TESIS DOCTORAL

EL DERECHO AL OLVIDO EN EL *BIG DATA*: NUEVOS RETOS PARA LA PROTECCIÓN DE LA PRIVACIDAD

Presentada por:

Marina Sancho López

Dirigida por:

Prof. Dr. Javier Plaza Penadés

Departamento de Derecho civil, Universitat de València

Programa de Doctorado:

Derechos Humanos, Democracia y Justicia Internacional

Instituto de Derechos Humanos, Facultad de Derecho

Universitat de València

València, Septiembre 2018

La presente tesis doctoral se ha realizado en el marco de una beca para personal investigador en formación (PIF) dentro del proyecto GVA-PROMETEO II 2015-014 "Derecho Civil Valenciano y Europeo, CPI-15-400" de la Conselleria d'Educació, Investigació, Cultura i Esport, de la Generalitat Valenciana.

Para la elaboración de esta tesis doctoral ha sido de especial importancia la realización de estancias de investigación. En concreto, una estancia de investigación de 3 meses en el *Max-Planck-Institut für ausländisches und internationales Privatrecht* en Hamburgo (Alemania), en el período 29.03.2017-30.06.2017, bajo la supervisión de Frau Halsen-Raffel, así como una estancia de 1 mes en la Facultad de Derecho de la Universidad de Cambridge (Reino Unido), en el período 25.01.2018-27.02.2018, bajo la supervisión del Prof. Dr. David Erdos, *Senior Lecturer* en Derecho por la Universidad de Cambridge y *Deputy Director, Centre for Intellectual Property and Information Law* (*CIPIL)*. Todas estas estancias han sido subvencionadas por organismos públicos dependientes de la Conselleria d'Educació, Investigació, Cultura i Esport, de la Generalitat Valenciana.

GENERALITAT VALENCIANA
Conselleria d'Educació, Investigació, Cultura i Esport

Shot by a security camera
You can't watch your own image
And also look yourself in the eye

Black mirror, black mirror, black mirror
I know a time is coming
All words will lose their meaning
Please show me something that isn't mine
But mine is the only kind that I relate to

Arcade Fire, Black Mirror.

Neon Bible, 2007.

AGRADECIMIENTOS

Debo empezar agradeciéndole a mi Director, Javier Plaza Penadés, la confianza que depositó en mí sin haber sido alumna suya, así como la gran autonomía que me ha concedido en la investigación, siempre dispuesto a aceptar mis propuestas por muy complejas o heterodoxas que fueran. A día de hoy creo que sigue sin ser consciente de la gran puerta que me abrió su proyecto y de cuanto he disfrutado esta incursión académica. Valgan estas palabras para remediarlo.

Hago extensible mi agradecimiento a las compañeras y compañeros del Departamento de Derecho civil de la UV que me han ayudado de diversas formas en este camino, así como a todas aquellas personas que, sin pretenderlo, con una conversación entre pasillos o una broma, han roto la soledad del estudio y me han hecho sentir bienvenida.

Agradecer también al Prof. Javier Palao Gil, cuyas provocativas clases originaron en mí esta vocación, por la dignidad con la que reivindica la enseñanza universitaria. De él he aprendido que el rigor científico no está reñido con el sentido del humor, así como que la incorrección política a veces es el mejor de los caminos.

En el terreny més personal, a Maria i a Josep, la preocupació dels quals ha estat sempre la prevalença de la meua felicitat, per donar-me contínuament la llibertat necessària per tal de prendre les meues pròpies decisions, equivocades o no. Ací, la prova que tot s'acaba resolent.

A la meua família més disfuncional: amigues i amics, per fer-me riure, donar-me suport i estimar sense condicions. Als de la terreta i als que estan arreu del món, buscant-se la vida o perseguint somnis.

A tu, Jorge, que has patit aquesta tesi com si fóra pròpia, per l'agost més llarg i estranyament divertit que recorde, perquè ens ha costat Déu i ajuda arribar fins ací.

ABREVIATURAS UTILIZADAS

AEPD	Agencia española de protección de datos
AN	Audiencia nacional
Art.	Artículo
BCR	Binding Corporate Rules
Cap.	Capítulo
CDFUE	Carta Derechos Fundamentales Unión Europea
CC	Código Civil
CE	Constitución española
Cfr.	Confer
CEDH	Convenio Europeo de Derechos Humanos
CP	Código penal
Dir.	Director
DPA	Data Protection Act
Ed.	Editor
FIES	Ficheros de Internos de Especial Seguimiento
FJ	Fundamento Jurídico
GDPR	General Data Protection Regulation
GT29	Grupo de Trabajo del Artículo 29

HRA	Human Rights Act
ICO	Information Comissioner Officer
LEC	Ley de Enjuiciamiento Civil
LODR	Ley Orgánica 2/1984, de 26 de marzo, sobre el derecho de rectificación
LOPD	Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal
LOPDH	Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, la intimidad personal y familiar y la propia imagen
LOPJ	Ley Orgánica del Poder Judicial
LORTAD	Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter persona
nº	Número
Ob. cit.	Obra Citada
p./pp.	Página/Páginas
para.	Párrafo
PIA	Privacy Impact Assessments
RLOPD	Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 5/1992, de 29 de octubre, de

	regulación del tratamiento automatizado de los datos de carácter personal
RP	Reglamento Penitenciario
ss.	Siguientes
SAP	Sentencia Audiencia Provincial
SAN	Sentencia Audiencia Nacional
STC	Sentencia Tribunal Constitucional
STJUE	Sentencia Tribunal Justicia Unión Europea
STS	Sentencia Tribunal Supremo
TEDH	Tribunal Europeo de Derechos Humanos
TC	Tribunal Constitucional
TJUE	Tribunal Europeo de Justicia de la Unión Europea
TFUE	Tratado Funcionamiento de la Unión Europea
TS	Tribunal Supremo
TUE	Tratado de la Unión Europea
UE	Unión Europea
v.	Versus
Vid.	Vide (véase)
Vol.	Volumen

SUMARIO

ÍNDICE

INTRODUCCIÓN

Esta tesis doctoral constituye un estudio sobre el desarrollo del derecho al olvido digital como derecho fundamental. Para ello, se ha presentado una aproximación doctrinal y jursprudencial a este derecho de nueva generación, con la finalidad de elaborar una caracterización, tanto en términos formales como materiales, que permita exponer el estatus legal del derecho al olvido como derecho fundamental.

Para la realización de la investigación, se parte de dos premisas: en primer lugar, la importancia del *Big data* como proceso integrante de la revolución digital, fenómeno de cambio transversal que ha venido a redefinir los códigos, usos y formas de interacción social propios de la *posmodernidad*. En segundo lugar, como esta dinámica de transformación social afecta necesariamente al ámbito jurídico, especialmente en lo relativo al entendimiento tradicional de conceptos como intimidad o vida privada. Por ello, se ha considerado necesario repensar el significado de la privacidad, entendida como esfera personal del sujeto, para así desarrollar los presupuestos estructurales sobre los que este trabajo pueda adoptar una voluntad propositiva respecto de la caracterización del derecho al olvido digital como derecho fundamental.

En este sentido, las premisas metodológicas empleadas en este trabajo se construyen a partir de la integración del derecho al olvido como respuesta a las necesidades evolutivas que acontecen en el contexto del *Big data* respecto de la protección de la privacidad, partiendo de la realidad material como presupuesto necesario para formular postulados jurídicos. Sobre dicha cuestión, esta tesis doctoral ofrece una conexión entre ambos fenómenos, reconociendo la importancia del derecho al olvido como derecho fundamental, en tanto que supone una respuesta desde el ámbito de las normas jurídicas a las nuevas condiciones sociales determinadas por el tratamiento de los datos masivos. En consecuencia, el desarrollo del marco de referencia de este trabajo parte de la adecuación de la protección de la privacidad a un nuevo estado de cosas: el propio de la *posmodernidad* y la sociedad líquida derivada de las nuevas

formas de interacción social propias del *Big data*. Así las cosas, la metodología utilizada se ha basado en considerar la necesidad de desarrollar el estatus legal de derecho fundamental propio del derecho al olvido, para dar así una respuesta desde el ordenamiento jurídico a este contexto de cambio social.

Como puede apreciarse, la investigación tiene un objeto de estudio cuya naturaleza jurídica es innegablemente multidisciplinar, pues abarca una diversidad de ramas jurídicas que coexisten en plena armonía.

Es cierto que, según la diferenciación clásica entre materias y doctrinas de la tradición jurídica continental, la perspectiva de este trabajo puede sorprender ya que no responde a la rígida lógica a la que venimos acostumbrados. Así, el tratamiento del objeto de estudio, si bien apriorísticamente puede resultar un tanto heterodoxo, se justifica a partir de un examen en profundidad de la cuestión, el cual deja en evidencia la necesidad de estudiar la misma desde distintas perspectivas jurídicas cuyas raíces se encuentran en constante conexión.

En consecuencia, a lo largo de la presente disertación encontraremos elementos de Derecho constitucional, Derecho privado, Filosofía del Derecho, Derecho penal, Derecho comunitario, Derecho internacional y hasta ciertos aspectos de Derecho mercantil, cuyas nociones resultan tangenciales al objeto de estudio y que se integran plenamente en la argumentación elaborada.

Este carácter multidisciplinar desde el punto de vista de las ciencias jurídicas se explica, fundamentalmente, por dos razones. En primer lugar, porque el campo de las nuevas tecnologías en el contexto de la revolución digital, donde se manifiesta el surgimiento del tratamiento y análisis de datos masivos conocido como *Big data*, obligan necesariamente a repensar las estructuras jurídicas vigentes y sus mecanismos de protección, que rápidamente se han visto superados por un fenómeno de tal globalización que ha afectado nociones tan tradicionales como “Estado” o “jurisdicción”.

En segundo lugar, y más particularmente en relación con el derecho al olvido, porque se trata de una cuestión de derechos fundamentales que, ciertamente, operan de modo transversal

sobre el conjunto del ordenamiento jurídico sin que puedan ser ignorados por ninguna rama jurídica pues, asimismo, derivan del propio significado del Estado social y democrático de Derecho en el cual se insertan. En este sentido, la necesidad de repensar el concepto de privacidad, a partir de la *refundamentación* que se desarrollará en este trabajo, entronca con las propias necesidades evolutivas de dicha configuración estatal puesto que, para la salvaguarda de los derechos y libertades de la ciudadanía, es necesaria una protección integral de la privacidad, dado que ésta se presenta como una condición material para el propio ejercicio de la libertad.

