerado como “un agravante de todo hecho punible que sea ejecutado o incrementado por motivo de la pertenencia, real o presunta, de la víctima a determinado grupo racial, étnico, religioso o político, así como por motivos de género, orientación sexual, identidad de género, expresión de género o cualquier otro motivo discriminatorio. En estos casos la sanción aplicable será el límite máximo de la pena establecida para el hecho punible correspondiente” (artículo 21). Por último, esta Ley recoge que “en el caso de las redes sociales y medios electrónicos, la difusión de mensajes que constituyan propaganda a favor de la guerra o apología del odio nacional, racial, religioso, político o de cualquier otra naturaleza no es retirada dentro de las seis horas siguientes a su publicación, la persona jurídica responsable de la misma será

sancionada con multa desde cincuenta mil a cien mil unidades tributarias. Así mismo, dará lugar al bloqueo de los portales, sin perjuicio de la responsabilidad penal y civil a que hubiere lugar” (artículo 23).

6.4.1.3. Estados Unidos: las fake news frente a la libertad de expresión

El problema surge de las interpretaciones que se hacen de la Primera Enmienda. En ese sentido Sunstein señala que muchas interpretaciones que se hacen de ella, son débiles porque el documento original es muy ambiguo, reconociendo que “el texto de la Primera Enmienda no es rígido y no es absoluto. La historia confirma la ambigüedad del texto. Muestra que la concepción que tenían de la libertad de expresión era bastante más estrecha que la nuestra, pero no revela una comprensión clara de qué discurso se protegió y cuál no. Por más tentador que sea pretender lo contrario, los casos difíciles de la Primera Enmienda no pueden resolverse de manera plausible simplemente invocando el texto o su historia. Como guía para nuestros dilemas actuales, la insistencia en el texto es básicamente inútil e incluso fraudulenta”⁴¹⁷. Como señala Goldman, “el razonamiento parte de la suposición de que la sociedad pretende obtener la verdad, cuanto más verdad, mejor. La mejor manera para que la sociedad obtenga la verdad es dejar que todos expresen sus puntos de vista a los demás. Cuando el gobierno se mantiene fuera de la escena, y permite que todos expongan y defiendan sus puntos de vista, otros obtendrán un rango más amplio de evidencia y se beneficiarán de ello obteniendo más verdad”⁴¹⁸.

Un concepto muy usado en Estados Unidos y empleado para justificar esta diversidad de opiniones, que sirve para defender de una manera generalizada la libertad de expresión, estrechamente relacionada con la Primera Enmienda, es el del “mercado de ideas”⁴¹⁹. La teoría clásica del mercado asume que la verdad se descubre a través de la

⁴¹⁷ SUNSTEIN, C. (1993). *Democracy and the problema of free speech*. The Free Press. Nueva York, págs. XIV-XV.

⁴¹⁸ GOLDMAN, A. (2018). *Free speech, fake news and democracy*. Rutgers University, pág. 6.

⁴¹⁹ Aunque esta teoría se remonta a los filósofos ingleses John Milton y John Stuart Mill, el Juez Holmes introdujo por primera vez el concepto en la jurisprudencia estadounidense en su disidencia de 1919 en el caso *Abrams v. Unites States*, 250 U.S. 616 (1919), señalando que: "la mejor prueba de la verdad es el poder de pensamiento para ser aceptado en la competencia del mercado". Esta teoría asume que un proceso de debate sólido, si no está inhibido por la interferencia gubernamental, conducirá al

competencia con la falsedad y subraya que cualquier verdad impuesta por la autoridad está plagada del peligro de error. En este sentido, John Stuart Mill argumentó que “la represión puede interferir con la capacidad del mercado para buscar la verdad: primero, si la opinión censurada contiene la verdad, su silenciamiento disminuirá la posibilidad de que descubramos esa verdad; en segundo lugar, si las opiniones en conflicto contienen cada una parte de la verdad, el choque entre ellas es el único método para descubrir la contribución de cada uno hacia la verdad total; por último, incluso si la opinión censurada es totalmente falsa y la opinión confirmada es totalmente cierta, debe permitirse el desafío de la opinión aceptada si las personas deben considerar esa opinión aceptada como algo más que dogma y prejuicio; si no lo hacen, su significado se perderá o se debilitará”⁴²⁰.

6.5. PROPUESTAS PARA COMBATIR LAS FAKE NEWS. EL DERECHO AL OLVIDO COMO LÍMITE A LAS FAKE NEWS

6.5.1. La responsabilidad de las redes sociales

La proliferación de noticias falsas es un hecho y las grandes compañías tecnológicas (Facebook, Google y Twitter) están trabajando para tratar de paliar el problema, aunque no es sencillo, y están adoptando medidas para combatir las noticias falsas y la desinformación que provocan. En este sentido, Pauner señala que estos gigantes de Internet, “sí tienen responsabilidades que derivan de su inmenso poder informativo y no pueden ser considerados estrictamente como compañías tecnológicas neutras, porque cuando un término de búsqueda da resultados diferentes en función del historial de búsquedas, del navegador que se usa o de la ideología y gustos del usuario hay, sin lugar a dudas, una toma de decisión subyacente y la plataforma está tomando partido por un modo concreto de servir las noticias lo que es, en última instancia, una decisión

descubrimiento de la verdad, o al menos a las mejores perspectivas o soluciones para los problemas de la sociedad. Por lo tanto, un mercado de ideas que funcione correctamente, en la perspectiva de Holmes, asegura en última instancia “la evolución adecuada de la sociedad, dondequiera que la evolución pueda conducir”. [Gitlow v. New York, 268 U.S. 652 (1925)] remarcando en dicho caso que si “a largo plazo, las creencias expresadas en la dictadura proletaria están destinadas a ser aceptadas... el único significado de la libertad de expresión es que se les debe dar su oportunidad y tener su camino”.

⁴²⁰ MILL, J. S. (1948). *On liberty and considerations on representative government*. McCallum, págs. 46-47.

informativa... Esta aceptación de responsabilidad no es lo mismo que clasificar a las redes sociales como editores, porque no publican nada pero son parte de lo que se ha denominado como la infraestructura de la libertad de expresión y como tal, tienen responsabilidades cívicas y democráticas. Esta responsabilidad se concreta en un deber de colaboración para impedir la propagación de las de noticias falsas partiendo siempre de un principio de transparencia”⁴²¹.

En una entrevista a principios de 2019, Pandu Nayak, vicepresidente del departamento de Google que se encarga de la herramienta de búsqueda, confesó que “es duro decirlo, pero no creo que se puedan crear algoritmos que identifiquen qué información es falsa y cuál no”⁴²². Como Google ve muy difícil filtrar y eliminar la información falsa de sus resultados de búsqueda, la solución que ha encontrado es “posicionar mejor la información relevante que procede de fuentes autorizadas”. Un mal menor, ya que como señalábamos con anterioridad, el problema del periodismo actual es que esas fuentes autorizadas, es decir los medios de comunicación, muchas veces recogen su información de sitios poco fiables, convirtiéndose ellos mismos en los transmisores de las propias fake news.

Pero esas no son las únicas medidas que pretenden llevar a cabo para enfrentarse a este fenómeno social. Junto con Youtube ha puesto en marcha el programa *Be Internet Citizens*, que ha sido diseñado para enseñar a los adolescentes sobre la alfabetización mediática, el pensamiento crítico y la ciudadanía digital, con el objetivo de alentar a los jóvenes a tener una voz positiva en línea. El programa proporciona una base sólida que les da la confianza necesaria para convertirse en productores de contenido en línea, donde pueden expresar sus identidades, compartir sus historias, generar un impacto social y unir a las comunidades.

En 2016, Google implementó en sus artículos la etiqueta verificación de datos, con la que pretendía marcar artículos que hayan pasado por un proceso de *fact-checking*. Esta etiqueta permite a los usuarios encontrar contenido de este tipo en las noticias

⁴²¹ PAUNER, Cristina. *Noticias falsas y libertad de expresión e información... ob. cit.*, pág. 307.

⁴²² Entrevista a Pandu Nayak realizada el 19 de enero de 2019. Disponible en línea en: <https://www.efe.com/efe/espana/sociedad/nayak-google-no-hay-algoritmo-capaz-de-saber-si-una-informacion-es-falsa/10004-3872032>

importantes. Para determinar si se debe utilizar esta etiqueta, desde Google, inciden en que se debe comprobar si la información cumple los siguientes criterios, que suelen ser característicos de los sitios web de verificación de datos. En primer lugar, las verificaciones y afirmaciones independientes basadas en datos deben identificarse fácilmente en el cuerpo de los artículos de verificación de datos. Los lectores deben poder entender el contenido que se ha verificado y las conclusiones a las que se ha llegado. Por otro lado, los análisis deben basarse en fuentes y métodos identificables y transparentes, además de incluir citas y referencias a las fuentes principales. Además, los títulos de los artículos deben indicar que se está revisando una reclamación, el estado de las conclusiones a las que se ha llegado o, simplemente, que el contenido del artículo consiste en la verificación de hechos⁴²³.

⁴²³ Google Search. *¿Qué significa cada etiqueta?* Disponible en línea en: <https://support.google.com/news/publisher-center/answer/4582731?hl=es>. Además de las políticas generales que se aplican a todo el mercado de datos estructurados, Google señala que también hay que tener en cuenta las siguientes directrices adicionales: “**1.** Las verificaciones de datos aparecen solo en los resultados de búsqueda combinados, salvo cuando están relacionadas con noticias, que pueden aparecer también en la sección de resultados de Noticias. **2.** Las verificaciones de datos sobre noticias deben seguir los criterios de los editores de Google Noticias para las verificaciones de datos. **3.** Es posible que las verificaciones de datos no se muestren en los resultados de la Búsqueda de Google, puesto que su inclusión se determina automáticamente. Estos elementos obtienen puntos en función de la clasificación programática del sitio web, que se realiza con un proceso similar a la clasificación de páginas: si el sitio web tiene una buena clasificación, el elemento de verificación de datos puede mostrarse junto a la página en los resultados de búsqueda. El proceso se realiza automáticamente, de modo que tan solo participaría una persona si algún usuario nos informara de una infracción de los criterios de los editores de Google Noticias para las verificaciones de datos, las directrices generales para datos estructurales o en los casos en los que el editor (sea o no un sitio web de noticias) no cumpliera los estándares de responsabilidad, transparencia, legibilidad o información falsa como se estipula en nuestras directrices generales de Google Noticias. **4.** Una única página puede alojar varios elementos ClaimReview, cada uno para una declaración diferente (como se indica más adelante). **5.** Si varios revisores verifican el mismo dato en una página, puedes añadir un elemento ClaimReview al análisis de cada revisor (como se indica más adelante). **6.** La página en la que se aloja el elemento ClaimReview debe incluir la evaluación y la verificación de datos completa, o al menos un breve resumen. Cada elemento ClaimReview debe alojarse solo en una página de tu sitio web. No repitas una verificación de datos en páginas diferentes, salvo si son versiones distintas de la misma página. Por ejemplo, sí puedes publicar el mismo elemento ClaimReview en la versión para dispositivos móviles y la versión para ordenadores de una misma página”. Disponible en línea en: <https://developers.google.com/search/docs/data-types/factcheck>

Por su parte, Facebook a raíz de la invasión de fake news en 2016, ha empezado a trabajar con diferentes agencias y medios de comunicación (Associated Press, Weekly Standard, Politifact y Snopes, entre otros) con la intención de confiar en los periodistas para marcar las noticias falsas y limitar su difusión, porque una parte importante de la estrategia de la compañía es combatir la información errónea. Esa es su idea inicial, pero la investigación y las pruebas anecdóticas han sugerido en repetidas ocasiones que el trabajo de desacreditación ha tenido problemas para marcar la diferencia, como se expone en un artículo de The Guardian, ya que, aunque ha pasado poco tiempo desde su puesta en marcha, algunos periodistas señalan que la compañía ha ignorado sus preocupaciones y no ha utilizado su experiencia para combatir la desinformación, dejándose llevar por intereses económicos y publicitarios. La pregunta surgida al respecto es “¿Por qué deberíamos confiar en Facebook cuando está haciendo correr los mismos rumores que sus propios verificadores de datos están llamando noticias falsas?”. La respuesta por parte de Brooke Binkowski, ex editora de Snopes, fue tajante: "creo firmemente que están difundiendo noticias falsas en nombre de potencias extranjeras hostiles y gobiernos autoritarios como parte de su modelo de negocios" y remarcó que, “al menos en una ocasión, Facebook presionó a los periodistas para que dieran prioridad a la información errónea que afectaba a los anunciantes de Facebook”⁴²⁴.

Por otro lado, Facebook también ha desarrollado dos proyectos para ayudar y educar a sus usuarios para que puedan tomar decisiones inteligentes sobre las noticias que leen, y tener conversaciones significativas sobre lo que les importa. El primero de ellos es el Facebook Journalism Project que surge de la necesidad de los usuarios de compartir y discutir ideas y noticias, tratando de asegurarse de que existe un entorno de noticias sanas para que el periodismo pueda prosperar. En primer lugar, a través del desarrollo colaborativo de noticias, para lo que realizarán colaboraciones con medios de comunicación y diferentes organizaciones para poder construir juntos las primeras etapas del proceso de desarrollo del producto. Además, dentro de este proyecto quieren apostar por la noticias locales, a las que consideran el punto de partido para un gran periodismo, por eso pretenden impulsarlas y promover los medios independientes. Por

⁴²⁴ LEVIN, S. (2018). “*They don't care*”: Facebook factchecking in disarray as journalists push to cut ties. The Guardian. Disponible en línea en: <https://www.theguardian.com/technology/2018/dec/13/they-dont-care-facebook-fact-checking-in-disarray-as-journalists-push-to-cut-ties>

otro lado, pretenden crear herramientas para periodistas y crear grupos de opinión en los que discutir las mejoras que puede llevar a cabo Facebook para descubrir información en su plataforma⁴²⁵.

El otro proyecto es el News Integrity Initiative, un fondo creado por la Craig Newmark Graduate School of Journalism de Nueva York que apoya los esfuerzos para conectar a periodistas, tecnólogos, instituciones académicas, organizaciones sin fines de lucro y otras organizaciones de todo el mundo para fomentar comunidades comprometidas, combaten la manipulación de los medios y apoyan el discurso cívico inclusivo, constructivo y respetuoso. Una idea idílica con la que aspiran a que las “personas estén armadas con noticias e informaciones precisas e integrales que fortalezcan su sentido de pertenencia y oportunidades en los lugares donde viven y trabajan y que las capaciten para participar en la toma de decisiones de la comunidad”. Sus objetivos son claros: “ayudar a los periodistas a aprender nuevas formas de escuchar, empatizar y reflejar las necesidades y objetivos de las comunidades a las que sirven. Daremos prioridad al trabajo que represente de manera significativa y llegue a diversas comunidades. Además, ayudaremos a las organizaciones de noticias a llevar el periodismo al público donde están, en conversaciones en muchas plataformas. Además, examinaremos nuevas formas de lograr una alfabetización noticiosa, ampliamente definida, e investigaremos las raíces de la confianza y la desconfianza en las noticias, así como la influencia y el impacto de la manipulación y la desinformación en la conversación pública”⁴²⁶.

En cuanto a Twitter quizá haya sido la que menos medidas ha puesto en marcha hasta el momento, debido a que reconocen que es imposible valorar la veracidad de todos los tuits publicados cada día. Por eso, su principal objetivo es reducir la visibilidad de tuits y cuentas mientras se investiga su contenido malicioso y en caso de que se confirme, suspender su actividad.

⁴²⁵ *Facebook Journalism Project*. Disponible en línea en:

<https://www.facebook.com/facebookmedia/blog/introducing-the-facebook-journalism-project>

⁴²⁶ *News Integrity Initiative*. Disponible en línea en: <https://www.journalism.cuny.edu/centers/tow-knight-center-entrepreneurial-journalism/news-integrity-initiative/>

6.5.2. Los algoritmos como solución al problema

Si consideramos las fake news como un virus que se propaga a una gran velocidad, el mejor método para acabar con él es atajarlo de raíz y parece que una opción puede ser a través de algoritmos, ya que, como señala Pablo Rodríguez, “el inmenso caudal de información que llega a los portales agregadores de contenidos y que circula por las redes sociales hace muy difícil que los editores humanos puedan verificar rápidamente una determinada noticia, especialmente cuando se trata de una historia nueva. Por eso, las máquinas pueden aportar rapidez y eficiencia a la tarea de cazar bulos. En concreto, nos pueden superar en el análisis de los atributos cuantificables de la noticia, como la estructura gramática, la elección de palabras, la puntuación y la complejidad del texto, aunque el verdadero desafío para construir un buen detector de fake news no es tanto el diseño del algoritmo, sino encontrar los datos adecuados para alimentarlo y entrenarlo en suficiente cantidad”⁴²⁷.

En el trabajo *Automatic detection of fake news*, los investigadores se centraron en la identificación automática de contenido falso en las noticias en línea. En primer lugar presentan dos nuevos conjuntos de datos que cubren siete dominios diferentes. Uno de los conjuntos de datos se recopila combinando enfoques de anotación manual y de colaboración colectiva, mientras que el segundo se recopila directamente desde la web con la intención de identificar las diferencias lingüísticas, la estructura gramatical, la selección de palabras, la puntuación y la complejidad en el contenido de noticias falsas y legítimas. En segundo lugar, realizaron un conjunto de experimentos de aprendizaje para construir detectores de noticias falsas precisos.

Como conclusiones, en primer lugar, apuntaron que “la lingüística computacional puede ayudar en el proceso de identificar noticias falsas de manera automatizada y muy por encima del nivel de oportunidad. El enfoque impulsado por la lingüística propuesto sugiere que para diferenciar entre contenido falso y genuino vale la pena mirar el nivel léxico, sintáctico y semántico de una noticia en cuestión. El rendimiento del sistema desarrollado es comparable al de los humanos en esta tarea, con una precisión de hasta el 76%. Sin embargo, aunque las características lingüísticas parecen prometedoras,

⁴²⁷ RODRÍGUEZ, Pablo. *Algoritmos a la caza de fake news*. Revista TELOS. Fundación telefónica. 25 de febrero de 2019. Disponible en línea en: <https://telos.fundaciontelefonica.com/la-cofa/algoritmos-a-la-caza-de-fake-news/>.

argumentamos que los esfuerzos futuros en la detección de información errónea no deben limitarse a estas y también deben incluir meta características (por ejemplo, número de enlaces hacia y desde un artículo, comentarios sobre el artículo), y características de diferentes modalidades, como la composición visual de un sitio web. En segundo lugar, demostramos que es posible crear recursos para la tarea de detección de noticias falsas mediante la combinación de enfoques de anotación manuales y de recursos. Nuestro artículo presentó el desarrollo de dos conjuntos de datos utilizando estas estrategias y mostró que exhiben propiedades lingüísticas relacionadas con el contenido engañoso. Además, a diferencia de otros conjuntos de datos de noticias falsas disponibles, nuestro conjunto de datos consta de extractos de noticias reales, en lugar de declaraciones breves que contienen información de noticias falsas”⁴²⁸.

El desafío de construir un detector de noticias falso no depende solo del algoritmo en sí, sino de ser capaces de encontrar los datos correctos con los que poner en práctica ese algoritmo. Por eso, aunque parecen la mejor solución, de momento, no se está realizando una apuesta clara por los sistemas algorítmicos, ya que podemos considerar que pueden conllevar un alto riesgo de error y coartar la libertad de expresión de los usuarios.

⁴²⁸ PÉREZ-ROSAS, V., KLEINBERG, B., LEFEVRE, A., y MIHALCEA, R. (2018). *Automatic detection of fake news*. Actas de la 27ª Conferencia Internacional de Lingüística Computacional. Santa Fe (Nuevo México). Agosto, págs. 3391-3401. El trabajo consistió en la recopilación de 240 noticias legítimas, pertenecientes a seis temas diferentes (deportes, negocios, entretenimiento, política, tecnología y educación) y recogidas de sitios web de noticias relevantes de los Estados Unidos –ABC News, CNN, New York Times, Fox News...–. Para garantizar la veracidad de las noticias, se realizó una verificación manual de los hechos del contenido de las noticias, que incluía la verificación de la fuente de noticias y la información de referencias cruzadas entre varias fuentes. Para generar versiones falsas de las noticias legítimas, hicimos uso de crowdsourcing a través de Amazon Mechanical Turk (AMT), pidiendo a los trabajadores, en la medida de lo posible, que imitaran un estilo periodístico en sus escritos para que pudiéramos obtener noticias con un estilo de escritura homogéneo. Para simplificar la tarea de producción de noticias falsas optaron por trabajar con una versión más corta del artículo de noticias original, dando como resultado 240 extractos de noticias falsas. Se realizó un estudio para evaluar la capacidad humana de detectar noticias falsas en los dos conjuntos de datos desarrollados. Se creó una interfaz de anotación que muestra un anotador, ya sea una noticia falsa o legítima, y les pide que juzguen su credibilidad de acuerdo con sus propias percepciones al leer la noticia.

La startup Fabula AI ha desarrollado un sistema de aprendizaje que puede ayudar a identificar noticias falsas en las plataformas en línea. La compañía ha desarrollado una nueva clase de algoritmos de aprendizaje automático llamados Geometric Deep Learning⁴²⁹, que están compuestos por redes neuronales convolucionales que son capaces de aprender patrones en conjuntos de datos complejos y distribuidos, como las redes sociales. La detección automática de noticias falsas plantea desafíos, ya que las noticias a menudo tienen muchos matices y su interpretación requiere el conocimiento del contexto político o social o del sentido común, del que carecen los algoritmos actuales de procesamiento del lenguaje natural.

La compañía aprovecha el aprendizaje “profundo y geométrico patentado para identificar noticias falsas con un 93% de precisión a las pocas horas de su difusión, allanando el camino para la creación de noticias de riesgo de verdad en el mundo, adoptando un enfoque radicalmente diferente para la detección de noticias falsas algorítmicas. En lugar de considerar el contenido de las noticias, la tecnología analiza la forma en que se difunden las historias en las redes sociales. Las noticias falsas y reales se difunden de manera diferente, lo que hace posible encontrar patrones característicos que los diferencian”. Una de las ventajas clave de su tecnología en comparación con los métodos basados en el contenido es que es agnóstico con respecto al lenguaje de las noticias y mucho más difícil de superar por las técnicas de confrontación, ya que se basa en el comportamiento colectivo de los usuarios de la plataforma social⁴³⁰.

6.5.3. El derecho al olvido: una eficaz respuesta a las fake news

La sentencia del Tribunal Supremo 19/2019, de 11 de enero de 2019, citada anteriormente, ha supuesto un gran paso para que el derecho al olvido se muestre como una eficaz respuesta a las fake news, ya que reconoce que “la persona afectada por una supuesta lesión del derecho al honor, a la intimidad personal y familiar y a la propia imagen está legitimada para fundamentar válidamente una acción de reclamación ante la

⁴²⁹ BRONSTEIN, M., BRUNA, J., LECUN, Y., SZLAM, A., y VANDERGHEYNST, P. (2017). Geometric Deep Learning. Going beyond Euclidean data. *IEEE Signal Processing magazine*, julio, págs. 18-42.

⁴³⁰ MANNION, D. (2019). *Fabula AI announces breakthrough in algorithmic fake news detection*. Disponible en línea en: <https://www.fabula.ai/news-index/2019/2/7/fabula-ai-announces-breakthrough-in-algorithmic-fake-news-detection>

entidad proveedora de los servicios de motor de búsqueda en Internet o ante la Agencia Española de Protección de Datos cuando los resultados del motor de búsqueda ofrezcan datos sustancialmente erróneos o inexactos que supongan una desvalorización de la imagen reputacional que se revele injustificada por contradecir los pronunciamientos formulados en una resolución judicial firme”.