De acuerdo con este último aspecto, puede hacerse especial mención al ensamblaje entre el Derecho civil –área en la cual se ha elaborado la presente tesis doctoral– encargado del estudio de la esfera personal de privacidad de la ciudadanía (como representan los derechos de la personalidad), en relación con el estudio de los Derechos fundamentales. Esto es así porque en esta categoría se inserta el derecho al olvido, cuyo contenido resulta habitualmente ubicado en otras disciplinas jurídicas, más cercanas a la Filosofía del Derecho o el Derecho constitucional.

En la actualidad, y pese a lo que puedan defender algunos autores, el Derecho civil no es un sector independiente del ordenamiento jurídico, sino que debe interpretarse a tenor de lo dispuesto en la Constitución, que establece las reglas del juego y, entre ellas, dispone cual es la conciencia social de cada época, por lo que el Derecho privado no puede mantenerse alejado de su evolución. Así, el Derecho civil es el encargado de dotar de contenido al derecho al olvido, siguiendo la estructura de los derechos subjetivos, delimitando así un sujeto, un objeto, un contenido y unos límites dentro de dicha figura jurídica.

Si bien es cierto que el Derecho civil ha sido reiteradamente garante de los derechos y las libertades más fundamentales, a través de los llamados "derechos de la personalidad", se ha caracterizado por su capacidad de adaptación (un ejemplo de ello se encuentra en el propio Código Civil, cuya vigencia data de 1889), pues tradicionalmente ha sabido adecuar sus postulados al orden político y social cambiante. En este sentido, no puede defenderse su

carácter autosuficiente pues no resulta ajeno al sistema constitucional de derechos fundamentales, frente al cual resulta del todo permeable.

Así, la autonomía de la voluntad recogida en el artículo 1.255 del Código Civil no puede entenderse sino en los términos del artículo 10 de la Constitución española y el Derecho fundamental a la libertad personal, que no permite interpretación alguna que carezca de fundamento. Al contrario, los fueros de la libertad y la autonomía individual que inspiran el Derecho civil han de mantenerse intactos -en los términos de la propia doctrina civilista- en la medida en que dichos fueros son, eminentemente, la concreción de un Derecho fundamental de libertad íntimamente relacionado con la dignidad personal y el libre desarrollo de la personalidad.

De acuerdo con lo expuesto, el **Capítulo I** de este trabajo, titulado "**La influencia del *Big data* en el ordenamiento jurídico: una aproximación multidisciplinar**", supone el desarrollo de los presupuestos políticos y metodológicos de los que parte esta investigación. Con esta finalidad, se analizará desde una perspectiva transversal la influencia del *Big data* en el ordenamiento jurídico, a partir del marco de referencia de lo que se ha denominado como "modernidad líquida".

Por lo que respecta a los **presupuestos políticos del estudio**, se abordará de qué manera afecta al disfrute de los derechos y libertades del ciudadano la posición de preeminencia adoptada por el *Big data* en el medio social, así como su marcada orientación por la lógica matemática derivada del calculo algorítmico. Sobre esta cuestión, será especialmente debatida la supuesta neutralidad técnica de esta herramienta, discutiendo si efectivamente se le puede atribuir dicha posición de imparcialidad o, si por el contrario la vida basada en el algoritmo supone un determinismo incompatible con el libre desarrollo de la personalidad.

Sobre esta cuestión, será puesta de relevancia la posibilidad de que la generalización del cálculo algorítmico como presupuesto estructural del contexto *Big data* pueda suponer la creación de situaciones de discriminación de distinta índole en el medio social, originando espacios de exclusión o segmentación que puedan ser contrarias al reconocimiento de

principios básicos como la igualdad o la dignidad de la persona, viéndose estas vulneraciones especialmente conectadas con la protección jurídica de la intimidad o la vida privada. Así las cosas, en estos primeros puntos se discutirán los principios inspiradores del *Big data*, así como su recepción por el medio social, como estadio previo a su consideración por parte del ordenamiento jurídico.

Seguidamente, cabrá considerar la influencia del *Big data* en la creación de una nueva cultura de la vigilancia, lo que se ha denominado como *Dataveillance*. En este sentido, se estudiarán los nuevos espacios de control social originados por lo que se ha definido como *sociedad de la exposición* o *sociedad de la transparencia*, en tanto que se trata de cuestiones correlativas al *Big data*, que han supuesto una reorientación de las prácticas de control y vigilancia propias de los sistemas de control social formal, analizando cuestiones puntuales del ordenamiento jurídico español donde pueda observarse dicho fenómeno, como representa el supuesto de la criminalización de los delitos de opinión y los nuevos límites a la libertad de expresión en la era digital.

Iniciando la conexión de los presupuestos políticos de este trabajo con los presupuestos metodológicos, se expondrá la desnaturalización de la protección jurídica de la intimidad y la vida privada en el contexto del *Big data*, como consecuencia de la mercantilización de los datos personales en este marco de referencia. En este sentido, se analizará la lógica economicista que orienta el estándar de garantía de la privacidad en el ámbito digital, así como la pérdida de control sobre los datos personales que la ciudadanía ha experimentado a consecuencia del valor monetario atribuido a la información personal por las propias corporaciones que prestan sus servicios en la plataforma digital (señalando el caso de la red social *Facebook*), o por los terceros interesados en convertir en objeto de comercio los datos personales, como muestra la actividad de los llamados *data brokers*.

Pasando a los **presupuestos metodológicos** de esta tesis doctoral, éstos parten de la necesidad de repensar el concepto de privacidad, en tanto que del contexto propio del *Big data* se han derivado una serie de riesgos que ponen en duda la suficiencia de los estándares actuales de protección jurídica de la intimidad y la vida privada para enfrentarse a los nuevos patrones

de la "modernidad líquida". En este sentido, la difusión de los límites entre lo público y lo privado requieren de un nuevo estándar conceptual que efectivamente pueda garantizar el respeto a la esfera personal del sujeto. Para ello, se partirá de una contraposición entre los conceptos de intimidad y privacidad, con la finalidad de construir una noción integradora que supere las limitaciones expuestas, desarrollando así una *refundamentación* de la privacidad que permita adecuar su contenido garantista al contexto *Big data*, y servir así como presupuesto metodológico para la construcción del derecho al olvido como derecho fundamental. De acuerdo con lo expuesto, este derecho de nueva generación será entendido dentro de un concepto más amplio de *garantismo*, donde su ejercicio pueda servir, no únicamente para proteger la privacidad del sujeto que lo invoque, sino también para salvaguardar su propia capacidad para desarrollarse libremente, sin intromisiones de terceros contrarias al principio general de libertad y el concepto de seguridad jurídica.

Para la *refundamentación* del concepto de privacidad propuesto en estas páginas, se partirá de un estudio de Derecho comparado donde se dirigirá la mirada hacia el ámbito jurídico del *common law*, concretamente a la regulación del llamado *right to privacy* en el Reino Unido. Así, el **Capítulo II** de este trabajo llevará por título: "**El concepto de privacidad en el ámbito jurídico del *common law*: desarrollo del *right to privacy* en el Reino Unido**". El estudio de un ordenamiento jurídico propio de la cultura legal anglosajona supone asumir una voluntad integradora, especialmente considerando la tradicional desatención al *common law* por parte de la práctica *iuscomparativa* realizada desde la doctrina continental. En este sentido, el estudio presentado no pretende reconocer en sus instituciones los mismos rasgos inherentes a la cultura legal continental, sino que se realizará un análisis estructural no-discriminatorio de sus conceptos para el enriquecimiento de esta investigación.

Así las cosas, para el desarrollo del concepto de privacidad propuesto en esta tesis doctoral, será especialmente provechoso el estudio del *right to privacy* propio del ordenamiento jurídico británico dado que su desarrollo evolutivo ha permitido reconocer en sus proposiciones una integración de los conceptos de intimidad y vida privada, representando una aproximación

en conexión con la propuesta de este trabajo para el desarrollo del derecho al olvido como derecho fundamental.

En esta tarea, se estudiará el marco normativo británico en torno a la protección de datos personales en toda su extensión, focalizando dicho estudio en la *Data Protection Act 1998* –en vigor durante la realización de la presente disertación- como norma principal en materia sustancial de protección de datos que, siguiendo la estela de su antecesora y pionera *Data Protection Act 1984*, incorpora una garantía integral para la información privada de los ciudadanos, como algo intrínsecamente ligado a la identidad personal y, en definitiva, a la privacidad de los sujetos. Se examinarán así las herramientas jurídicas que proporciona dicha legislación tanto a los particulares como a los órganos jurisdiccionales que, hasta dicho momento, sólo concedían exigua protección a la privacidad a través de las figuras tradicionales del *common law*.

Asimismo, será expuesta la importancia para el desarrollo del *right to privacy* que supone su reconocimiento en el artículo 8 de la *Human Rights Act 1998*, declaración de derechos y libertades incorporada al ordenamiento jurídico británico que traspone de forma directa el contenido del Convenio Europeo de Derechos Humanos. Sobre esta cuestión, puede destacarse la función renovadora desarrollada por este cuerpo normativo, en tanto que establece una serie de criterios prescriptivos para el *case law* en la interpretación de la normativa interna, fundamentados en el respeto a los derechos y libertades del Convenio Europeo de Derechos Humanos y la delimitación que de éstos ha realizado el Tribunal de Estrasburgo.

Por último, teniendo presente el escenario futuro proporcionado por la coyuntura del *Brexit*, se inquirirá sobre el impacto que conllevará la salida de Gran Bretaña de las instituciones comunitarias, en especial, las consecuencias que ello originará sobre las relaciones que tendrán lugar a partir de entonces entre la Unión Europea y el Reino Unido, que podría pasar a considerarse un tercer Estado a efectos de la normativa europea de protección de datos. Partiendo de la conciencia de que se trata de una cuestión abierta aún sin determinar, se llevará a cabo un abanico propositivo teniendo en cuenta los distintos escenarios que podrían sucederse, ofreciendo respuestas encaminadas a mantener una vía cooperativa en la naturaleza

de las relaciones en materia de datos personales entre ambos territorios que, a partir de entonces, tendrán la consideración de "transferencias internacionales". Asimismo, se debatirá si en los últimos años, a consecuencia de los recientes fenómenos económicos y político-sociales acontecidos en el Reino Unido, se ha producido una variabilidad de su estándar de protección de la privacidad, para la cual se examinará la legislación especial dictada en los últimos quince años.

Finalmente, en el **Capítulo III**, titulado "**El desarrollo del derecho al olvido: concepto y principios inspiradores**", será presentada una caracterización del derecho al olvido como derecho fundamental. En este sentido, la aproximación se realizará atendiendo a los presupuestos metodológicos de este trabajo, esto es, la necesidad de *refundamentar* el concepto de privacidad en el contexto *Big data*. De este modo, será posible afirmar la idoneidad del derecho al olvido como estándar de garantía que permita una protección efectiva de las condiciones materiales para el desarrollo de la libre personalidad del sujeto, de ahí su consideración como derecho fundamental de nueva generación.

De forma previa a esta caracterización del derecho al olvido, se presentará una detallada exposición del contexto normativo internacional, comunitario y nacional que sirva como marco de referencia para la apreciación del derecho al olvido digital en España, de estrecha relación con el derecho a la protección de datos personales. De igual modo, serán comentados los *leading cases* en materia jurisprudencial que, desde distintas instancias judiciales (Tribunal de Justicia de la Unión Europea, Tribunal Europeo de Derechos Humanos, Tribunal Constitucional, Tribunal Supremo o Audiencia Nacional) han modelado el desarrollo del derecho al olvido digital desde una perspectiva de *law in action*, esto es, considerando el desarrollo jurisprudencial de su contenido.

La categorización del derecho al olvido propuesta en estas páginas busca responder a la ausencia de un desarrollo integral de su contenido por parte de la doctrina y la jurisprudencia. De este modo, pretende ofrecerse solución a la ausencia de un marco legal concreto que regule la implementación normativa de este nuevo derecho. Para ello, en el tercer capítulo de esta tesis doctoral se establece una caracterización del derecho al olvido siguiendo la estructura clásica

para el desarrollo de los derechos de la personalidad y derechos subjetivos, examinando los aspectos clave para su configuración legal y proponiendo ciertas pautas para su evolución.

Así las cosas, se ofrece un concepto integral al derecho al olvido, partiendo de la *refundamentación* de la privacidad formulada como presupuesto metodológico de la presente investigación. En este sentido, se incorporarán valores jurídicos tales como la propia intimidad y vida privada, pero también el honor, la propia imagen o la protección de datos personales, consecuencia del carácter poliédrico de la privacidad y del derecho al olvido digital.

Asimismo, a efectos de delimitar su contenido, se analizarán los límites inherentes al derecho al olvido que, más allá del principio general de buena fe y la prohibición del abuso de derecho, se centran en la colisión eventual con otros derechos fundamentales, principalmente la libertad de expresión e información. Sobre esta cuestión, se recomendarán los criterios a tener en cuenta por los órganos jurisdiccionales para la resolución de dichos conflictos, a partir del mecanismo de la ponderación, incidiendo en la reciente modificación de la doctrina del Tribunal Constitucional según la cual, se invalida la veracidad como elemento a considerar al tiempo que se incorpora el factor tiempo como ingrediente esencial de dicho examen hermenéutico.

De igual manera, se realizarán diversas reflexiones sobre la titularidad activa del derecho al olvido, así como respecto de su posible ejercicio por las personas jurídicas, sirviéndose de la posición de oligopolio de las corporaciones del *Big data* como presupuesto legitimador para dotar al derecho al olvido de un efecto horizontal, así como de su eficacia en torno a las personas fallecidas. Igualmente, se tratará de confeccionar una argumentación definitiva acerca de la legitimación procesal pasiva de los motores de búsqueda que, si bien fue afirmada por la jurisprudencia europea, ha sido controvertidamente aplicada por los tribunales españoles y ahora parece consolidada en el nuevo marco normativo europeo.

Por lo que respecta a la tutela procesal del derecho al olvido, se proporcionará una panorámica sobre su desarrollo, desde su vertiente administrativa y civil. Sobre esta cuestión, se debatirá la idoneidad de ceder a intereses privados el ejercicio de ponderación respecto de

los intereses en conflicto. De igual modo, se construirá una argumentación que permita aceptar la posibilidad de proteger el derecho al olvido mediante el recurso de amparo ante el Tribunal Constitucional. Igualmente, se incidirá sobre la tutela penal de la esfera de privacidad del sujeto, así como acerca de los mecanismos supranacionales de protección del derecho al olvido digital.

Finalmente, se examinarán algunas cuestiones accesorias, como la diferenciación del derecho al olvido con algunas figuras legales afines o complementarias como el derecho de cancelación, de oposición o de rectificación, y se verificará la capacidad de la responsabilidad extracontractual para el resarcimiento de los daños y perjuicios producidos en la privacidad de los sujetos.

A modo de reflexión final, se incluirán algunas consideraciones críticas que han surgido de manera tangencial a lo largo de este trabajo y en cuyo estudio no se ha podido profundizar por razones de extensión. Se pretende aportar así algunas pinceladas respecto de cuestiones, quizás no estrictamente jurídicas pero íntimamente relacionadas con el objeto de estudio que, se considera, contribuyen a la proyeccióna transversal de la disertación así como enriquecen la discusión llevada a cabo por la presente tesis doctoral.

INTRODUCTION

This doctoral thesis is a study on the development of the right to be digitally forgotten as a fundamental right. To this end, a doctrinal and jurisprudential approach to this new generation right has been presented, with the goal of developing a characterisation, both in formal and material terms, which enables the legal status of the right to be digitally forgotten as a fundamental right to be described.

The carrying out of this study arises from two premises: firstly, the importance of Big Data as an integrating process of the digital revolution, a phenomenon of transversal change that has come to redefine the codes, uses and forms of social interaction typical of *postmodernity*. Secondly, this dynamic of social transformation necessarily affects the legal sphere, especially in relation to the traditional understanding of concepts such as intimacy or private life. Therefore, it is necessary to rethink the meaning of privacy, understood as the personal sphere of the individual, in order to develop the structural assumptions on which this work can adopt a proposal regarding the characterisation of the right to be digitally forgotten as a fundamental right.

In this sense, the methodological foundations of this work are constructed from the integration of the right to be forgotten as an answer to the evolutionary needs of the right to privacy. About this topic, this doctoral thesis develops a connection between both phenomenons, recognising the importance of the right to be forgotten as a fundamental right, given that it supposes the answer from the legal system to the new social conditions consequence of *Big data*. Consequently, the development of the theoretical framework of this work starts from the adaptation of the right to privacy to a new context, of postmodernism itself and liquid society, where social interaction is adapting to *Big data.* In this context, the methodology chosen for this thesis is founded in the need of developing the legal position of the right to be forgotten as a fundamental right, with the purpose of answering from the legal system to this social transformation context.

As can be seen, the research has an object of study whose legal nature is undeniably multidisciplinary, since it covers a variety of legal branches that coexist in complete harmony.

It is true that, according to the classical differentiation between subject areas and doctrines of the continental legal tradition, the treatment of this work may be surprising since it does not respond to the rigid logic to which we are accustomed. However, the treatment of the object of study, which *a priori* may appear somewhat heterodox, is justified from an in-depth examination of the issue, while evidencing the need to study it from different legal perspectives whose roots lie in constant connection.

On this question, throughout this dissertation we will find elements of constitutional law, private law, philosophy of law, criminal law, community law, international law and even certain traces of commercial law, whose notions are tangential to the object of study and that are fully integrated into the presented argument.

This multidisciplinary nature from the point of view of the legal sciences has, fundamentally, two explanations. Firstly, the field of new technologies in the context of the digital revolution, where the treatment and analysis of massive databases known as Big data has emerged, necessarily requires us to rethink the legal structures in force and their mechanisms of protection, which have quickly been overcome by a phenomenon of intense globalisation that has made traditional notions such as "state" or "jurisdiction" obsolete.

Secondly, and more particularly in relation to the right to be digitally forgotten, it is a question of fundamental rights that, assuredly, operate transversally over the entire legal system without being able to be ignored by any branch of law. In addition, they derive from the very meaning of the social and democratic rule of law in which they are inserted. Accordingly, the need to rethink the concept of privacy, from the *refoundation* that will be developed in this work, connects with the evolutionary needs of the social and democratic rule of law itself, since the safeguarding of the rights and freedoms of the public requires the comprehensive protection of privacy, given that it is presented as a material condition for the exercise of freedom itself.

In accordance with this last aspect, special mention may be made of the combination of civil law—the area in which the doctoral thesis has been prepared, involved with the study of the personal sphere of privacy of the public (as represented by the rights related to personal identity)—with the study of fundamental rights. This is because the right to be digitally forgotten is inserted in this latter category, whose content is usually located in other legal disciplines closer to the Philosophy of Law or Constitutional Law.

At present, and despite what some authors have suggested, civil law is not an independent sector of the legal system, but must be interpreted in accordance with the provisions of the Constitution, which determines the rules of the game and, among them, establishes what the social conscience is of each era, so that private law never strays far from its evolution.

While it is true that civil law has repeatedly been the guarantor of the most fundamental rights and freedoms, it has been characterised by its ability to adapt—an example of this is found in the Civil Code itself, in force since 1889—because, traditionally, it has known how to adjust its postulates to the changing political order. Accordingly, once cannot defend its self-sufficient nature since it is not foreign to the constitutional system of fundamental rights, against which it is entirely permeable.

Thus, the autonomy of the will contained in Article 1255 of the Civil Code cannot be understood except in the terms of Article 17 of the Spanish Constitution and the fundamental right to personal freedom, which does not allow any interpretation that lacks foundation. On the contrary, the privileges of freedom and individual autonomy that inspire civil law must remain intact—in terms of the civil law doctrine itself—to the extent that these privileges are, eminently, the realisation of a fundamental right of freedom intimately related to personal dignity and the free development of personality.

In accordance with the above, **Chapter I** of this work, entitled: "**The influence of Big data on the legal system: a multidisciplinary approach**", involves the development of the political and methodological underpinnings from which this research arises. With this aim, the

influence of Big data on the legal system will be analysed from a transversal perspective, based on the frame of reference of what has been termed postmodernity or "liquid modernity."

With regard to the **political underpinnings of the study**, the thesis will explore how the public's enjoyment of their rights and freedoms are affected by the position of dominance adopted by Big data in social media, as well as its pronounced orientation caused by the mathematical logic derived from the algorithm. On this question, the supposed technical neutrality of this tool will be examined, discussing whether, indeed, this position of impartiality can be attributed to it, or if, on the contrary, life based on the algorithm implies a deterministic existence incompatible with the free development of personality.

On this question, this work will explore the possibility that the generalisation of the algorithmic calculation as a structural prerequisite of the Big data context may lead to the creation of different sorts of situations of discrimination in the social environment, creating spaces of exclusion or segmentation that may be contrary to the recognition of basic principles, such as equality or the dignity of the person, with these infringements especially linked to the legal protection of intimacy or privacy. Therefore, this thesis will begin with a discussion of the underlying principles of Big data itself, as well as its reception by social media, prior to its consideration by the legal system.