Además, en su fallo, el TS señala que “la ausencia de exactitud de la información facilitada en los enlaces ofrecidos por el buscador de Google y su carácter lesivo para la privacidad, consideración social y profesional del reclamante, determina que, en la ponderación de intereses que la Sala debe efectuar, y a la vista de los hechos expuestos, consideramos, compartiendo en este punto el criterio de la resolución combatida, que debe prevalecer en éste supuesto, el derecho a la protección de datos del reclamante sobre el derecho a la libertad de expresión del buscador de Google, y que el tratamiento de los datos personales del denunciante sin su consentimiento, realizado por el demandante no encuentra amparo en el legítimo ejercicio de la libertad de información, al no tener constancia de su veracidad, por lo que el reclamante ostenta un derecho a que dicha información no se vincule a su nombre a través de los buscadores de Internet”. Por tanto, las fake news han encontrado en el derecho al olvido una eficaz respuesta, ya que la sentencia sienta un precedente y establece que se eliminen de los buscadores aquellos enlaces que estén vinculados con noticias falsas o que contengan datos erróneos o inexactos, aplicándose en estos casos el derecho al olvido. Ante un posible caso de difamación se debe atender, según señala el TC, al interés general de la información, que se debe analizar caso por caso atendiendo al contexto de la noticia, y a la veracidad de la información.

El problema de la veracidad, como expone De Aguinaga, está en que el periodismo “no busca la verdad, porque lo que busca es la noticias, que, evidentemente, no es lo mismo, aunque, por definición la noticia periodística deba ser verdadera, eso sí, con una exigencia atenuada por matices y licencias, porque no hay información veraz y, por ende, información mendaz, sino información verdadera o información falsa... La veracidad o la mendacidad son cualidades del sujeto, del informador; pero no del objeto, en este caso, la noticia. Todos entendemos lo que la Constitución quiere decir y todos sabemos que la expresión información veraz es de uso corriente; pero el error gramatical del artículo 20 ahí está. Al establecer el derecho a la libertad de información,

la Constitución lo refiere al reconocimiento y protección del derecho a comunicar o recibir libremente información veraz por cualquier medio de difusión”⁴³¹.

No hay que olvidar que las fake news pueden atacar contra el derecho al honor, la intimidad y la propia imagen del sujeto. Por eso, ahora es más necesario que nunca que las personas puedan ejercitar su derecho al olvido, ya que su imagen no solo se va a poder ver dañada por noticias de su pasado sino por noticias falsas. De ahí que la protección de la vida privada y la reputación encuentran en el derecho al olvido un instrumento útil y efectivo para limitar el daño que pueden provocar las noticias falsas divulgadas en las redes sociales, ya que, al hecho que conlleva la publicación de una información falsa, se suma la intensificación de su capacidad para difamar al aprovechar la red para propagarse sin ningún límite físico de espacio y tiempo que pudiese minimizar el daño.

⁴³¹ DE AGUINAGA LÓPEZ, E. (1998). ¿Información veraz? *Estudios sobre el mensaje periodístico* nº4, pág. 124. Véase también AZURMENDI ADARRAGA, A. (2005). De la verdad informativa a la “información veraz” de la Constitución Española de 1978. Una reflexión sobre la verdad exigible desde el derecho de la información. *Comunicación y Sociedad*. Vol. XVIII, nº2, págs. 9-48; GALÁN-JUÁREZ, M. (2006). Derecho a transmitir libremente información veraz. *Persona y derecho: Revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos* nº55, págs. 597-617; y MACÍAS CASTILLO, A. (2010). Concepto de información veraz cuando se produce colisión entre el derecho a la información y el derecho al honor. *Actualidad Civil* nº20.

CONCLUSIONES

1. El TJUE y la UE a favor del derecho al olvido

La sentencia del TJUE C-131/12, de 13 de mayo de 2014, caso *Google Spain, S.L. y Google Inc. v. AEPD y Mario Costeja* fue un primer paso para borrar las informaciones obsoletas, pero se quedó en el intento de abordar y dar, por fin, una solución al derecho al olvido y fijar quién es realmente el responsable. La retirada de las informaciones o datos se harán en los motores de búsqueda no en las hemerotecas de la web de origen, sobre todo, si se tratan de medios de comunicación digitales, ya que el derecho al olvido digital no puede suponer una censura retrospectiva de las informaciones correctamente publicadas en su día ni permitir que cada individuo construya un pasado a su medida. Como ya hemos visto, por medios de comunicación no se entienden sólo los medios tradicionales, ya que se ha incluido a Twitter como tal. Eso no quiere decir que se creen procedimientos de control distintos para regular la libertad de expresión en Internet, ya que se pueden hacer extensibles y aplicables las normas y principios de los medios de comunicación tradicionales. Por su parte, la UE formalizó su reconocimiento con la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, en el que, por primera vez, se recoge el concepto de derecho al olvido.

2. La sentencia del TJUE no coarta la libertad de expresión

En nuestra opinión, la sentencia lejos de lo que vienen a pensar muchos autores no coarta la libertad de expresión, ya que el TJUE actúa directamente contra Google no contra el medio de comunicación (La Vanguardia) que es quien publicó la noticia. Por tanto, la sentencia no deja de ser más que un mero instrumento para ocultar los datos, no para borrarlos, ya que lo que se ha conseguido es que introduciendo en Google: Mario Costeja, se haya desvinculado su nombre de las informaciones de su embargo por deuda con la Seguridad Social, pero si se usan otras palabras clave, los artículos seguirán apareciendo en el buscador. Por lo tanto, podemos decir que el derecho al olvido no es más que un control de los datos personales que circulan por la red.

3. El principal responsable de las informaciones publicadas es el editor y no Google

Discrepamos, en parte, de la sentencia al considerar que el principal responsable de las informaciones publicadas es el editor y no sólo Google, como reconoce la STJUE, que fue a quien se le obligó a desindexar los contenidos al tener una responsabilidad subsidiaria por su actividad de almacenaje e indexación. La solución para nosotros estaría en que, a través de las reclamaciones a las agencias de protección de datos, los editores de los medios de comunicación incluyesen los datos de los reclamantes en un fichero “robots.txt”. Además, no creemos que Google tenga el mismo grado de responsabilidad que las páginas web que indexa, ya que podemos considerar al motor de búsqueda como un índice de enlaces, sin tener que ser ellos los que se preocupen de los contenidos que alberguen dichos enlaces. Es mucho más sencillo que cada web restrinja el acceso a aquellos contenidos que considera delicados a que sea Google quien tenga que hacer la labor de evitar que ciertas informaciones aparezcan en su índice de búsqueda.

4. La responsabilidad del tratamiento de datos tiene que ser de la sede central y no de su filial del país del demandante

Otro aspecto a tener en cuenta es si la responsabilidad del tratamiento de datos es sólo de la filial de Google del país del demandante, como señala la sentencia del TJUE, o las medidas para poner en práctica el derecho al olvido han de ser adoptadas también por Google Inc., borrando todos los resultados de búsqueda rastreados en www.google.com. Consideramos que, si de verdad queremos que el derecho al olvido sea efectivo, las decisiones de los Tribunales tienen que ir encaminadas a exigir la adopción de medidas a la sede central de Google como responsable de la gestión del buscador, además de hacerlo sobre sus filiales.

5. El derecho al olvido no es un derecho fundamental

Podemos concluir que el derecho al olvido no es un derecho fundamental sino un derecho instrumental derivado del derecho al honor, a la intimidad o a la propia imagen, que permite a las personas solicitar la protección de dichos derechos constitucionales. Y por otro lado, es un derecho derivado también del derecho a la protección de datos, que permite exigir la retirada de informaciones o contenidos relacionados con los sujetos que consideren perjudiciales, aunque sean lícitas, mediante los derechos de oposición,

rectificación y cancelación, después de un periodo de tiempo que las haga obsoletas e irrelevantes.

A pesar de que la sentencia del TC 58/2018, de 4 de junio de 2018 cambia completamente esta idea al reconocer expresamente el derecho al olvido como facultad inherente al derecho a la protección de datos personales, y por tanto como derecho fundamental, lo que supone la automática aplicación al mismo de la jurisprudencia relativa a los límites de los derechos fundamentales, seguimos considerando que el derecho al olvido no es un derecho fundamental, principalmente, por dos motivos. En primer lugar, obviamente, porque no aparece como tal recogido en la CE. En segundo lugar, el objeto principal de dicho derecho es borrar información del pasado de una persona que ésta considera innecesaria u obsoleta, considerando, en todo momento, que es veraz. En este sentido, la articulación del derecho al olvido se puede realizar a través de los derechos de rectificación o cancelación, estando, por tanto, limitado por los derechos constitucionales. Además, en el caso de que la información sea confusa o engañosa, podemos considerar el derecho al olvido como un derecho instrumental del derecho al honor.

6. El derecho al olvido es un derecho de supresión

Cada vez toma más fuerza asociar el derecho al olvido con el derecho a la protección de datos. Esta teoría se ve reforzada con el nuevo Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, en el que, por primera vez, aparece recogido en una normativa el concepto de derecho al olvido como un derecho de supresión que obliga al responsable del tratamiento a suprimir los datos personales del demandante y se abstenga de darles más difusión. Esta visión no aporta nada nuevo a las medidas que, hasta el momento, venían adoptando las agencias de protección de datos. Lo único que hace es configurar un concepto de derecho al olvido muy limitado y ya utilizado en el campo de la protección de datos, debido a que las personas ya tenían derecho a que sus datos personales fuesen retirados o rectificadas cuando eran inexactos o incorrectos.

7. La dificultad de revisar la información en un espacio virtual incalculable

Uno de los principales problemas del derecho al olvido radica en una cuestión de espacio, nos referimos a un espacio virtual y no físico, ya que Internet permite almacenar unas amplias cantidades de información que no se podrían almacenar en un espacio físico. Por lo tanto, es mucho más sencillo guardar la información que, cada cierto tiempo, ir revisando cuál sigue siendo relevante o cuál no. Por lo tanto, se trata de una rentabilidad temporal y económica, es más fácil mantenerla que borrarla, debido a la cantidad de tiempo que se perdería revisando todas esas informaciones y supondría un gasto tener a personas releendo esos contenidos.

8. La necesidad de fijar un periodo de prescripción tanto para las informaciones como para los datos

La inmediatez con la que circula el flujo informativo en Internet ocasiona, en algunos casos, que se infrinja la ley de protección de datos, llegándose, a veces, a incurrir también en delito de injurias y calumnias. La difusión pública de cualquier sentencia no puede utilizarse para llevar a cabo actividades que puedan vulnerar otros derechos fundamentales, como es el derecho a la protección de datos personales. En este sentido, sería un gran paso configurar un periodo de tiempo para que las informaciones o los datos prescribiesen, lo difícil es saber cuánto es ese tiempo y, sobre todo, variaría en función de si una persona es pública o privada, ya que la difusión y repercusión de las informaciones no sería la misma. El problema en este caso es que no hay formas efectivas de controlar su difusión, el daño ya se ha producido porque el implicado actuará cuando sus datos ya hayan sido difundidos en la red y los derechos se ejecutarían a posteriori, lo que dificultaría saber los perjuicios que han podido llegar a causar al implicado.

Por este motivo, Mayer-Schönberger es de la opinión de poner fecha de caducidad a las informaciones, lo que permitiría a los usuarios a ejercer un derecho al olvido a priori, ya que una vez cumplido el plazo establecido, se borrarían. Esto sólo se podría hacer en aquellas páginas, principalmente en las redes sociales, en las que el usuario suba sus datos, fotos o informaciones, ya que en el resto de páginas web tendrían que ser los propios responsables, los encargados de establecer esa fecha de caducidad y parece complicado que lo hagan si la ley no les obliga a ello.

9. Debe ponderar el principio de proporcionalidad entre la libertad de información y el derecho al olvido

Para buscar un equilibrio entre la libertad de información y el derecho al olvido habría que entrar a valorar cada caso para conocer si la información divulgada tiene interés público, dando por supuesto su veracidad –si no estaríamos hablando de un delito de injurias y calumnias–, ya que, en este caso, si se diesen ambos condicionantes, el derecho a la información imperará sobre el derecho a la intimidad. Por lo tanto, cada caso necesita un estudio suficiente para valorar la información y saber si la difusión de noticias pasadas, obsoletas a primera vista, pueden causar a la persona implicada inconvenientes en su vida actual.

10. Los usuarios de las redes sociales no pueden ampararse en el anonimato y tienen que ser responsables de lo que publican

En relación con la libertad de expresión y el derecho al olvido, nos encontramos con la problemática de los comentarios ofensivos e injuriosos vertidos en foros o blogs que permanecen perpetuos en la red. La dificultad surge a la hora de saber cómo lograr que se olviden esos contenidos y quién tiene la responsabilidad de hacer que dichos contenidos se olviden. El TEDH en el caso *Delfi AS v. Estonia* estableció que el responsable de los comentarios de los usuarios es la página web por no haber adoptado las medidas necesarias y exigibles para retirar dichos comentarios. Creemos que, si bien es cierto que el portal web ha de ser responsable de los comentarios publicados en él, teniendo que ejercer un mayor control sobre sus contenidos, los usuarios, apoyados en el anonimato, no pueden salir impunes de sus comentarios y tienen que ser también responsables de lo que publican, ya que si no seguirán escribiendo sin ningún tipo de control.

11. Los nombres y apellidos de las personas no públicas no aportan nada a las informaciones

El TC en su sentencia 58/2018, de 4 de junio de 2018, viene a ser un paso más en la lucha a favor del derecho al olvido, extendiendo su ámbito a las hemerotecas digitales, al prohibirse la indexación de los datos personales de las demandantes de amparo, en lo que se refiere al nombre y apellidos de las recurrentes, para su uso por el motor de búsqueda interno de la hemeroteca digital, ya que los nombres y apellidos de los solicitantes no agregan nada de interés a la noticia y han de ser suprimidos o sustituidos

por sus iniciales. La medida requerida es necesaria porque su adopción limitará la búsqueda y localización de la noticia en la hemeroteca digital sobre la base de datos personales inequívocamente identificativos de las personas recurrentes. Además, el TC entiende que tanto el valor del paso del tiempo a la hora de calibrar el impacto de difusión de la noticia como la importancia de la digitalización de los documentos informativos son dos variables determinantes.

12. Necesidad de ampliar la normativa concreta que regula el acceso a los documentos en Internet

Existe una escasez de normativa concreta, pública y privada, que regula el acceso a los documentos en Internet. En el ordenamiento jurídico español, el acceso a la información es un derecho de configuración legal, lo que hace depender su contenido de la voluntad del legislador, por lo que en algunos casos, se favorece la opacidad. La ley española supedita el ejercicio efectivo del derecho de acceso al principio de eficacia administrativa, cuando debería ser al contrario.

13. La importancia, por parte de las redes sociales y de los proveedores, de regular los datos de carácter personal y las imágenes

La captación y reproducción de imágenes de terceros, constituyen datos de carácter personal, y su publicación en Internet se encuentra sometida al consentimiento de sus titulares. En la comunicación electrónica, sin embargo, lo importante es, además de la captación de una imagen, el uso o tratamiento que se pueda hacer de ella en la red. La publicación de imágenes de terceras personas sin su consentimiento en un perfil de la red social puede vulnerar dos derechos fundamentales: el derecho a la propia imagen y el derecho a la protección de datos personales. Las redes sociales al igual que los proveedores de servicios de Internet tienen que controlar los contenidos en ellos alojados. La verificación de la edad en las redes sociales es una obligación legal y por tanto, tienen que instaurar mecanismos de acreditación para los menores.

14. La globalización de las leyes para acabar con la protección territorial

Internet y su naturaleza globalizada ha provocado una nueva situación en la que los conflictos, sobre todo los sujetos en ellos no están territorializados y esto plantea un problema de identificación de la ley aplicable. El TEDH en el caso *Arlewin v. Sweden* consideró que lo relevante para determinar la competencia judicial en un caso de

difamación es a quién se difama y no desde donde se difama. Estamos, por tanto, hablando de que ya no existen unas fronteras físicas como hasta ahora estaban delimitadas, sino que el mundo se ha fusionado gracias a la Red.

15. La muerte digital, una regulación necesaria

Otro aspecto importante es el derecho a la muerte digital. Francia ha sido el primer país en reconocerlo y permitir a los usuarios que establezcan sus condiciones relativas a la conservación y a la comunicación de sus datos de carácter personal tras su muerte. Lo que permite esta Ley es que los usuarios puedan dejar en su testamento lo que quieren que se hagan con sus cuentas en las redes sociales, claves de acceso y bibliotecas digitales (música, películas y libros adquiridas por el usuario en formato digital), designando un albacea o bien a través de sus sucesores. Es importante que se regule en todos los países el derecho a la muerte digital, porque no es muy agradable para los familiares de los fallecidos que no puedan cerrar sus cuentas o acceder a ellas y ver cómo siguen activas en Internet.

16. El derecho al olvido como respuesta a las fake news

Las fake news pueden atentar contra el derecho al honor, la intimidad y la propia imagen del sujeto. Por eso, ahora es más necesario que nunca que las personas pueden ejercitar su derecho al olvido, ya que su imagen no solo se va a poder ver dañada por noticias de su pasado sino por noticias falsas. De ahí que la protección de la vida privada y la reputación encuentren en el derecho al olvido un instrumento eficaz para limitar el daño que pueden provocar las noticias falsas divulgadas en las redes sociales, ya que, al hecho que conlleva la publicación de una información falsa, se suma la intensificación de su capacidad para difamar al aprovechar la red para propagarse sin ningún límite físico de espacio y tiempo que pudiese minimizar el daño.

17. Las hemerotecas digitales como estandartes de la libertad de información

La sentencia del TC 58/2018, de 4 de junio de 2018 cambia completamente esta idea al reconocer expresamente el derecho al olvido como facultad inherente al derecho a la protección de datos personales. Los datos personales cuya supresión se solicita por las personas recurrentes están contenidos en la hemeroteca digital de Ediciones El País, y el recurso de amparo está relacionado con el rechazo a ocultar los nombres de las personas recurrentes u oscurecerlos a través del uso de sus iniciales. Nos encontramos con un

conflicto circunscrito al uso de nombres propios como criterio de búsqueda y localización de noticias en el entorno de una hemeroteca digitalizada.

JURISPRUDENCIA

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA

STJUE C-101/01, de 6 de noviembre de 2003, caso *Lindqvist*.

STJUE C-465/00, de 20 de mayo de 2003, caso *Österreichischer Rundfunk*.

STJUE C-275/06, de 29 de enero de 2008, caso *Promusicae c. Telefónica España*.

STJUE C-131/12, de 13 de mayo de 2014, caso *Google Spain, S.L. y Google Inc. c. AEPD y Mario Costeja González*.

STJUE C-362/14, de 6 de octubre de 2015, caso *Maximillian Schrems c. Data Protection Commissioner*.

Conclusiones del Abogado General TJUE asunto C-131/12, de 25 de junio de 2013.

TRIBUNAL EUROPEO DE DERECHOS HUMANOS

STEDH, de 8 de julio de 1986, caso *Lingens c. Austria*.

STEDH, de 11 de julio de 2000, caso *Jabari c. Turquía*.

STEDH, de 18 de mayo de 2004, caso *Éditions Plon c. Francia*.

STEDH, de 24 de junio de 2004, caso *Von Hannover c. Alemania*.

STEDH, de 1 de marzo de 2016, caso *Arlewin c. Sweden*.

STEDH, de 1 de junio de 2010, caso *Gutiérrez Suárez c. España*.

STEDH, de 15 de marzo de 2011, caso *Otegui Mondragón c. España*.

ESPAÑA

- TRIBUNAL CONSTITUCIONAL

STC 6/1981, de 16 de marzo.

STC 11/1981, de 8 de abril.

STC 52/1983, de 17 de junio.

STC 107/1984, de 23 de noviembre.

STC 110/1984, de 26 de noviembre.

STC 53/1985, de 11 de abril.

STC 99/1985, de 30 de septiembre.

STC 104/1986, de 17 de julio.

STC 168/1986, de 22 de diciembre.

STC 165/1987, de 27 de octubre.

STC 231/1988, de 2 de diciembre.

STC 171/1990, de 12 de noviembre.
STC 172/1990, de 12 de noviembre.
STC 197/1991, de 17 de octubre.
STC 20/1992, de 14 de febrero.
STC 223/1992, de 14 de diciembre.
STC 240/1992, de 21 de diciembre.
STC 254/1993, de 20 de julio.
STC 99/1994, de 11 de abril.
STC 242/1994, de 20 de julio.
STC 176/1995, de 11 de diciembre.
STC 207/1996, de 16 de diciembre.
STC 134/1999, de 15 de julio.
STC 144/1999, de 22 de julio.
STC 187/1999, de 25 de octubre.
STC 192/1999, de 25 de octubre.
STC 91/2000, de 30 de marzo.
STC 98/2000, de 10 de abril.
STC 115/2000, de 10 de mayo.
STC 186/2000, de 10 de julio.
STC 290/2000, de 30 de noviembre.
STC 292/2000, de 30 de noviembre.
STC 81/2001, de 26 de marzo.
STC 139/2001, de 18 de junio.
STC 156/2001, de 2 de julio.
STC 83/2002, de 22 de abril.
STC 127/2003, de 30 de junio.
STC 196/2004, de 15 de noviembre.
STC 89/2006, de 27 de marzo.
STC 196/2006, de 3 de julio.
STC 72/2007, de 16 de abril.
STC 206/2007, de 24 de septiembre.
STC 29/2009, de 26 de enero.
STC 70/2009, de 23 de marzo.
STC 159/2009, de 29 de junio.

STC 173/2011, de 7 de noviembre.

STC 12/2012, de 30 de enero.

STC 170/2013, de 7 de octubre.

STC 58/2018, de 4 de junio.

- **TRIBUNAL SUPREMO**

STS 1588/1988, de 7 de marzo. Sala de lo Civil.

STS 7765/1997, de 17 de diciembre. Sala de lo Civil (nº de recurso: 30/1994).

STS 4851/1998, de 18 de julio. Sala de lo Civil (nº de recurso: 1319/1994).

STS 1105/1999, de 18 de febrero. Sala de lo Penal (nº de recurso: 3256/1998).

STS 3424/2000, de 24 de abril. Sala de lo Civil (nº de recurso: 432/2000).

STS 7601/2000, de 23 de octubre. Sala de lo Penal (nº de recurso: 465/1999).

STS 3256/2001, de 20 de abril. Sala de lo Civil (nº de recurso: 918/1996).

STS 3818/2002, de 28 de mayo. Sala de lo Civil (nº de recurso: 3761/1996).

STS 1578/2002, de 2 de octubre. Sala de lo Penal (nº de recurso: 451/2001).

STS 1750/2003, de 14 de marzo. Sala de lo civil (nº de recurso: 2313/1997).

STS 2162/2003, de 28 de marzo. Sala de lo Social (nº de recurso: 81/2002).

STS 4149/2006, de 19 de junio. Sala de lo Penal (nº de recurso: 1392/2005).

STS 769/2006, de 22 de febrero. Sala de lo Civil (nº de recurso: 2926/2001).

STS 3164/2008, de 26 de junio. Sala de lo Contencioso-administrativo (nº de recurso: 6818/2003).

STS 4866/2008, de 25 de septiembre de 2008. Sala de lo Civil (nº de recurso: 2578/2002).

STS 613/2009, de 26 de febrero. Sala de lo Civil (nº de recurso: 465/2004).

STS 3931/2009, de 15 de junio. Sala de lo Penal (nº de recurso: 1721/2008).

STS 6147/2010, de 17 de noviembre. Sala de lo Contencioso-administrativo (nº de recurso: 1513/2009).

STS 6858/2011, de 14 de octubre. Sala de lo Penal (nº de recurso: 10365/2011).

STS 817/2014, de 26 de noviembre. Sala de lo Penal (nº de recurso: 20811/2013).

STS 4132/2015, de 15 de octubre. Sala de lo Civil (nº recurso: 2772/2013).

STS 5809/2015, de 10 de diciembre. Sala de lo Penal (nº de recurso 912/2015).

STS 964/2016, de 14 de marzo. Sala de lo Contencioso-administrativo (nº recurso: 1380/2015).

STS 1280/2016, de 5 de abril. Sala de lo Civil (nº recurso: 3269/2014).

STS 19/2019, de 11 de enero de 2019. Sala de lo Contencioso (nº recurso: 5579/2017).

- **AUDIENCIA NACIONAL**

SAN 62/2001, de 12 de enero. Sala de lo Contencioso-administrativo.