Next, we will consider the influence of Big data on the creation of a new culture of surveillance, which has been dubbed *Dataveillance*. In this context, we will study the new spaces of social control created by what has been called the *exposition society* or the *transparency society*, as well as issues related to Big data, which have led to a reorientation of the very practices of monitoring and surveillance of the formal social monitoring systems. Specific areas of the Spanish legal system where this context can be observed will be analysed, as they represent the appearance of the criminalisation of opinion offences and the new limits on freedom of expression in the digital age.

To initiate the connection of the political underpinnings of this work with the methodological underpinnings, this work will examine the distortion of the legal protection of

intimacy and private life in the Big data context, as a consequence of the commercialisation of the protection of personal data in this reference framework. Accordingly, the economistic logic guiding the digital privacy standard of protection will be analysed, as well as the loss of control over personal data that the public has experienced as a consequence of the monetary value attributed to personal data by the very corporations that provide their services on the digital platform (highlighting the case of the social network *Facebook*), or by third parties interested in converting personal data into an object of commerce, as shown by the activity of the so-called data brokers.

Turning to the **methodological underpinnings** of this doctoral thesis, the starting point is the need to rethink the concept of privacy, insofar as the very context of Big data has led to a series of risks that call into question the idea that the current standards of legal protection of intimacy and private life are sufficient to handle what "liquid modernity" involves for their maintenance. Accordingly, the diffusion of the limits between public and private require a new conceptual standard that can effectively safeguard respect for the personal sphere of the individual. To achieve this, it will be based on a contrast between the concepts of intimacy and privacy, with the aim of building an inclusive concept that overcomes the highlighted limitations, thereby developing a *refoundation* of privacy that allows the content to be adapted to the Big data context, and also serves as a methodological underpinning for the construction of the right to be digitally forgotten as a fundamental right. In accordance with the above, this new generation right will be understood within a broader concept of *guaranteeism*, where its exercise can serve not only to protect the privacy of the individual who invokes it, but also to safeguard their own capacity to develop freely, without interference from third parties contrary to the general principle of freedom and the concept of legal security.

The *refoundation* of the concept of privacy proposed in these pages will be based on a comparative law study where the focus will be on the legal field of the common law, specifically the regulation of the so-called right to privacy in the United Kingdom. Thus, **Chapter II** of this work is entitled: **"The concept of privacy in the common law legal sphere: the development of the right to privacy in the United Kingdom"**. The study of an

independent legal system typical of the Anglo-Saxon legal culture requires an integrative willingness, especially considering the traditional neglect of the common law by the comparative practice carried out from the continental doctrine. Accordingly, the presented study will not attempt to recognise in its institutions the same features inherent in continental legal culture, but a non-discriminatory structural analysis of its concepts will be undertaken to enrich this research.

For the development of the concept of privacy proposed in these pages, the study of the right to privacy in the British legal system will be especially useful. This is the case because its evolutionary development has meant that one can recognise within its propositions an integration of the concepts of intimacy and private life, representing an approach linked to that of this work with regard to the development of the right to be digitally forgotten as a fundamental right. Therefore, the evolution of the right to privacy will be studied in accordance with the regulatory framework of the British legal system regarding the protection of personal data.

In carrying out this task, the British regulatory framework with regard to the protection of personal data will be studied in its entirety, focusing on the *Data Protection Act 1998*—in force during the preparation of this dissertation—as the main regulation in substantive matters of data protection that, following the path of the earlier and pioneering *Data Protection Act 1984,* incorporates comprehensive protections for the private information of the public, as something intrinsically linked to personal identity and, ultimately, to the privacy of individuals. The work will examine the legal tools provided by said legislation both to individuals and to jurisdictional bodies that, until that moment, had only granted minimal privacy protection through the traditional features of the common law.

Likewise, this dissertation will discuss the importance for the development of the right to privacy the fact of its recognition in Article 8 of the *Human Rights Act 1998*, a declaration of rights and freedoms incorporated into the British legal system that directly transposes the content of the European Convention on Human Rights. On this issue, the innovative role developed by this regulatory body can be highlighted, since it establishes a series of

prescriptive criteria for case law in the interpretation of internal regulations, based on respect for the rights and freedoms of the European Convention on Human Rights and the delimitation of these established by the Court of Strasbourg.

Finally, bearing in mind the future scenarios provided by the *Brexit* situation, the impact that the departure of Great Britain will have on EU institutions will be speculated upon, especially the consequences that this may have on the interactions that will take place from then on between the EU and the UK, which could be considered a third-party state for the purposes of European data protection regulations. Based on the awareness that this is an open question yet to be determined, a range of potential consequences will be explored, taking into account the different scenarios that could play out, offering possible solutions aimed at maintaining a cooperative path for future relations regarding personal data transfers between both territories that, after *Brexit*, will be considered "international transfers." It will also be debated whether, in the last few years, as a result of the recent economic and socio-political phenomena that have taken place in the United Kingdom, there has been variability in its privacy protection standards, and thus the special legislation enacted in the last fifteen years will be examined.

Finally, in **Chapter III**, entitled: "**The development of the right to be forgotten: concept and inspiring principles**", a characterisation of the right to be forgotten as a fundamental right will be presented. In this regard, the approach will be based on the methodological assumptions of this work, that is, the need to re-establish the concept of privacy within the context of Big data. In this way it will be possible to affirm the suitability of the right to be digitally forgotten as a standard of protection that allows for the effective safeguarding of the material conditions for the development of the free personality of the individual, hence its consideration as a fundamental new generation right.

Prior to this characterisation of the right to be digitally forgotten, this work will provide a detailed presentation of the international, EU and national regulatory framework that serves as a reference framework for the evaluation of the right to be digitally forgotten in Spain, closely related to the right to the protection of personal data. Likewise, the leading cases in

jurisprudential matters will be commented on, which, from different judicial spheres (Court of Justice of the European Union, European Court of Human Rights, Constitutional Court, Supreme Court or National Court) have modelled the development of the right to be digitally forgotten from the perspective of law in action, in other words, considering the jurisprudential development of its content.

The categorisation of the right to be digitally forgotten proposed herein aims to respond to the absence of a comprehensive development of its content through doctrine and jurisprudence. The intention is thus to offer a response to the absence of a specific legal framework that regulates the normative implementation of this new generation right. Therefore, in the third chapter of this doctoral thesis, a characterisation of the right to be forgotten is established following the classical structure for the development of fundamental rights, examining the key aspects for its legal configuration and proposing certain guidelines for its evolution.

Thus, among other things, an integrated approach to the right to be digitally forgotten is offered, based on the *refoundation* of privacy offered as a methodological underpinning of the present study. In this regard, legal values such as individual intimacy and private life will be incorporated, but also honour, self-image or the protection of personal data, as a consequence of the polyhedral nature of the right to be digitally forgotten.

Likewise, in order to delimit its content, the limits inherent in the right to be forgotten will be analysed, which, beyond the general principle of good faith and the prohibition of the abuse of rights, focus on the collision with other fundamental rights, mainly freedom of expression and information. On this issue, the criteria to be taken into account by the jurisdictional bodies for the resolution of these conflicts will be presented, based on the weighting mechanism, with special emphasis placed on the recent modification of the doctrine of the Constitutional Court, mainly due to the invalidity of veracity as an element to be considered and the incorporation of the time factor as an essential ingredient of said hermeneutical examination.

Furthermore, various reflections will be made on the active ownership of the right to be forgotten, as well as its possible exercise by legal persons, using the oligopoly position of Big data corporations as just cause to endow the right to be forgotten with a horizontal effect, as well as its effectiveness regarding deceased persons. Likewise, we will try to make a definitive argument about the passive procedural legitimation of the search engines that, although it was affirmed by the jurisprudence, has been controversially applied by the Spanish courts and is now consolidated within the new European normative framework.

With regard to the procedural protection of the right to be forgotten, an overview of its development will be provided from its administrative and civil sides. On this issue, this work will examine the appropriateness of handing over to private interests the weighting exercise with respect to the interests in conflict. In the same way, an argument will be constructed that permits the possibility of protecting the right to be forgotten by means of the remedy of the writ of amparo before the Constitutional Court. Similarly, it will focus on the criminal protection of the subject's sphere of privacy, as well as on the supranational mechanisms of protection of the right to be digitally forgotten.

Finally, some accessory issues will be examined, such as the differentiation of the right to be forgotten from some related or complementary legal mechanisms such as the right to cancel or rectify. In addition, the capacity of non-contractual liability to compensate for the damages and losses suffered with regard to the privacy of the individual will be assessed.

CAPÍTULO I. LA INFLUENCIA DEL BIG DATA EN EL ORDENAMIENTO JURÍDICO: UNA APROXIMACIÓN MULTIDISCIPLINAR

1. El derecho al olvido como respuesta a los retos planteados para la protección de la privacidad en el *Big data*

Cada cierto tiempo, se producen determinados fenómenos sociales que suponen un cambio de paradigma sustancial en las prácticas políticas, económicas, sociales, o incluso culturales, propias de un determinado contexto espacio-temporal. En este sentido, la revolución tecnológica y digital aparejada a la Sociedad de la Información, ha venido a redefinir amplios espacios de la vida en comunidad, y a variar continuamente las formas de interacción social propias de nuestro momento histórico. En la *posmodernidad* actual, el *Big data*, sobre cuyo concepto se profundizará en el aprtado siguiente, supone una de las manifestaciones más intensas de un nuevo paradigma, donde conceptos jurídicos que tradicionalmente no presentaban mayores discusiones, como por ejemplo los de intimidad o vida privada, requieren de un proceso de reflexión para adaptar sus proposiciones al nuevo estado de cosas.

Esta nueva coyuntura reclama de la Ciencia, el Derecho, la Ética, la Economía y la Política, una "responsabilidad tecnológica", es decir, una actitud reflexiva, crítica y consciente de los nuevos problemas que, en las diversas esferas de la vida suscita la tecnología y a los cuales la sociedad y, particularmente el ordenamiento jurídico, no pueden ignorar[1]. La necesaria evolución de la colectividad no puede restar un ápice del contenido garantista que requiere la protección de los derechos fundamentales en un Estado social y democrático de Derecho, que debe adoptar las precauciones necesarias así como accionar los mecanismos indispensables para lograr un progreso tecnológico y social compatible con el respeto a esos derechos fundamentales[2].

[1] PÉREZ LUÑO/GONZÁLEZ-TABLAS. "Ciberciudadanía y teledemocracia", en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. I, Libro II, Dykinson, Madrid, 2013, p. 1113.

[2] Como bien señala DÍEZ-PICAZO, la experiencia histórica nos ha enseñado que el Derecho, como fenómeno en sí mismo considerado, es ante todo "un proceso de cambio y de progreso jurídico". Cfr. *Experiencias jurídicas y teoría del Derecho*, Ariel, Barcelona, 1983, p. 300.

Así las cosas, el propio cambio de paradigma que representa este nuevo escenario exige reconstruir el ámbito de libertad personal de los sujetos así como su esfera privada, para que el proceder de las empresas tecnológicas, las corporaciones del *Big data* y los nuevos medios de información no supongan una minusvaloración de dichas nociones, tan estrechamente ligadas a la protección del libre desarrollo de la personalidad de la ciudadanía. Efectivamente, un cambio de tal magnitud como el *Big data*, que sin duda representa un avance notable para el progreso social, debe cohonestarse con una respuesta efectiva desde el ordenamiento jurídico, para así adecuar sus proposiciones a los presupuestos estructurales de la protección de la privacidad. En otras palabras, es necesario realizar un esfuerzo desde el ámbito de las ciencias jurídicas para así elaborar propuestas doctrinales que, siendo compatibles con los beneficios propios de la revolución tecnológica, no permitan un retroceso en la protección de los derechos y libertades de la ciudadanía.

En la actualidad, viviendo en plena sociedad de la información y del conocimiento, dónde la era digital es una realidad asumida plenamente y en la cual se avecinan nuevos retos inmediatos debido, principalmente, a la proliferación de la inteligencia artificial, el derecho al olvido se presenta como una suerte de garantía personal que aspira a poner remedio a los inconvenientes y perjuicios que genera la enorme multiplicación de datos personales que pasan a engordar bancos de almacenamiento y procesamiento fuera de nuestro control. De acuerdo con lo expuesto, el desarrollo del derecho al olvido como derecho fundamental supone una exigencia para el Estado social y democrático de Derecho, en tanto que éste debe adecuar sus presupuestos estructurales al cambio de paradigma que representa el *Big data*.

Para lograr integrar de forma coherente los nuevos fenómenos desde un punto de vista jurídico, se ha considerado ofrecer, en primer lugar, una descripción circunstanciada sobre la influencia multidisciplinar del *Big data* en el ordenamiento, como punto de partida previo a la categorización presentada en esta tesis doctoral sobre el derecho al olvido. Esto es así en la medida en que la protección de los derechos de la personalidad, al operar sobre conceptos como la intimidad o la vida privada que no pueden entenderse desde una perspectiva unidireccional, requiere de una visión poliédrica, de una misma concepción integral con la que

ha de tratarse el derecho al olvido digital. En consecuencia, será necesario realizar en primera instancia una aproximación al concepto de *Big data*, así como a su propia lógica de funcionamiento y su capacidad disruptiva, para así reconocer el fenómeno al que se enfrenta la construcción del derecho al olvido digital propuesta en esta investigación.

1.1. ¿De qué hablamos cuando hablamos de Big data?

En 2017 se calculó que, en un minuto en Internet, se generaron 3,5 millones de búsquedas en *Google*, se visualizaron más de 70.000 horas de vídeos online de *Netflix*, se escribieron 452.000 tuits, se escucharon 40.000 horas de música en *Spotify*, se unieron a *Facebook* casi un millón de nuevos usuarios, se subieron 46.200 fotos a Instagram, se vieron más de 4 millores de vídeos en YouTube, se enviaron 16 millones de mensajes instantáneos y se descargaron 342.000 Apps[3]. En un solo minuto se transfirieron más de 1.500 terabytes de información en Internet.

A la velocidad a la que se expande la tecnología a nivel planetario, en pleno 2018, estas cifras se han incrementado exponencialmente. Como es bien sabido, la revolución digital ha modificado por completo nuestras pautas de comportamiento. Vivimos en un momento de cambio constante, donde la técnica no se detiene y dónde la distracción de un solo pestañeo puede alejarte de la vanguardia; usando la terminología de BAUMAN, es ésta una época de "modernidad líquida"[4]. En esta acelerada etapa se produce un cambio radical en la cohabitación humana, en el condicionamiento social de las políticas de vida. Conceptos como la velocidad del movimiento o el espacio han dado un giro radical hasta diluir sus fronteras, llegando incluso a desaparecer. Así por ejemplo, los avances tecnológicos han logrado una instantaneidad en la comunicación que ha supuesto la eliminación de la concepción del espacio como límite de las relaciones sociales, pues nuestros actos ya no se circunscriben al entorno más inmediato, sino que van más allá del espacio físico.

---

[3] Estudio elaborado por la consultora Cumulus Media, última consulta 19.05.2018, https://www.allaccess.com/merge/archive/26034/what-your-audience-is-doing-when-they-re-not.

[4] Cfr. BAUMAN . *Modernidad líquida*, Fondo de Cultura Económica, Madrid, 2017.

En este sentido, nuestra forma de entender la vida ha cambiado de tal modo que ya no es tan significativo, ni tal siquiera fácil, distinguir entre lo *offline* y lo *online*, dado que en la actualidad todo tiende a estar conectado y dichas barreras se interrelacionan constantemente (un ejemplo muy sencillo: realizar una compra por Internet para luego devolver lo adquirido en una tienda *física* –de hecho, la necesidad de especificar el carácter físico o virtual del proveedor de servicios o bienes es en sí mismo una alegoría de este escenario–). Del mismo modo, la interacción de las personas en el ciberespacio es tan real como frecuente, por lo que éste ha pasado a convertirse en una prolongación de la sociedad física.

Cada uno de esos movimientos en la Red genera información que se digitaliza en código binario y se almacena masivamente para, con técnicas de lo más complejas, analizarlos y extraer nuevas referencias que en el futuro puedan aplicarse a la transformación del mundo real. Este proceder supone un uso y tratamiento masivo de datos destinados a inferir, a partir de su análisis, nuevas percepciones o indicadores, los cuales tienen una dimensión valorativa o axiológica que puede servir como fundamento para la transformación de los mercados, organizaciones o entes, e incluso la propia forma de relacionarse entre el Estado y la ciudadanía.

Así las cosas, llamamos *Big data* al almacenamiento, tratamiento y transferencia de datos a gran escala a través de las tecnologías de Internet. En la globalización del siglo XXI, las innovaciones tecnológicas junto con el nuevo modelo económico y social, han hecho proliferar enormes cantidades de bases de datos relativos a realidades tangibles (datos físicos) o intangibles *a priori* pero convertidos mediante algoritmos en información digital. Entre los unos y los otros hay un número descomunal de datos de carácter personal. La relevancia de estos datos masivos no sólo afecta a cuestiones directa e indirectamente vinculadas a nuestra privacidad, sino que tiene una trascendencia que abarca la propia configuración del tejido social. Como señalan MAYER-SCHÖNBERGER y CUKIER, "la era de los datos masivos pone en cuestión la forma en que vivimos e interactuamos con el mundo. Y aún más, la sociedad tendrá que desprenderse de parte de su obsesión por la causalidad a cambio de meras correlaciones: ya no sabremos por qué, sino solo qué. Esto da al traste con las prácticas

establecidas durante siglos y choca con nuestra comprensión más elemental acerca de cómo tomar decisiones y aprehender la realidad"[5]. De este modo, si bien en el pasado los datos podían tener un valor asociado de forma específica a la propia información personal o a la propiedad intelectual e industrial, el nuevo escenario resultante del *Big data* supone reconocer el valor intrínseco, como categoría independiente, de los datos, pues como se verá en este capítulo su tratamiento masivo supone un nuevo paradigma en el medio social, que como tal debe ser asumido desde el punto de vista del ordenamiento jurídico.

Las nuevas tecnologías inteligentes funcionan a partir de datos y metadatos –los metadatos son datos sobre los propios datos, además de qué y quién, dan respuesta al cuándo, cómo, dónde…permitiendo crear catálogos de ficheros de datos con el objetivo de explotarlos posteriormente, por ejemplo, para fines publicitarios–[6]. Estos datos y metadatos se consiguen, generalmente, a través de las aplicaciones que descargamos en nuestros dispositivos inteligentes que cada vez exigen con más frecuencia acceso a información personal para proceder a la instalación[7]. Piénsese, por ejemplo, en los permisos para acceder a la geolocalización del dispositivo resultantes de la aceptación en bloque de las condiciones de uso de dichas aplicaciones. En la medida en que los propios hábitos de búsqueda del usuario a través de sus dispositivos estén a disposición de las empresas privadas, si a esto le sumamos la posibilidad de acceder a los datos de geolocalización en todo momento, ello permite, por ejemplo, introducir una publicidad personalizada allá donde esté, o aún más inquietante, allá

[5] Cfr. *Big data. La revolución de los datos masivos*, Turner, Madrid, 2015, p. 18.

[6] Así, si un teléfono móvil tradicional tenía información sobre a quién llamábamos y de cuántos SMS enviábamos al mes, un Smartphone sabe infinidad de datos acerca de nosotros: cuántas calorías consumimos de media, cuánto tiempo dormimos, cuánto dinero solemos gastar en el supermercado, qué tipo de prensa leemos habitualmente, en qué noticias estamos más interesados…hasta el punto de poder hacernos una configuración de nosotros a imagen de patrones de comportamiento –que muchas veces no tiene por qué coincidir con la verdadera-, como por ejemplo el nivel adquisitivo de una persona, o su entorno social.

[7] Sobre esta cuestión, HARCOURT señala la construcción de perfiles comerciales elaborados por Google a través del estudio de los correos electrónicos de sus usuarios de Gmail, lo que el autor norteamericano ha denominado como "conocimiento digital" (*digital knowledge*). La construcción del perfil mediante la monitorización de las palabras escritas en los correos, los archivos adjuntos, el contenido de las páginas web visitadas por el usuario de Gmail, así como toda la información demográfica obtenida en el momento de crear la cuenta permite a Google obtener un retrato robot del consumidor, pudiendo así incidir en sus hábitos comerciales, o lo que eufemísticamente denomina el autor norteamericano: "hacer la experiencia online más personal y disfrutable para el usuario/consumidor". Cfr. "Governing, Exchanging, Securing: Big Data and the production of a digital knowledge", *Public Law and Legal Theory Working Paper Group*, Columbia Law School, 2014, pp. 4-5.

dónde se prevea vaya a estar una persona, algo que ya hemos comprobado ocurrir en nuestras búsquedas, o visitas a sitios, de Internet.