SAN 170/2012, de 11 de abril. Sala de lo Contencioso-administrativo (nº de recurso: 410/2010).

SAN 5129/2014, de 29 de diciembre. Sala de lo Contencioso-administrativo (nº de recurso: 725/2010).

Auto AN 19/2012, de 27 de febrero. Sala de lo Contencioso-administrativo. Sección 1ª.

- **TRIBUNAL SUPERIOR DE JUSTICIA**

STSJ de Cataluña 7044/2003, de 11 de junio. Sala de lo social (nº de recurso: 8186/2002).

STSJ Castilla y León 5546/2004, de 8 de noviembre. Sala de lo Social (nº de recurso: 2006/2004).

- **AUDIENCIA PROVINCIAL**

SAP Lugo 00538/2009, de 9 de julio. Sección 1ª.

SAP de Barcelona 486/2013, de 11 de octubre. Sección 14.

SAP Barcelona 8246/2014, de 17 de julio. Sección 16.

Auto AP Madrid AP de Madrid 11574/2011, de 21 de julio. Sección 11ª (nº de recurso: 129/2011).

- **JUZGADOS DE PRIMERA INSTANCIA O INSTRUCCIÓN**

Sentencia del Juzgado de 1ª Instancia número 44 de Madrid, núm. 00184/2007, de 19 de septiembre.

Sentencia del Juzgado de lo Penal número 11 de Barcelona, núm. 140/2008, de 20 de julio.

Sentencia del Juzgado de lo Mercantil número 7 de Barcelona, núm. 67/2010, de 9 de marzo.

Sentencia del Juzgado de lo Mercantil número 6 de Barcelona, núm. 149/2010, de 22 de abril.

Sentencia del Juzgado de lo Mercantil número 4 de Madrid, núm. 133/2011, de 25 de noviembre.

Sentencia del Juzgado de 1ª Instancia número 5 de Pamplona, núm. 213/2012, de 15 de octubre.

Sentencia del Juzgado de lo Penal número 28 de Barcelona, núm. 416/2013, de 3 de octubre.

Sentencia del Juzgado de Instrucción número 2 de Granada, núm. 239/2012, de 15 de octubre.

Auto del Juzgado de lo Mercantil número 11 de Madrid, núm. 246/2015, de 16 de junio.

Auto del Juzgado de lo Mercantil número 1 de A Coruña, núm. 203/2015, de 26 de noviembre.

ALEMANIA

Sentencia Tribunal Constitucional Federal de Alemania, de 15 de diciembre de 1983.

ARGENTINA

Sentencia Sala J de la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, de 31 de agosto de 2012.

Sentencia Sala I de la Cámara Nacional de Apelaciones en lo Civil y Comercial Federal, de 6 de septiembre de 2012.

COLOMBIA

Sentencia Corte Constitucional de Colombia T-414/92, de 16 de junio.

ESTADOS UNIDOS

Sentencia de la Corte Suprema de los Estados Unidos en el caso *Silverman v. United States*, de 6 de marzo de 1961.

Sentencia de la Corte Suprema de los Estados Unidos en el caso *New York Times Co. v. Sullivan*, de 9 de marzo de 1964.

Sentencia de la Corte Suprema de los Estados Unidos en el caso *Bowers v. Hardwick*, de 30 de junio de 1986.

Sentencia de la Corte Suprema de los Estados Unidos *ACLU v. J. Reno*, de 26 de junio de 1997.

Sentencia de la Corte Suprema de los Estados Unidos *Lawrence v. Texas*, de 26 de marzo de 2003.

Sentencia Corte de Apelación de California en el caso *Melvin v. Reid*, de 28 de febrero de 1931.

Sentencia Corte de Apelación 9ª de Estados Unidos en el caso *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme and L'union Des Etudiants Juifs De France* (No. 01-17424), de 12 de enero de 2006.

Sentencia de la Corte de Apelación 2ª de Estados Unidos en el caso *Martin v. Hearst Corporation*, de 28 de enero de 2015.

Sentencia Corte del Distrito Este de Pennsylvania en el caso *Snyder v. Millersville University*, de 3 de diciembre de 2008.

FRANCIA

Sentencia *Tribunal de Grande Instance* de París, de 20 de abril de 1983.

Sentencia *Tribunal de Grande Instance* de París, 22 de mayo de 2000.

Sentencia *Tribunal de Grande Instance* de París, 15 de febrero de 2012.

Sentencia *Tribunal de Grande Instance* de París, de 16 de septiembre de 2014.

Sentencia *Tribunal de Grande Instance* de París, de 19 de marzo de 2015.

ITALIA

Sentencia Corte Suprema de Casación 5525/2012, de 5 de abril de 2012.

BIBLIOGRAFÍA

- ABERASTURI GORRIÑO, Unai (2016). Derecho a ser olvidado en Internet y medios de comunicación digitales. A propósito de la Sentencia del Tribunal Supremo de 15 de octubre de 2015. *Revista Española de Derecho Administrativo* nº175.
- ABRIL, Patricia y PIZARRO MORENO, Eugenio (2014). La intimidad europea frente a la privacidad americana. *Revista InDret*. Barcelona.
- ADAMS, Fred (2003). The informational turn in philosophy. *Minds and Machines* nº13.
- AGUIRRE ROMERO, Joaquín María (2004). Ciberespacio y comunicación. Nuevas formas de vertebración social en el siglo XXI. *Espéculo. Revista de Estudios Literarios* nº27.
- AGUSTINA, José R. (2014). Cibercriminalidad y perspectiva victimológica: Un enfoque explicativo de la cibervictimización. *Cuadernos de Política Criminal* nº114.
- AISCH, Gregor, HUANG, Jon, y KANG, Cecilia (2016). *Dissecting the #PizzaGate Conspiracy Theories*. New York Times.
- ALARCÓN SEVILLA, Verónica (2011). *El BOE deberá seguir utilizando el fichero "robots.txt"*. Legal Today.
- ALDERMAN, Ellen y KENNEDY Caroline (1997). *The right to privacy*. Vintage.
- ALLCOTT, Hunt y GENTZKOW, Matthew (2017). *Social Media and Fake News in the 2016 Election*. NBER Working Paper nº23089.
- ALLEGRI, Maria Romana (2018). Diritto all'oblio, tutela della web reputation individuale e "eccezione giornalistica": spunti giurisprudenziali. *Forum di Quaderni Costituzionali*.

ALONSO GARCÍA, Enrique (1984). *La interpretación de la Constitución*. Centro de Estudios Constitucionales. Madrid.

ÁLVAREZ CARO, María (2015). *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la red digital*. Editorial Reus.

AMORÓS, Marc (2018). *Fake news. La verdad de las noticias falsas*. Plataforma editorial.

ARBELÁEZ-GIRALDO, A. (2017). El ciberespacio y el problema de la realidad virtual. *Revista de Filosofía UIS* nº16 (2).

ARENAS RAMIRO, Mónica (2014). Unforgettable: a propósito de la STJUE de 13 de mayo de 2014. Caso Costeja (Google vs. AEPD). *Revista Teoría y Realidad Constitucional*, nº3.

AYALA PÉREZ, Teresa (2016). *Memoria versus olvido: La paradoja de Internet*. UNIVERSUM. Vol. 31, nº1.

AZURMENDI ADARRAGA, Ana (1997). *El derecho a la propia imagen: su identidad y aproximación al derecho a la información*. Civitas.

AZURMENDI ADARRAGA, Ana (2005). De la verdad informativa a la “información veraz” de la Constitución Española de 1978. Una reflexión sobre la verdad exigible desde el derecho de la información. *Comunicación y Sociedad*. Vol. XVIII, nº2.

AZURMENDI ADARRAGA, Ana (2014). *Derecho de autodeterminación informativa y el derecho al olvido: la generación “Google” del derecho a la vida privada*. Universitat Oberta de Catalunya. Huygens. Barcelona.

AZURMENDI ADARRAGA, Ana (2015). Por un derecho al olvido para los europeos: aportaciones jurisprudenciales de la sentencia del Tribunal de Justicia Europeo del caso Google Spain y su recepción por la Sentencia de la Audiencia Nacional

española de 29 de diciembre de 2014. *Revista de Derecho Político* nº92. UNED, págs. 273-310.

BAGDIKIAN, Ben (2004). *The new media monopoly*. Beacon Press Books. USA.

BALKIN, Jack (2017). Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation. *UC Davis Law Review*. Vol. 51, pág. 1151-1209.

BAÑOS, José María (2010). *Ley Facebook: Modificaciones en la legislación de protección de datos alemana*. Legal Today.

BASTIDA FREIJEDO, Francisco José (1994). *El régimen jurídico de la comunicación social*. Instituto de Estudios Económicos. Madrid.

BASTIDA FREIJEDO, Francisco José (2004). *Concepto y modelos históricos de los derechos fundamentales en Teoría General de los derechos fundamentales en la Constitución Española de 1978*. Tecnos.

BASTIDA FREIJEDO, Francisco José (2005). El fundamento de los derechos fundamentales. *Revista electrónica del Departamento de Derecho de la Universidad de La Rioja* nº3.

BEL, Ignacio y CORREDOIRA Loreto (directores) (2015). *Derecho de la información. El ejercicio del derecho a la información y su jurisprudencia*. Centro de Estudios Políticos y Constitucionales. Madrid.

BENAVENTE MORADA, Pilar (2013). Identidad y contexto inmediato de la persona. *Anuario de la Facultad de derecho* nº17. Universidad Autónoma de Madrid.

BENITO MARTÍN, Ruth (2014). *Consideraciones en torno al derecho al olvido*. Observatorio Iberoamericano de Protección de Datos.

- BERNAL, Paul (2014). *Internet Privacy Rights. Rights to Protect Autonomy*. Cambridge University Press. New York.
- BERROCAL LANZAROT, Ana Isabel (2017). *Derecho de supresión de datos o derecho al olvido*. Editorial Reus. Madrid.
- BERTONI, Eduardo (2014). *Derecho al olvido: ¿es problemática la decisión del Tribunal de Justicia de la Unión Europea para América Latina?*
- BOGHARDT, Thomas (2009). Soviet Bloc Intelligence and Its AIDS Disinformation Campaign. *Studies in Intelligence*. Vol. 53. N°4.
- BOIX PALOP, Andrés (2015), El equilibrio entre los derechos del artículo 18 de la Constitución, el«Derecho al olvido» y las libertades informativas tras la sentencia Google. *Revista General de Derecho Administrativo* n°38.
- BOIZARD, Maryline (2015). *Le droit à l'oubli*. Faculté de droit et de science politique. Rennes.
- BORGES, Jorge Luis (1994). *La Biblioteca de Babel, Obras completas (1923-1949)*. Emece Editores. Buenos Aires.
- BOTANA GARCÍA, Gema Alejandra, y OVEJERO PUENTE, Ana María (2014). Claves de la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 en la cuestión prejudicial planteada en el caso Google. *Actualidad Civil*, 9 de junio de 2014. Editorial La Ley.
- BOYD, Danah y ELLISON, Nicole (2007). Social Network Sites: Definition, history and scholarship. *Journal of Computer-Mediated Communication* n°13 (1).
- BRADSHAW, Samantha y HOWARD, Philip (2018). Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation. *Computational Propaganda Research Project*. University of Oxford.

- BRANDT, Allan M. (1978). Racism and research: The case of the Tuskegee Syphilis study. *The Hastings Center Report* 8(6), págs. 21-29.
- BREY, Antoni (2009). *La sociedad de la ignorancia y otros ensayos*. Infonomia. Barcelona.
- BRINGUÉ, Xavier y SÁDABA-CHALEZQUER, Charo (2009). *La generación interactiva en España. Niños y adolescentes ante las pantallas*. Colección Fundación Telefónica. Cuaderno nº22. Ariel.
- BROCK, George (2016). *The Right to be Forgotten: Privacy and the Media in the Digital Age*. I.B.Tauris. London.
- BRONSTEIN, Michael, BRUNA, Joan, LECUN, Yann, SZLAM, Arthur, y VANDERGHEYNST, Pierre (2017). Geometric Deep Learning. Going beyond Euclidean data. *IEEE Signal Processing magazine*, julio.
- BROTONS MOLINA, Olga (2013). Caso Google: Tratamiento de datos y derecho al olvido. Análisis de las conclusiones del abogado general, asunto C-131/12. *Revista Aranzadi de Derecho y Nuevas Tecnologías* nº33.
- BRUBAKER, Jed R., HAYES, Gillian R. Y DOURISH, Paul (2013). Beyond the Grave: Facebook as a Site for the Expansion of Death and Mourning. *The Information Society*. Vol. 29, nº3.
- BUISÁN GARCÍA, Nieves (2014). El derecho al olvido: el nuevo contenido de un derecho antiguo. *El Cronista del Estado Social y Democrático de Derecho* nº46.
- CABALLERO SÁNCHEZ, Rafael (1999). *Prescripción y caducidad en el ordenamiento administrativo*. McGraw-Hill. Madrid.
- CAMPUZANO TOMÉ, Herminia (2000). *Vida privada y datos personales: su protección jurídica frente a la sociedad de la información*. Tecnos. Madrid.