Asimismo, los metadatos también pueden inferirse de la interacción del usuario en redes sociales. Por ejemplo, en una actualización en el muro de *Facebook* de un usuario crítico con la última medida del gobierno de turno, lo menos interesante desde la perspectiva del almacenamiento, tratamiento y comercialización de los datos masivos, son sus valoraciones políticas. Los metadatos asociados a dicha interacción, lo que se ha denominado como "información de la información", se revelan de mayor utilidad para los interesados en explotar datos masivos. Si bien parte de esta información secundaria no tiene mayor interés –denominación, foto de perfil, software utilizado para acceder a la aplicación–, sí puede ser más provechosa la posibilidad de acceder a las páginas que siga el usuario, la propia geolocalización o sus hábitos de consumo[8], trazando así un perfil digital de la persona.

Estos bancos de datos contienen información relativa a nuestra identidad (nombres, lugar de residencia, profesión, estado civil, propiedades…) así como otra información personal tan diversa como nuestra religión, ideología, clase social, salud… La información, en el primer caso, se obtiene de registros públicos o privados y por ello podíamos decir que es "real" mientras que, en el segundo caso, ésta es obtenida a través de otros parámetros -no siempre fiables- como nuestras pautas de comportamiento, preferencias culturales o patrones de consumo. Podría aquí diferenciarse entre los datos estructurados, aquellos que provienen de fuentes de información conocidas y que, por a tanto, son fáciles de medir y analizar en los sistemas tradicionales, en contraposición a lo que se ha dado en llamar datos no estructurados. Para que sea posible analizar estos últimos, teniendo en cuenta la variedad de su origen, así como la rapidez con que se incrementa su volumen, ha sido necesario el desarrollo de nuevos modelos de software para adecuarse a su carácter disperso y heterogéneo[9].

[8] Nótese que muchas personas utilizan su cuenta de *Facebook* como modo de identificación para iniciar sesión en páginas de compra de entradas, ropa u otras formas de comercio electrónico.

[9] Cfr. PUYOL MORENO. "Una aproximación a Big Data", *Revista de Derecho, UNED*, nº 14, 2004, p. 483.

Centrándonos en los datos personales, puede seguirse la triple clasificación presentada por HARCOURT distinguiendo, en primer lugar, los "datos inteligentes" (*Smart data*), en referencia a los datos masivos que han sido previamente procesados y analizados para responder a una necesidad particular. En segundo lugar, señala los "datos de identidad" (*Identity data*) como los datos masivos de mayor importancia para su uso comercial, en tanto que contiene información personal de la ciudadanía que actúa como fuerza motriz para el desarrollo de los modelos predictivos. Esta modalidad de datos viene a describir la personalidad del ciudadano en el mundo digital, incluyendo contenido de redes sociales, hábitos comerciales, análisis de su comportamiento online, etc. Finalmente, relacionados con estos últimos, aparecen los "datos colectivos" (*People data)*, creados a partir de su agregación continuada y progresiva a lo largo de un espacio de tiempo concreto. Supone un análisis conjunto de los datos masivos de un número concreto de usuarios, con la finalidad de establecer una serie de patrones de comportamiento a nivel social[10].

Los distintos tipos de información quedan almacenadas en enormes bases de datos y unos y otros permiten identificarnos o reconstruir nuestra identidad. Este proceso, llevado a cabo masivamente por parte de las empresas de telecomunicaciones, sumado a los datos generados por las administraciones públicas y las industrias privadas de seguridad, es lo que se ha denominado por algunos autores como *Dataveillance,* o dicho de otra forma: la normalización social de la cultura de la vigilancia[11]. Esta es una de las vertientes más interesantes del nuevo contexto resultante del *Big data*, en tanto que supone un nuevo paradigma en los itinerarios de evolución del control social formal. Teniendo en cuenta su trascendencia para la protección de los derechos y libertades de la ciudadanía, se le dedicará un punto aparte en este capítulo[12].

[10] Cfr. "Governing, Exchanging, Securing: Big Data and the production of a digital knowledge", ob. cit., p. 20.

[11] En inglés, *surveillance* significa vigilancia. Para la construcción lingüística del concepto reseñado se ha introducido *data* en lugar de *sur* para, con el juego de palabras, remarcar la importancia de los datos masivos en el advenimiento de nuevas formas de control social.

[12] Vid. *infra* Cap. I.2

Pero no sólo se trata de acumular datos y datos, sino de interrelacionarlos entre sí para lograr aumentar exponencialmente la información a obtener y, de ese modo, sacarle un mayor partido. Es lo que SOLOVE llama *agregación*[13]: conformar el perfil de una persona a través de la triangulación y organización de la información que se ha obtenido sobre ella, generando nuevos datos sobre un individuo. Contar con estos nuevos datos resulta especialmente útil para el desarrollo de determinadas campañas publicitarias que se elaboran a partir de este proceso de *agregación*. Sin embargo, dicho proceso, al alterar las expectativas de las personas, supone una amenaza para la intimidad, ya que el sujeto no ostenta control alguno sobre el conocimiento que se está obteniendo a través de su información personal. Como expone O'NEIL, "nos clasifican y categorizan y nos asignan puntuaciones en cientos de modelos en base a los patrones y preferencias que hemos desvelado. Y esto constituye un poderoso fundamento para muchas campañas publicitarias legítimas, aunque también alimenta a la publicidad depredadora: los anuncios que identifican a las personas con grandes necesidades y les venden promesas falsas o productos a precios excesivos"[14].

Para la filtración de los datos (lo que se conoce como *data mining*, expresión traducida como minería de los datos) hay software específicos que se encargan de cruzarlos atendiendo a los parámetros que para su finalidad concreta resulte interesante y la información obtenida vuelve a almacenarse de nuevo en otras bases de datos, compartimentadas según los criterios empleados y que reciben el nombre de bancos de datos[15]. Unos mismos datos pueden clasificarse según distintos parámetros y, en consecuencia, pueden formar parte de infinidad de bases de datos. De acuerdo con esta técnica, cualquier fenómeno social puede terminar siendo tabulado y analizado a partir de los datos masivos previamente obtenidos, esto es, *datificado*. Esto lleva a reconocer un segundo estadio en el proceso de filtración de datos, próximo a su

[13] Cfr. SOLOVE. "A Taxonomy of Privacy", *University of Pennsylvania Law Review*, Vol. 154, nº 13, pp. 477 ss.

[14] Cfr. *Armas de destrucción masiva. Cómo el Big data aumenta la desigualdad y amenaza la democracia*, Capitán Swing, Madrid, 2018, p. 89.

[15] Una definición de este concepto se proporciona en la *Directiva del Parlamento Europeo y del Consejo sobre los derechos de autor en el mercado único digital COM/2016/0593 final – 2016/0280 (COD)*, cuyo polémico texto fue aprobado el pasado 12 de septiembre de 2018. En su artículo 2.2) se define el *data mining* como "*cualquier técnica analítica automatizada para analizar textos y datos en formato digital a fin de general información sobre pautas, tendencias o correlaciones*", remitiéndose a su artículo 3 para los detalles de su regulación.

correlación con el medio social. Se denomina *reality mining* (en este caso, traducido como minería de la realidad) a la técnica inicialmente desarrollada en el Laboratorio de Dinámica Humana del Massachusetts Institute of Technology, consistente en procesar datos masivos procedentes de dispositivos móviles para extraer inferencias y predicciones sobre el comportamiento humano[16]. En este segundo estadio, los datos previamente obtenidos tienden a situarse en correlación con distintas variables de aplicación en el medio social, con la finalidad de desarrollar una serie de criterios o pautas para el estudio de determinados comportamientos o fenómenos de alcance sociológico.

Como se ha dicho, Internet ha logrado aumentar exponencialmente el tráfico de información y, a través de la interconexión mundial de bases de datos y la cantidad de copias de las mismas, puede afirmarse que el aumento de tráfico de información que discurre por esta vía, es hoy en día imparable[17]. Esto en sí mismo no es negativo, gracias a ello tenemos acceso a una cantidad enorme de fuentes de casi cualquier parte del mundo que de otro modo sería impensable alcanzar. ¿Cual es la otra cara de la moneda? La falta de privacidad de la ciudadanía[18].

Así las cosas, la poderosa correlación establecida entre el *Big data* y la revolución digital nos hace pensar que no estamos presenciando ni mucho menos un fenómeno cerrado, sino que

---

[16] Ampliamente, EAGLE/ GREENE. *Reality mining. Using big data to engineer a better world*, MIT Press, Boston, 2014. Sin duda, esta técnica no tiene que ser rechazada *per se*, en tanto que su uso responsable permitiría, por ejemplo, erradicar problemas de salud pública. No obstante, la posibilidad de desviarse de los parámetros deontológicos propios de las ciencias sociales, así como lo atractivo de utilizar estos procesos para la consecución de un beneficio económico o de un control social, plantean serias dudas sobre su uso raramente aséptico.

[17] Así, MORENO MUÑOZ apunta cómo "datificación, internet de las cosas y *big data* convergen sobre una base común de herramientas, tecnologías y procesos a gran escala que consolidan una tendencia a definir el modo en que las organizaciones o empresas tradicionales prestan sus servicios, entendidos en el nuevo contexto tecnológico como actividades dependientes de una infraestructura global de datos, de la que se extraen conocimiento e información para desarrollar procesos críticos de su negocio, adoptar decisiones estratégicas y responder a la evolución de la competencia con un mejor control de los datos relevantes para su actividad". Cfr. "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", *Dilemata,* nº 24, 2017, p. 9.

[18] Nótese que se habla de privacidad y no de intimidad, utilizando, se verá más adelante, una nomenclatura más próxima a la tradición jurídica del *common law*, y no tan acorde con nuestro ordenamiento jurídico. A lo largo de este trabajo se usará el término 'privacidad' de forma consciente y precisamente para hacer notar que los datos personales pueden tener incidencia en el espacio "privado" de la persona más allá de su 'intimidad'. Es decir, se pretende poner de manifiesto que, si bien todas las conductas que aquí se describen no afectan a la intimidad estricta de la persona (en el sentido doctrinal más tradicional y consolidado) sí que tienen incidencia en una esfera menos íntima pero igualmente privada y, por ende, con un resultado lesivo de determinados derechos y libertades). Sobre esta cuestión, Vid. *infra* Cap. I. 4. I.

éste es un paradigma todavía en construcción, donde el tamaño y escala de los datos seguirá acrecentándose, así como el desarrollo de herramientas analíticas de procesamiento cuyo incremento es proporcional a esta escalada. En este escenario, todo parece apuntar a que la privacidad, al menos en su acepción tradicional, se encuentra en peligro ante los riesgos de minimizar su protección por la mala *praxis* en la gestión de los datos masivos[19].