- CARBONELL MATEU, Juan Carlos y GONZÁLEZ CUSSAC, José Luis (1999). *Derecho penal. Parte especial*. Tirant lo Blanch. Valencia.
- CARR, Nicholas (2008). *Superficiales, ¿Qué está haciendo Internet con nuestras mentes?* Editorial Taurus.
- CARRILLO LÓPEZ, Marc (2003). *El derecho a no ser molestado. Información y vida privada*. Aranzadi. Navarra.
- CARRILLO LÓPEZ, Marc (2008). La intimidad, las celebridades y el derecho a la información. *Diario La Ley* nº 6979, año XXIX.
- CARRILLO LÓPEZ, Marc (2009). *El derecho al olvido en Internet*.
- CASINO RUBIO, Miguel (2012). El periódico de ayer, el derecho al olvido en Internet y otras noticias. *Revista española de Derecho Administrativo* nº156.
- CASTELLS, Manuel (2009). *Comunicación y poder*. Madrid. Alianza Editorial.
- CASTILLO JIMÉNEZ, Cinta (2001). *Protección del Derecho a la Intimidad y uso de las nuevas tecnologías de la información; en Derecho y conocimiento: anuario jurídico sobre la sociedad de la información y del conocimiento*. Vol. 1. Universidad de Huelva.
- CATE, Fred H. (2001). *Privacy in Perspective*. The American Enterprise Institute. Washington.
- CATE, Fred H., MAYER-SCHÖNBERGER, Viktor y CULLEN, Peter (2014). *Data Protection Principles for the 21st Century. Revising the 1980 OECD Guidelines*. Universidad de Oxford.
- CELAYA, Javier (2008). *La Empresa en la WEB 2.0*. Editorial Grupo Planeta.

- CERRILLO-I-MARTÍNEZ, Agustí, PEGUERA, Miquel, PEÑA-LÓPEZ, Ismael y VILASAU SOLANA, Mónica (2011). *Neutralidad de la red y otros retos para el futuro de Internet*. Huygens Editorial.
- CHÉLIZ INGLÉS, María del Carmen (2016). El “derecho al olvido digital”. Una exigencia de las nuevas tecnologías, recogida en el futuro reglamento general de protección de datos. *Actualidad jurídica iberoamericana* nº5.
- COBACHO LÓPEZ, Ángel y BURGUERA AMEAVE, Leyre (2013). *Responsabilidad de los webmasters y derecho al olvido digital*. Thomson Reuters-Aranzadi.
- COOK, Lyndsay (2015). The Right to Be Forgotten: A Step in the Right Direction for Cyberspace Law and Policy. *Journal of Law, Technology & The Internet*. Vol. 6.
- COOLEY, Thomas McIntyre (1879). *A treatise on the law of torts or the wrongs which arise independently of contract*. Callaghan. Chicago.
- CORTÉS, Carlos e ISAZA, Luisa (2017). Noticias falsas en Internet: la estrategia para combatir la desinformación. *Centro de Estudios en Libertad de Expresión y Acceso a la Información*. Universidad de Palermo.
- COSTAZ, Catherine (1995). Le droit à l’oubli. *Gazette du Palais*, págs. 961-970.
- COTINO HUESO, L. (2010). *Datos personales y libertades informativas. Medios de comunicación social como fuentes accesibles al público (Art. 3 de la LOPD)*. Thomsom-Civitas.
- COTINO HUESO, Lorenzo (2014). *La STJUE del caso Google vs AGPD de 2014. Algunos “olvidos” y otras tendencias negativas respecto de las libertades informativas en Internet*. Ponencia en el seminario de la Facultad de Derecho de Valencia: Google, el derecho al olvido y la responsabilidad de prestadores e intermediarios.

- COTINO HUESO, Lorenzo (2015). *El conflicto entre las libertades de expresión e información en internet y el derecho a la protección de datos. El derecho al olvido y sus retos: “un falso derecho, a juzgar por un falso tribunal”*. Centro de Estudios Políticos y Constitucionales. Madrid.
- CHRISTENSEN, Dorthé Refslund y SANDVIK, Kjetil (2014). *Mediating and Remediating Death*. Ashgate.
- DAVARA RODRÍGUEZ, Miguel Ángel. (2013). El derecho al olvido en Internet. *Diario La Ley* nº 8.137.
- DE AGUINAGA LÓPEZ, Enrique (1998). ¿Información veraz? *Estudios sobre el mensaje periodístico* nº4.
- DE BAETS, Antoon (2016). A historian's view on the right to be forgotten. *International Review of Law, Computers & Technology*. Vol. 30 (1-2).
- DE LA CUESTA ARZAMENDI, José Luis y PÉREZ MACHÍO, Ana Isabel (2010). Cibercriminales y cibervíctimas. *Derecho Penal Informático*. Pamplona.
- DE LA CUEVA GONZÁLEZ-COTERA, Javier (2012). Relato del VII Congreso Internacional sobre Internet, Derecho y Política: Neutralidad de la red y derecho al olvido. *Revista de Internet, Derecho y Política* nº13, febrero. Universitat Oberta de Catalunya.
- DE LA IGLESIA CHAMARRO, Asunción (2003). El derecho a la propia imagen de los personajes públicos. *Revista Española de Derecho Constitucional* nº 67.
- DE MIGUEL ASENSIO, Pedro (2012). Buscadores de Internet y protección de datos: la cuestión prejudicial de la Audiencia Nacional sobre Google. *Diario La Ley* nº7870.

- DE TERWANGNE, Cécile (2012). Privacidad en Internet y el derecho a ser olvidado/derecho al olvido. *Revista de Internet, Derecho y Política* n°13, febrero. Universitat Oberta de Catalunya.
- DEL CAMPO, Agustina (2018). La regulación de Internet y su impacto en la libertad de expresión en América Latina. *Centro de Estudios en Libertad de Expresión y Acceso a la Información* (CELE). Universidad de Palermo, marzo.
- DEL REY GUANTER, Salvador (2005). *Relaciones Laborales y Nuevas Tecnologías*. La Ley. Madrid.
- DENTITH, Matthew (2017). The problem of fake news. *Public Reason* 8 (1-2), págs. 65-79.
- DÉTRAIGNE, Yves y ESCOFFIER, Anne-Marie (2009). *Rapport d'information relatif au respect de la vie privée à l'heure des mémoires numériques*.
- DURÁN RUIZ, Francisco (2014). *Autodeterminación informativa y derecho al olvido en la Unión Europea, particularidades respecto de los menores de edad*. Actas del VII simposio de “Las sociedades ante el reto digital”.
- EMERSON, Thomas (1979). *The Right of Privacy and Freedom of the Press*. Yale Law School.
- ERDOS, David (2012). *Confused? Analysing the Scope of Freedom of Speech Protection vis-à-vis European Data Protection*. Universidad de Oxford.
- EUROPEAN COMMISSION (2018). *A multi-dimensional approach to disinformation: Report of the independent High level Group on fake news and online disinformation*. Communications Networks, Content and Technology.
- FARRIOLS I SOLÁ, A. (coord.) (2006). *La protección de datos de carácter personal en los centros de trabajo*. Editorial Cinca. Colección Estudios Laborales.

- FAULKNER, Paul (2018). Fake Barns, Fake News. *Social Epistemology Review and Reply Collective* 7, nº6.
- FERNÁNDEZ ESTEBAN, María Luisa (1998). Limitaciones constitucionales e inconstitucionales a la libertad de expresión en Internet. *Revista Española de Derecho Constitucional* nº53.
- FERNÁNDEZ GARCÍA-ARMERO, Pablo (2018). El derecho al olvido. *Cuadernos de Dereito Actual* nº9.
- FERNÁNDEZ TOLEDO, María Piedad y FERRERAS RODRÍGUEZ, José Gabriel (coord.) (2012). *Del yo al nosotros. Los discursos y la comunicación en la colectividad digital*. Editorial Académica Española.
- FERNÁNDEZ VILLAZÓN, Luis Antonio (2016). El nuevo reglamento europeo de protección de datos. *Revista Foro. Nueva Época*. Vol. 19, nº1.
- FISS, Owen (1999). *La ironía de la libertad de expresión*. Gedisa Editorial, Barcelona.
- FLORES VIVAR, Jesús Miguel (2009). Nuevos modelos de comunicación, perfiles y tendencias en las redes sociales. *Comunicar. Revista Científica de Educomunicación*. Vol. 17, nº33.
- FORMAN, Abbe E., KERN, Rebecca y GIL-EGUI, Gisela (2012). Death and Mourning as Sources of Community Participation in Online Social Networks: R.I.P. Pages in Facebook. *First Monday*. Vol. 17, nº9.
- GALÁN-JUÁREZ, Mercedes (2006). Derecho a transmitir libremente información veraz. *Persona y derecho: Revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos* nº55.
- GALÁN MUÑOZ, Alfonso (coord.) (2014). *La protección jurídica de la intimidad y de los datos de carácter personal frente a las nuevas tecnologías de la información y comunicación*. Tirant lo Blanch. Valencia.

- GARCÍA-ATANCE Y GARCÍA DE MORA, María Victoria (2011). *Derechos y libertades en la Constitución Española de 1978*. Editorial Sanz y Torres. Madrid.
- GARCÍA-BERRIO HERNÁNDEZ, Teresa (2003). *Informática y libertades. La protección de datos personales y su regulación en Francia y España*. Colección Estudios de Derecho. Universidad de Murcia.
- GARRIGA DOMÍNGUEZ, Ana (2015). *Nuevos retos para la protección de datos personales*. Dykinson. Madrid.
- GELFERT, Axel (2018). Fake news: a definition. *Informal Logic*. Vol. 38, nº1, págs. 84-117.
- GERARDO, Scotti (2015). Dall'Habeas Corpus all'Habeas Data: il diritto all'oblio ed il diritto all'anonimato nella loro dimensione costituzionale. *Diritto Civile e Commerciale*.
- GIAMPA, Giovanna (2016). Americans have a right to be forgotten. *Law School Student Scholarship*. Seton Hall University.
- GILBERT, Françoise (2014). Article 29 Working Party Supports European Court of Justice "Right to Be Forgotten" Rule. *Computer & Internet Lawyer*. Vol. 31, nº8.
- GIL GONZÁLEZ, Elena (2016). *Big data, privacidad y protección de datos*. Agencia Española de Protección de Datos.
- GLEICK, James (2011). *La información. Historia y realidad*. Editorial Crítica.
- GOERTZEL, Ted (1994). Belief in Conspiracy Theories. *Political Psychology* nº 15.
- GÓMEZ LOECHES, Luis (1998). *El acceso a la documentación de las actuaciones judiciales*. VI Jornadas Españolas de Documentación. FESABID.

- GOBERNADO SERRANO, José Manuel (2012). *Demencias*. Unidad de Demencias del Servicio de Neurología del Hospital Ramón y Cajal. Madrid.
- GOLDMAN, Alvin (2018). *Free speech, fake news and democracy*. Rutgers University.
- GÓMEZ BACEIREDO, Beatriz, MARTÍNEZ RODRÍGUEZ, Lourdes, y TORRADO MORALES, Susana (2012). *¿Compartimos mentiras? El periodismo, la credibilidad y el “efecto bola de nieve” en Internet*, págs. 86-106.
- GOMES DE ANDRADE, Norberto Nuno (2012). El olvido: El derecho a ser diferente... de uno mismo. Una reconsideración del derecho a ser olvidado. *Revista de Internet, Derecho y Política* nº13, febrero. Universitat Oberta de Catalunya.
- GÓMEZ DE LIAÑO FONSECA-HERRERO, Marta (2012). La prohibición constitucional del uso de cámaras ocultas en el marco del denominado periodismo de investigación. *Revista Derecom* nº13.
- GONZÁLEZ BALLESTEROS, Teodoro (2011). *Diccionario jurídico*. Dykinson, Madrid.
- GOTVED, Stine (2014). Research Review: Death Online - Alive and Kicking! *Thanatos*. Vol. 3
- GRAUER RODOY, Isaac (2014). Bases para una jurisprudencia unificada sobre desindexación de contenidos en Internet. *Diario la Ley*, nº8374.
- GREENBERG, Susan (2007). Why doesn't Britain have a culture of serious non-fiction journalism like the US? *Revista Prospect*, febrero.
- GUASCH PORTAS, Vicente y SOLER FUENSANTA, José Ramón (2015). El derecho al olvido en Internet. *Revista de Derecho UNED* nº16.

- GUERRERO ZAPLANA, José (2014). La sentencia del asunto Google. Configuración del derecho al olvido realizada por el TJUE. *Revista Aranzadi Doctrinal* nº4.
- GUESS, Andrew; NAGLER, Jonathan; y TUCKER, Joshua (2019). Less than you think: Prevalence and predictors of fake news dissemination on Facebook. *Science Advances*. Vol. 5, nº1, enero.
- GUICHOT REINA, Emilio (coord.) (2015). *Derecho de la comunicación*. Iustel. Madrid.
- GUTIÉRREZ MARÍN, Daniel (2014). *Los efectos del analfabetismo tecnológico: consecuencias en la formación universitaria*. Libro de actas Primer Congreso Internacional “Infoxicación: mercado de la información y psique”. Ladecom. Sevilla.
- HELLER, Jean (1972). *Syphilis victims in U.S. study went untreated for 40 years*. New York Times.
- HERNÁNDEZ RAMOS, Mario (2013). El derecho al olvido digital en la web 2.0. *Revista Cátedra Telefónica de la Universidad de Salamanca* nº11, mayo.
- HOWARD, Philip; KOLLANYI, Bence, BRADSHAW, Samantha; NEUDERT, Lisa-Maria (2017). *Junk News and Bots during the U.S. Election: What Were Michigan Voters Sharing Over Twitter?* University of Oxford.
- HORNUNG, Gerrit y SCHNABEL Christoph (2009). Data protection in Germany I: The population census decision and the right to informational self-determination. *Computer Law & Security Report*. Vol. 25 (1).
- HORNUNG, Gerrit y SCHNABEL Christoph (2009). Data protection in Germany II: Recent decisions on online-searching of computers, automatic number plate recognition and data retention. *Computer Law & Security Report*. Vol. 25 (2).

- HOWARD, Philip; KOLLANYI, Bence, BRADSHAW, Samantha; NEUDERT, Lisa-Maria (2018). *Social Media, News and Political Information during the US Election: Was Polarizing Content Concentrated in Swing States?* Project on Computational Propaganda. University of Oxford.
- ILLADES, Esteban (2018). *Fake news. La nueva realidad*. Grijalbo.
- JACOBS, James B. y LARRAURI, Elena (2010). ¿Son las sentencias públicas? ¿Son los antecedentes penales privados? Una comparación de la cultura jurídica de Estados Unidos y España. *Revista InDret*. Barcelona.
- KAPLAN, Daniel (2010). *Informatique, libertés, identité*. Éditions Fyp.
- KERSCH, Ken I. (2003). *Freedom of speech. Rights and liberties under the law*. ABC-Clio.
- KOOPS, Bert-Jaap (2008). *Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice*. Tilburg Law School. Países Bajos.
- KREBS, Brian (2008). *Court Rules Against Teacher in MySpace 'Drunken Pirate' Case*. Blog Security Fix. Washington Post.
- LE MASURIER, Megan (2015). What is slow journalism? *Journalism Practice*. Vol. 9.
- LEVIN, Sam (2018). "They don't care": Facebook factchecking in disarray as journalists push to cut ties. *The Guardian*.
- LI, Qing (2006). Cyberbullying in schools: A research of gender differences. *School Psychology International* nº27.
- LÓPEZ GARCÍA, Xosé (2000). Los medios tradicionales en los nuevos escenarios de la comunicación. *Revista Latina de la Comunicación Social* nº32.

- LÓPEZ PORTAS, María Begoña (2015). La configuración jurídica del derecho al olvido en el derecho español a tenor de la doctrina del TJUE. *Revista de Derecho Político* nº93. UNED.
- LUCENA CID, Isabel Victoria (2014). *El concepto de la intimidad en los nuevos contextos tecnológicos*. Tirant lo Blanch. Valencia.
- MACÍAS CASTILLO, Agustín (2010). Concepto de información veraz cuando se produce colisión entre el derecho a la información y el derecho al honor. *Actualidad Civil* nº20.
- MANNION, Damon (2019). *Fabula AI announces breakthrough in algorithmic fake news detection*.
- MARTÍNEZ LÓPEZ-SÁEZ, Mónica (2017). Los nuevos límites al derecho al olvido en el sistema jurídico de la Unión Europea: la difícil conciliación entre las libertades económicas y la protección de datos personales. *Estudios de Deusto*. Vol. 65, nº 2.
- MARTÍNEZ MARTÍNEZ, Ricard (2014). Privacidad Estados Unidos y España. Tan lejos, tan cerca. *Revista TELOS* (Cuadernos de Comunicación e Innovación) nº97. Fundación Telefónica, febrero-mayo.
- MARTÍNEZ OTERO, Juan María (2015). El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs. AEPD y Mario Costeja. *Revista de Derecho Político* nº93. UNED.
- MARTÍNEZ OTERO, Juan María (2016). Derechos fundamentales y publicación de imágenes ajenas en las redes sociales sin consentimiento. *Revista Española de Derecho Constitucional* nº106.
- MASON, Kimberly L. (2008). Cyberbullying: A preliminary assessment for school personnel. *Psychology in the School*. Vol. 45, nº4.

- MATA y MARTÍN, Ricardo (2006). La protección penal de datos como tutela de la intimidad de las personas. Intimidad y nuevas tecnologías. *Revista Penal* n°18, julio.
- MAYER-SCHÖNBERGER, Viktor (2009). *Delete: The virtue of forgetting in the digital Age*. Princeton University Press.
- MAYER-SCHÖNBERGER, Viktor (2014). *Omission of search results is not a 'right to be forgotten' or the end of Google*.
- McLUHAN, Marshall (1962). *The Gutenberg Galaxy: The Making of Typographic Man*. University of Toronto Press.
- McLUHAN, Marshall (1964). *Understanding Media: The Extensions of Man*. McGraw-Hill. New York.
- MEZZANOTTE Massimiliano (2009). *Il diritto all'oblio. Contributo allo studio della privacy storica*. Edizioni Scientifiche Italiane.
- MESTRE VÁZQUEZ, José Miguel (2010). La protección de potenciales trabajadores en los procesos de selección: Incidencia de las redes sociales. *Capital Humano* n°248, noviembre.
- MIERES MIERES, Luis Javier (2002). *Intimidación personal y familiar. Prontuario de Jurisprudencia Constitucional*. Editorial Aranzadi. Navarra.
- MIERES MIERES, Luis Javier (2014). *El derecho al olvido digital*. Fundación Alternativas.
- MILL, John Stuart (1948). *On liberty and considerations on representative government*. McCallum.
- MILLER, Arthur R. (1971). *The Assault on Privacy: Computers, Data Banks, and Dossiers*. University of Michigan Press.

- MINERO ALEJANDRE, Gemma (2014). A vueltas con el “derecho al olvido”. Construcción normativa y jurisprudencia del derecho de protección de datos de carácter personal en el entorno digital. *Revista Jurídica* nº30. Universidad Autónoma de Madrid. Dykinson.
- MINERO ALEJANDRE, Gemma (2017). Presente y futuro de la protección de datos personales. Análisis normativo y jurisprudencial desde una perspectiva nacional y europea. *Anuario jurídico y económico escurialense* nº50.
- MIRÓ LLINARES, Fernando (2011). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. *Revista Electrónica de Ciencia Penal y Criminología* nº 13-07.
- MITCHELL, William (2003). *Me++: The Cyborg Self and the Networked City*. Cambridge. The MIT Press.
- MONTANO, Pedro (2018). Fake news y libertad de expresión. *Revista Hacer Empresa*, junio. Montevideo.
- MORENO BOBADILLA, Ángela (2019). El derecho al olvido digital: una brecha entre Europa y Estados Unidos. *Revista de comunicación* nº18 (1).
- MUÑOZ, Joaquín (2014). El llamado «derecho al olvido» y la responsabilidad de los buscadores. Comentario a la sentencia del TJUE de 13 de mayo 2014. *Diario La Ley* nº 8.317.
- MURILLO DE LA CUEVA, Pablo Lucas (2006). *El derecho a la libertad informática*. Documentos TICs (Derecho de las Tecnologías de la Información y Comunicación).

- MURILLO DE LA CUEVA, Pablo Lucas (2008). El derecho a la autodeterminación informativa y la protección de datos personales. *Azpilcueta: Cuadernos de Derecho* nº20.
- NOVAL LLAMAS, Joaquín José (2012). Algunas consideraciones sobre la futura regulación del Derecho al olvido. *Revista de la contratación electrónica* nº120. Octubre-diciembre.
- OLLERO, Daniel (2018). *Quemados hasta la muerte entre aplausos por un bulo de Whatsapp que les acusaba de robar órganos a niños*. El Mundo.
- ORDÓÑEZ SOLÍS, David (2014). El Derecho al olvido en internet y la Sentencia Google Spain. *Unión Europea Aranzadi* nº6.
- ORIHUELA, José Luis (2002). Internet: nuevos paradigmas de la comunicación. *Chasqui: Revista Latinoamericana de Comunicación* nº77.
- ORZA LINARES, Ramón María y RUÍZ TARRÍAS, Susana (2011). *El derecho al olvido en Internet*. Huygens Editorial.
- ORZA LINARES, Ramón María (2012). Derechos Fundamentales e Internet: Nuevos problemas, nuevos retos. *Revista de Derecho Constitucional Europeo* nº18, julio-diciembre.
- PAUNER, Cristina (2018). Noticias falsas y libertad de expresión e información. El control de los contenidos informativos en la red. *Teoría y Realidad Constitucional* nº41. UNED.
- PAZOS CASTRO, Ricardo (2015). El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, ¿una relación imposible? *Revista InDret*.
- PAZOS CASTRO, Ricardo (2016). El derecho al olvido frente a los editores de hemerotecas digitales. *Revista InDret*. Barcelona.

- PELTZ-STEELE, Richard J. (2013). The new american privacy. *Georgetown journal of international law*. Vol. 44.
- PENNINGTON, Natalie (2013). You don't De-friend the Dead: An Analysis of Grief Communication by College Students Through Facebook Profiles. *Death Studies*. Vol. 37, nº7.
- PÉREZ-ROSAS, Verónica, KLEINBERG, Bennett, LEFEVRE, Alexandra, y MIHALCEA, Rada (2018). *Automatic detection of fake news*. Actas de la 27ª Conferencia Internacional de Lingüística Computacional. Santa Fe (Nuevo México).
- PIÑAR MAÑAS, José Luis (dir.) (2017). *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*. Editorial Reus.
- PIÑAR MAÑAS, José Luis (2018). *El derecho al olvido y las hemerotecas digitales*. Consejo General de la Abogacía Española.
- PLATERO ALCÓN, Alejandro (2016). El derecho al olvido en Internet. El fenómeno de los motores de búsqueda. *Revista Opinión Jurídica*. Vol. 15, nº 29.
- PRENSKY, Marc (2001). Digital natives, digital immigrants. *MCB University Press*. Vol. 9, nº5.
- PROSSER, William L. (1960). Privacy. *California Law Review*. Vol. 48, nº3.
- PUCCINELLI, Óscar (2012). El "derecho al olvido" en el derecho de la protección de datos. El caso argentino. *Revista Internacional de Protección de Datos* nº1, julio-diciembre. Universidad de los Andes.
- QUILEZ AGREDA, Ernesto (2000). *El Derecho a la protección de datos en la jurisprudencia constitucional*. III Jornadas sobre informática y sociedad. Facultad de Derecho Comillas.