Este proceso, además, es difícilmente reversible. En el que podemos llamar nuevo Internet de los datos[20] éstos se usan, se reutilizan, se vuelven a usar sus desechos y raramente se destruyen, cancelan o desaparecen; sino que se almacenan porque en el futuro serán objeto de nuevos usos. Esto no supone que el valor de los datos disminuya, dado que la posibilidad de procesarlos de forma indefinida no supone desgastar la información que contienen pues, a diferencia de los objetos materiales, ésta puede ser reutilizada sin que su valor vaya a verse resentido. De hecho, los datos masivos pueden ser explotados con propósitos múltiples, de modo que el valor pleno de los datos puede ser mayor que el obtenido únicamente por su primer uso. Este hecho significa también que las compañías pueden explotar datos de forma efectiva incluso cuando el primer uso, o cada uso subsiguiente, sólo haya aportado una pequeña cantidad de valor, siempre y cuando reutilicen los datos iniciales con distintos procesamientos.

Como consecuencia, los datos se han convertido en una materia prima para el Mercado, en un factor trascendenal capaz de crear una nueva forma de valor económico. Y esto parece ser sólo en principio, en tanto que el cambio de paradigma representado por el *Big data* puede rivalizar en significación con otras etapas de cambio de signo histórico, como por ejemplo la atribuida a la denominada revolución industrial. De acuerdo con MAYER-SCHÖNBERGER y CUKIER: "Los datos masivos están a punto de remodelar nuestro modo de vivir, trabajar y pensar. El cambio al que nos enfrentamos es, en ciertos sentidos, incluso mayor que el derivado de otras innovaciones que hicieron época, y que ampliaron acusadamente el alcance y la escala

[19] Como apunta ALBERTO GONZÁLEZ, "aplicando la terminología del mundo de la gestión de riesgos, puede afirmarse que el tratamiento masivo de datos personales tiene, por su propia naturaleza y según la forma en que se lleve a cabo, un *impacto* sobre los derechos de las personas afectadas y puede suponer un riesgo para las mismas, en el caso de que dicho tratamiento masivo de datos no cuente con medidas adecuadas para evitar o mitigar dichos riesgos". Cfr. "Responsabilidad proactiva en el tratamiento de datos masivos", *Dilemata*, nº 24, 2017, p. 116.

[20] Cfr. NAVAS NAVARRO. *Mercado digital. Principios y reglas jurídicas*, Tirant lo Blanch, Valencia, 2016, p. 29.

de la información en la sociedad. El suelo que pisamos se está moviendo. Las certezas anteriores se ven cuestionadas. Los datos masivos exigen una nueva discusión acerca de la naturaleza de la toma de decisiones, el destino, la justicia. Una visión del mundo que creíamos hecha de causas se enfrenta ahora a la primacía de las correlaciones. La posesión de conocimiento, que en tiempos significó comprender el pasado, está llegando a ser una capacidad de predecir el futuro"[21].

Una vez los datos son incorporados a Internet, circulan libremente por el ciberespacio pasando de unas bases de datos a otras y de un servidor de Internet a otro por lo que, si además tenemos en cuenta las copias periódicas que se hacen de las páginas web, aunque se consiga borrar la información de su fuente original, es prácticamente imposible hacerla desaparecer de todos los rincones del ciberespacio. Esto ha sido bautizado por el Prof. TRONCOSO como el "efecto Hotel California": *you may enter, but you may never leave*[22].

Por lo tanto, puede reconocerse que el *Big data* supone un cambio tanto cuantitativo como cualitativo en los estándares de riesgo que la propia privacidad podía tradicionalmente asumir con el surgimiento de Internet como vehículo de información y comunicación masivo. Hablamos de modificación cuantitativa porque aumenta la intensidad de los riesgos, siendo asimismo el nuevo paradigma de distinta percepción cualitativa en tanto que la propia naturaleza de estos riesgos se ha visto modificada.

Sobre esta cuestión, la nueva perspectiva axiológica parte de la necesidad de proteger la privacidad del ciudadano, no únicamente respecto de los terceros que pudieran invadir su esfera personal, sino también en relación con la posible explotación mercantil de los datos personales por entidades especializadas en estas prácticas[23], e incluso ante la necesaria protección de la privacidad que, paradójicamente, supone la constante y voluntaria exposición de nuestra vida privada en las redes sociales. De acuerdo con BAUMAN, "lo que está ocurriendo actualmente

[21] Cfr. *Big data. La revolución de los datos* masivos, ob. cit., p. 233.

[22] Cfr. TRONCOSO REIGADA. *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, Valencia, 2010, p. 43.

[23] Es decir, la actividad que desarrollan los llamados *data brokers*. Vid., *infra* Cap. I. 3. II.

no es tan sólo una nueva renegociación de la móvil frontera entre lo privado y lo público. Parece estar en juego una redefinición de la esfera pública como plataforma donde se ponen en escena los dramas privados, exponiéndolos a la vista del público. La definición actual de *interés público*, promovida por los medios y ampliamente aceptada por casi todos los sectores de la sociedad, es el deber de interpretar esos dramas en público y el derecho del público a asistir a la función. Las condiciones sociales que dieron lugar a este proceso y que lo hacen parecer *natural* se desprenden de la argumentación anterior, pero las consecuencias de esta situación no han sido plenamente exploradas. Es posible que sus alcances sean mayores de lo que se cree"[24]. Desde esta óptica, no es descabellado afirmar que las dinámicas propias del *Big data* han supuesto una redefinición de los procesos sociales sin precedentes.

El filtrado de datos masivos en su expresión genérica *data mining*, y más particularmente en su expresión *reality mining*, es decir, la de procesamiento de correlación social sobre comportamientos, requiere de sofisticados mecanismos entre los que ocupa un lugar de preeminencia el empleo de algoritmos o programas informáticos cuya caracterización técnica tan compleja se utiliza como coartada para una presentación aséptica, pretendidamente neutra de estas prácticas, lo que veremos del todo discutible en el apartado siguiente.

1.2. Vivir en la era del algoritmo

Toda dinámica de transformación social viene asociada a una serie de prácticas que determinan el nuevo estado de cosas a nivel político, económico e incluso cultural, resultantes del cambio histórico. En el caso del *Big data*, es indudable la importancia del cálculo algorítmico como presupuesto estructural sobre el que se sustenta, al menos considerándolo en términos funcionales, gran parte del marco de referencia acontecido con el *Big data*. Demasiadas veces la utilización del algoritmo[25] ha sido defendida desde la neutralidad asignada al pensamiento científico, en tanto que lenguaje perfectamente codificado mediante el uso de

[24] Cfr. *Modernidad líquida*, ob. cit., pp. 75-76.

[25] Una definición del concepto de algoritmo comprehensiva y operativa en el contexto del *Big data* es la propuesta por MONASTERIO ASTOBIZA como "código software que procesa un conjunto limitado de instrucciones". Cfr. "Ética algorítmica: implicaciones éticas de una sociedad cada vez más gobernada por algoritmos", *Dilemata*, nº 24, 2017, pp. 185-186.

las matemáticas como vehículo, impulsado (o acelerado, para continuar con el símil) en este contexto por la posición de preeminencia adoptada por la hegemonía del pensamiento neoliberal propio en las sociedades capitalistas o por el interés controlador de determinados aparatos de Estado en cualquiera de sus formas.

En dicho sentido, éste podría ser el primer aspecto a discutir respecto de la utilización del algoritmo como técnica de ordenación social pues la asunción previa de que el sistema en que éste se desarrolla funciona adecuadamente podría ser rebatible, considerando las dificultades con las que se ha encontrado el capitalismo, como forma político-estatal resultante de la hegemonía del pensamiento neoliberal, para adaptarse a los presupuestos estructurales de la *posmodernidad* en un mundo globalizado.

Como ejemplo de disfunción, puede mencionarse la vacuidad de las soluciones aportadas para responder a la crisis política, económica y social que tuvo como causa el estallido de los mercados financieros en 2008, con la consecuente repercusión en el ámbito de las Unión Europea[26]. Ante una situación de conflicto sistémico sólo supo responderse a partir de la *razón económica*[27], creando una mayor situación de desigualdad y retrocediendo en materia de derechos y libertades. De forma paralela, para justificar la aplicación de la llamada *razón económica*, fue defendido el carácter técnico, pretendidamente neutral, de este tipo de intervenciones (por cierto, presentadas como imprescindibles, humanizándolas con todo cinismo como sacrificios necesarios por el bien –para su misma subsistencia– de los propios damnificados) dirigidas a conservar las estructuras económicas de una sociedad capitalista. En

[26] Contra la postura adoptada en la salida de las crisis en el ámbito de la Unión Europea, pueden traerse a colación las palabras de ZIZEK: "a menudo se escucha que el verdadero mensaje de la crisis de la Eurozona es que no sólo el euro está muerto, sino también el propio proyecto de la Europa unida (…) Europa está muerta, de acuerdo, pero ¿qué Europa? La respuesta es: la Europa pospolítica de acomodación al mercado mundial, la Europa que ha sido repetidamente rechazada en los referéndums, la Europa de los tecnócratas y expertos en Bruselas. La Europa que se presenta a sí misma como representante de la fría razón europea contra la pasión y corrupción griegas, de las matemáticas contra lo sentimental. Pero aunque pueda parecer utópico, todavía existe espacio para otra Europa: una Europa repolitizada, fundada sobre un proyecto compartido". Cfr. "Un permanente estado de excepción económica", *New Left Review*, nº 64, 2010, p. 86.

[27] De acuerdo con la definición de DE CABO MARTÍN, este concepto de razón económica "elimina otras alternativas que no sean la económico-liberal, estableciendo con rotundidad el contenido (decisión) fundamental de la centralidad del Mercado, en el sentido de que vertebra todo el sistema al subordinar los demás componentes, o, al menos, los hace necesariamente compatibles con el mismo". Cfr. *Dialéctica de sujeto, dialéctica de la Constitución*, Trotta, Madrid, 2010, p. 111.

este sentido, puede resultar interesante la referencia a ZIZEK, cuando considera que el concepto de capitalismo como forma de ordenación social neutral es "ideología en su más pura extensión"[28].

Siguiendo este paralelismo, no podemos considerar el *Big data*, ni tampoco su desarrollo mediante el cálculo algorítmico, como una realidad social neutra, en tanto que pese a su carácter científico-técnico, la forma de orientar esta evolución, por ejemplo respecto al valor monetario atribuido a los datos masivos, muestra una opción ideológica concreta[29]. Recuperando la referencia anterior "esta negación de la ideología lo único que hace es proporcionar la prueba definitiva de que estamos inmersos en ella"[30]. En línea con el parecer de este autor, pueden asimismo destacarse las palabras de HAN reconociendo cómo "el dataísmo, que pretende superar toda ideología, es en sí mismo una ideología, y ello conduce al *totalitarismo digital*"[31].