- QUILLET, Etienne (2011). *Le droit à l'oubli numérique sur les réseaux sociaux*. Université Panthéon-Assas.
- RALLO LOMBARTE, Artemi (2010). El Derecho al olvido y su protección. *Revista TELOS* (Cuadernos de Comunicación e Innovación) nº 85, octubre-diciembre. Madrid.
- RALLO LOMBARTE, Artemi y MARTÍNEZ MARTÍNEZ, Ricard (2011). Protección de datos personales y redes sociales: obligaciones para los medios de comunicación. *Quaderns del CAC*. Vol. XIV (2), diciembre.
- RALLO LOMBARTE, Artemi (2014). *El derecho al olvido en Internet. Google versus España*. Centro de Estudios Políticos y Constitucionales.
- RALLO LOMBARTE, Artemi (2015). *El debate europeo sobre el derecho al olvido en internet*. Capítulo extraído de *Hacia un nuevo derecho de protección de datos*. Tirant lo Blanch. Valencia.
- RID, Thomas (2017). *Disinformation. A primer in russian active measures and influence campaigns*. Texto presentado durante el 115º Congreso del Comité de Inteligencia del Senado de los Estados Unidos, celebrado el 30 de marzo.
- RINI, Regina. Fake news and partisan epistemology. *Kennedy Institute of Ethics Journal*, nº 27. Special Issue: Trump and the 2016 election, págs. 43-64.
- RIZO GARCÍA, Marta (2003). *Redes. Una aproximación al concepto*. Consejo Nacional para la Cultura y las Artes (Conaculta). México.
- ROMEO CASABONA, Carlos María (2005). *Los delitos de descubrimiento y revelación de secretos*. Tirant lo Blanch. Valencia.
- ROMEO CASABONA, Carlos María (2006) (coord.). *El cibercrimen: nuevos retos jurídico-penales, nuevas respuestas político-criminales*. Comares. Granada.

- ROSEN, Jeffrey (2010). *The Web Means the End of Forgetting*. The New York Times.
- ROSEN, Jeffrey. (2012). The right to be forgotten. *Stanford Law Review*. Vol. 64.
- ROUVROY, Antoinette (2008). *Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?* University of Namur. Bélgica.
- RUIZ MARCO, Francisco (2001). *Los delitos contra la intimidad. Especial referencia a los ataques cometidos a través de la informática*. Colex. Madrid.
- RUIZ MIGUEL, Carlos (1994). *El derecho a la protección de la vida privada en la jurisprudencia del Tribunal Europeo de Derechos Humanos*. Civitas, Madrid.
- NEUMAN, W. RUSSELL (1991). *The future of the Mass Audience*. Cambridge University Press.
- SALDAÑA DÍAZ, María Nieves (2007). La protección de la privacidad en la sociedad tecnológica: El derecho constitucional a la privacidad de la información personal en los Estados Unidos. *Revista Iberoamericana de Filosofía, Política y Humanidades* nº18.
- SALDAÑA DÍAZ, María Nieves (2012). The right to privacy. La génesis de la protección de la privacidad en el sistema constitucional norteamericano: el centenario legado de Warren y Brandeis. *Revista de Derecho Político* nº85. UNED.
- SALVADOR CODERCH, Pablo (1987). *¿Qué es difamar? Libelo contra la Ley del Libelo*. Civitas. Madrid.
- SALVADOR CODERCH, Pablo y GÓMEZ POMAR, Fernando (2002). *Libertad de expresión y conflicto institucional. Cinco estudios sobre la aplicación judicial de los derechos al honor, intimidad y propia imagen*. Civitas.

- SÁNCHEZ DE DIEGO FERNÁNDEZ DE LA RIVA, Manuel (2010). De la libertad de expresión al derecho de acceso a la información pública. *Comunicación y pluralismo* nº9.
- SÁNCHEZ GARCÍA, Raquel (2002). La propiedad intelectual en la España contemporánea, 1847-1936. *Revista Hispania LXII*, nº212, págs. 993-1020.
- SCHOEMAN, Ferdinand David (1992). *Privacy and social freedom*. Cambridge University Press.
- SEISDEDOS POTES, Víctor (2014). Derecho al olvido. Jaque a Google en Europa. *Cuadernos de Dereito Actual* nº2.
- SELIGRAT GONZÁLEZ, Víctor Manuel (2015). El derecho al olvido digital. Problemas de configuración jurídica y derivados de su incumplimiento a la vista de la STS de 15 de octubre de 2015. *Actualidad Civil* nº12. Editorial La Ley. Diciembre.
- SERRANO MAÍLLO, Isabel (2011). El Derecho a la libertad de expresión en la jurisprudencia del Tribunal Europeo de Derechos Humanos: Dos casos españoles. *Teoría y Realidad Constitucional* nº28. UNED.
- SHORE, Jennifer y STEINMAN, Jill (2015). *Did You Really Agree to That? The Evolution of Facebook's Privacy Policy*. Universidad de Harvard.
- SIMÓN CASTELLANO, Pere (2011). *El Régimen Constitucional del Derecho al olvido en Internet en Neutralidad de la red y otros retos para el futuro de Internet*. Actas del VII Congreso Internacional Internet, Derecho y Política. Universitat Oberta de Catalunya. Huygens Editorial.
- SIMÓN CASTELLANO, Pere (2012). *El régimen constitucional del derecho al olvido digital*. Tirant lo Blanch. Valencia.
- SIMÓN CASTELLANO, Pere (2012). El derecho al olvido en el universo 2.0. *Textos universitaris de biblioteconomia i documentació* nº28. Universitat de Barcelona.

- SIMÓN CASTELLANO, Pere (2015). *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*. Bosch.
- SLONJE, Robert y SMITH, Peter (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology*. Vol. 49.
- SOLOVE, Daniel J. (2007). *The future of reputation: Gossip, rumor, and privacy on the Internet*. Yale University Press.
- SOLOVE, Daniel J. (2009). *Understanding Privacy*. Harvard University Press.
- STRATE, Lance (2012). El medio y el mensaje de McLuhan: La tecnología, extensión y amputación del ser humano. *Infoamérica: Iberoamerican Communication Review* nº7.
- STOKES, Patrick (2011). Ghosts in the Machine: Do the Dead Live on in Facebook? *Philosophy & Technology*. Vol. 25, nº3.
- SUÁREZ SÁNCHEZ-OCAÑA, Alejandro (2012). *Desnudando a Google. La inquietante realidad que no quieren que conozcas*. Deusto.
- SUÁREZ VILLEGAS, Juan Carlos y CRUZ ÁLVAREZ, Jesús (2013). *Problemas éticos de la instantaneidad informativa en el entorno digital*. I Congreso Internacional de Comunicación y Sociedad Digital. Logroño.
- SUCH MARTÍNEZ, Javier (2016). La prescripción y la caducidad en derecho administrativo. Dos instituciones vinculadas al espacio temporal del comienzo y finalización del procedimiento. *Economist & Jurist*. Vol. 24, nº199.
- SUNSTEIN, Cass (1993). *Democracy and the problema of free speech*. The Free Press. Nueva York.

- SUNSTEIN, Cass (2001). *Republic.com*. Princeton University Press.
- TELLO-DÍAZ, Lucía (2013). Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook. *Revista Comunicar*. Vol. XXI, nº41.
- TERRE, Francois (2002). *Libertés et droits fondamentaux*. Éditions Dalloz.
- TERUEL LOZANO, Germán (2010). *La libertad de expresión en Internet y sus garantías constitucionales en el control de contenidos de páginas web*. Magister Iuris Constitutionalis.
- TERUEL LOZANO, Germán (2010). Apuntes generales sobre la libertad de expresión en Internet. *Anales de Derecho*. Vol. 28.
- TORRES MANRIQUE, Jorge Isaac (2018). Analizando el derecho fundamental al olvido a propósito de su reciente reconocimiento y evolución. *Revista general de derecho constitucional* nº27.
- TORRES SORIANO, Manuel (2017). Hackeando la democracia: operaciones de influencia en el ciberespacio. *Revista Instituto Español de Estudios Estratégicos (IEEE)*, junio.
- TOURIÑO, Alejandro (2014). *El derecho al olvido y a la intimidad en Internet*. Los Libros de la Catarata. Madrid.
- TRONCOSO REIJADA, Antonio (dir.) (2010). *Comentario a la Ley Orgánica de Protección de Datos Personales*. Thomsom-Civitas.
- URÍAS, Joaquín (2003). *Lecciones de derecho de la información*. Tecnos. Madrid.
- URIONDO DE MARTINOLI, Amalia (2013). Difamación a través de Internet. Vacío legal argentino. *Anuario Hispano-luso-americano de derecho Internacional* nº21.

- VALERO TORRIJOS, Julián (2013). *La protección de los datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*. Thomson Reuters-Aranzadi.
- VILASAU SOLANA, Mónica (2014). El caso Google Spain: la afirmación del buscador como responsable del tratamiento y el reconocimiento del derecho al olvido (análisis de la STJUE de 13 de mayo de 2014). *Revista de Internet, Derecho y Política* nº18, junio.
- VILLAVERDE MENÉNDEZ, Ignacio (1994). Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993. *Revista española de Derecho Constitucional* nº41.
- VILLAVERDE MENÉNDEZ, Ignacio (1998). Esbozo de una teoría general de los derechos fundamentales. *Revista jurídica de Asturias* nº22.
- VILLAVERDE MENÉNDEZ, I. (2006). *La jurisprudencia del Tribunal Constitucional sobre el derecho fundamental a la protección de datos personales*. Editorial Cinca. Colección Estudios Laborales.
- VILLAVERDE MENÉNDEZ, Ignacio (2007). Ciberconstitucionalismo. Las TIC y los espacios virtuales de los derechos fundamentales. *Revista catalana de Dret Públic* nº35.
- VILLAVERDE MENÉNDEZ, Ignacio (2012). A propósito de la reciente jurisprudencia del Tribunal Constitucional sobre el empleo de “cámaras ocultas”. *Revista Derecom* nº13.
- VILLAVERDE MENÉNDEZ, Ignacio (2013). La intimidad, ese “terrible derecho” en la era de la confusa publicidad virtual. *Espaço Jurídico Journal of Law*. Vol 14, nº3, págs. 57-72.
- VOSOUGHI, Soroush; ROY, Deb; y ARAL, Sinan (2018). The spread of true and false news online. *Science*. Vol. 359, págs. 1146-1151.

- VV.AA. (2010). *Factbook: Protección de Datos Personales*. Aranzadi. Madrid.
- VV.AA. (2016). Procesos de reclutamiento y las redes sociales. *Revista Iberoamericana para la Investigación y el Desarrollo Educativo*. Vol. 6, nº12.
- WARREN, Samuel y BRANDEIS, Louis (1890). The right to privacy. *Harvard Law Review*. Boston. Traducido al español por Civitas (1995): *El derecho a la intimidad*.
- WESTIN, Alan (1967). *Privacy and freedom*. Atheneum. New York.
- WÖLFFLIN, Heinrich (1915). *Kunstgeschichtliche Grundbegriffe*. Traducido al español por Espasa-Calpe (2007): *Conceptos fundamentales de la Historia del Arte*.
- YANES MESA, Rafael (2007). La comunicación política y los nuevos medios de comunicación personalizada. *Revista Internacional de Comunicación* nº16.
- YBARRA, Michele L. y MITCHELL, Kimberly J. (2004). Online aggressor / targets, aggressors, and targets: a comparison of associated youth characteristics. *Journal of Child Psychology and Psychiatry* nº45.
- YOUM, Kyu y PARK, Ahran (2016). The right to be forgotten in european union law: data protection balanced with free speech? *Journalism and Mass Communication Quarterly*. Vol. 93 (2).
- ZÁRATE ROJAS, Sebastián (2013). La problemática entre el derecho al olvido y la libertad de prensa. *Revista Derecom* nº13.