Por mucho que los algoritmos puedan responder a razonamientos matemáticos ciertos fruto de una lógica científico-numérica, esto no obsta para que presenten determinados sesgos o limitaciones cuando traspasan el ámbito del *deber ser ideal* propio del pensamiento científico, para aplicarse en el *ser conflictivo* de los procesos sociales. De acuerdo con O'NEIL, "las aplicaciones fundamentadas en las matemáticas que alimentaban la economía de los datos se basaban en decisiones tomadas por seres humanos que no eran infalibles. Seguro que algunas de esas decisiones se tomaban con la mejor de las intenciones, pero muchos de estos modelos programaban los prejuicios, las equivocaciones y los sesgos humanos en unos sistemas informáticos que dirigían cada vez más nuestras vidas"[32]. Así las cosas, no puede despreciarse

[28] Cfr. *Primero como tragedia, después como farsa*, AKAL, Madrid, 2013, p. 31.

[29] En este sentido, es significativa la siguiente afirmación de MONASTERIO ASTOBIZA: "para contextualizar y entender la dependencia algorítmica de nuestras sociedades (el gobierno de los algoritmos o *algoritmocracia*) y la visión algorítmico-céntrica de la vida y el trabajo hay que saber que la historia reciente de los algoritmos, la computación y automatización de procesos, tiene su comienzo en los mercados de acciones de Wall Street". Cfr. "Ética algorítmica: implicaciones éticas de una sociedad cada vez más gobernada por algoritmos", ob. cit., p. 186.

[30] Cfr. *Primero como tragedia, después como farsa*, ob. cit., p. 45.

[31] Cfr. *Psicopolítica*, Herder, Barcelona, 2014, p. 88.

[32] *Armas de destrucción masiva. Cómo el Big data aumenta la desigualdad y amenaza la democracia*, ob. cit., p. 11.

el riesgo de que los parámetros que orienten el cálculo mediante los algoritmos puedan establecer una serie de desigualdades en el tratamiento de los ciudadanos a los cuales se dirijan[33].

Sobre esta cuestión, piénsese en la posibilidad de establecer variables relacionadas, por ejemplo, con el nivel económico o la procedencia social de los sujetos destinatarios del cálculo algorítmico. Si bien puede presentarse como un criterio técnico, sin ningún ánimo discriminatorio respecto de sus destinatarios, resultan innegables los riesgos de que este tipo de prácticas puedan terminar en un mero proceso, simplificador y reduccionista, de etiquetaje de la ciudadanía en función de su acceso a los recursos[34]. Siguiendo con el análisis del pensamiento de ZIZEK, podría argumentarse de qué manera la propia consideración del binomio capitalismo-algoritmo como una mera solución técnica a la ordenación de los procesos sociales puede ser discutible: "hay que fijarse en el término *solución técnica*: los problemas racionales tienen soluciones técnicas (…) no sorprende, entonces, que el propio capitalismo sea presentado en términos técnicos, no ya como una ciencia, sino simplemente como algo que funciona; no necesita justificación ideológica, porque su éxito es en sí mismo suficiente

[33] COTINO HUESO expone los riesgos de que el tratamiento de los datos masivos quede en unas pocas manos especializadas, en tanto que los responsables se convertirían en privilegiados, en posición de fijar las reglas reales sobre cómo van a ser utilizados y quienes podrían acceder a su conocimiento. Serían, en suma, quienes pueden *leer los datos*, "quienes tienen acceso al conocimiento y medios para realizar el tratamiento masivo de datos, pudiendo imponer barreras de acceso o limitar efectivamente o selectivamente al acceso a los datos o al conocimiento generado". Cfr. "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata,* nº 24, 2017, p. 138.

[34] De acuerdo con ALBERTO GONZÁLEZ: "la finalidad de la mayor parte de los tratamientos masivos de datos persigue la búsqueda de patrones, tendencias o perfiles que permiten sacar conclusiones y tomar decisiones en consecuencia. En ocasiones, estas consecuencias afectan directamente a los individuos que han aportado la información y, si ésta contuviese cualquier inexactitud, puede acarrear consecuencias negativas para los afectados, por el hecho de ser asignados a perfiles sobre los cuales se tomarán decisiones automáticamente. Pero también puede llegar a afectar a individuos que ni siquiera han participado en la aportación de datos, por el hecho de pertenecer a colectivos extrapolados a partir de los patrones o perfiles obtenidos". Cfr. "Responsabilidad proactiva en el tratamiento de datos masivos", ob. cit., p. 124. En sentido similar, MONASTERIO ASTOBIZA: "los algoritmos no existen independientemente de ideas, prácticas, instrumentos o contextos. Ideas que los profesionales de la ingeniería informática y ciencias de la computación tienen, muchas veces incluso de manera inconsciente en forma de prejuicios, sesgos, estereotipos que de manera flagrante se ven reflejadas en los mismos algoritmos que programan o la tecnología que diseñan". Cfr. "Ética algorítmica: implicaciones éticas de una sociedad cada vez más gobernada por algoritmos", ob. cit., p. 198.

justificación"[35]. Con esta visión acrítica, se viene a abrazar lo que HARARI ha denominado como una "religión de los datos"[36].

Los estudiosos nos advierten que si se mantiene constante el avance del *Big data* como forma de ordenación de los procesos sociales, podrían verse modificados los estándares de aproximación y aprehensión del conocimiento. De acuerdo con MAYER-SCHÖNBERGER y CUKIER, "ver el mundo como información, como océanos de datos que pueden explorarse cada vez más lejos y más hondo, nos ofrece un nuevo panorama de la realidad. Es una perspectiva mental que puede penetrar todas las áreas de la vida. Hoy formamos una sociedad aritmética porque presumimos que el mundo se puede comprender mediante los números y las matemáticas. Y damos por supuesto que el conocimiento se puede transmitir a través del tiempo y del espacio porque el concepto de la escritura está muy arraigado. Puede que el día de mañana las generaciones siguientes tengan una *conciencia de datos masivos*: la presunción de que hay un componente cuantitativo en todo cuanto hacemos, y de que los datos son indispensables para que la sociedad aprenda. La noción de transformar las innumerables dimensiones de la realidad en datos probablemente le parezca novedosa por ahora a la mayoría de la gente. Pero en el futuro, seguramente la trataremos como algo dado"[37].

Esta posibilidad presenta riesgos concretos, en tanto que el lenguaje matemático propio del cálculo algorítmico aspira a una pretensión de plenitud difícilmente compatible con el razonamiento crítico y la argumentación en base a principios que, especialmente en ámbitos como el propio de las ciencias jurídicas, no puede aceptar este carácter inmutable, en tanto que su desarrollo histórico está condicionado por la respuesta a las demandas sociales, que se tornan en nuevos desafíos a los que debe enfrentarse el Derecho. En esta tendencia se encuadra la crítica al pensamiento técnico del *Big data* formulada por GALPARSORO: "el cálculo es transparente, mientras que el pensamiento no es transparente para sí mismo; no sigue caminos previsibles, sino que se entrega a lo abierto, a lo desconocido, a lo que no se puede prever o

[35] Cfr. *Primero como tragedia, después como farsa*, ob. cit., p. 31.

[36] Cfr. HARARI. *Homo Deus. Breve historia del mañana*, Debate, Barcelona, 2016, p. 520.

[37] Cfr. *Big data. La revolución de los datos masivos*. ob. cit., pp. 122-123.

calcular por completo. El procesador no narra nada. Solamente hace cálculos: cuenta. En la sociedad de la transparencia o de la información no hay *tensión metafísica*, es decir, no hay ninguna aspiración a la *verdad*. No hay filosofía, en el sentido estricto del término. La masa de información no genera ninguna verdad, sino una paradójica y anestesiante sensación de vacua plenitud"[38].

Sobre esta cuestión, impera la necesidad de impugnar aquéllas formas de pensamiento que, amparadas en la técnica o la neutralidad, suponen una limitación de la capacidad crítica asentada en valores que se presentan como inmutables, y que por tanto deben ser aceptados con una confianza que se torna ciega. En este estado de cosas, se hace del todo necesaria una verdadera discusión pública sobre los límites de esta vida basada en el algoritmo, no buscando la impugnación completa del modelo, sino de aquéllas cuestiones que puedan limitar el libre desarrollo de la personalidad de la ciudadanía. Como sostiene GARCÉS, "el combate contra la credulidad no es el ataque a cualquier creencia. Las creencias son necesarias para la vida y el conocimiento. La credulidad, en cambio, es la base de toda dominación porque implica una delegación de la inteligencia y de la convicción"[39].

La preeminencia algorítmica acrítica, cuyos sesgos y consecuencias se han esbozado, sería especialmente asfixiante en el ámbito de las ciencias jurídicas, caso de instaurarse. No únicamente por la propia dinámica de reforma del ordenamiento jurídico en base a las necesidades sociales, sino también en la propia aplicación práctica de las normas jurídicas por los órganos jurisdiccionales. En este sentido, si consideráramos como irrefutable cualquier predicción desarrollada de acuerdo con el cálculo algorítmico, existirían dudas sobre la posibilidad de afirmar el libre albedrio como característica inherente del ser humano[40]. La responsabilidad podría diluirse dado que ésta quedaría probada en base al cumplimiento de los patrones en que se descompusiera el algoritmo. Esto conllevaría la aplicación de un modelo de

[38] Cfr. "Big data y psicopolítica. Vía de escape: de la vida calculable a la vida como obra de arte, *Dilemata,* nº 24, 2017, p. 27.

[39] Cfr. *Nueva ilustración radical*, Anagrama, Barcelona, 2017, p. 36.

[40] De acuerdo con ESPINOSA, cuando se pregunta ante los conflictos entre *Big data* y libertad: "¿dónde queda la autonomía humana ante una retroalimentación algorítmica infinita e independiente que puede decidir por sí misma?". Cfr. "Reflexiones antropolíticas sobre el mundo digital y la autonomía personal", *Dilemata,* nº 24, 2017.

justicia donde no se le exigiría a la ciudadanía adecuar su comportamiento a las normas jurídicas, en tanto que su conducta quedaría previamente restringida por su sumisión a las variables determinadas mediante los algoritmos. Así, sostienen MAYER-SCHÖNBERGER y CUKIER: "en la era de los datos masivos, tendremos que ampliar nuestra visión de la justicia y exigir que incluya salvaguardias para el albedrío humano, del mismo modo que, en la actualidad, velamos por la imparcialidad procesal. Sin esas salvaguardias, la idea misma de la justicia podría debilitarse por completo. Al garantizar la capacidad de decisión del ser humano, nos aseguramos de que el gobierno juzga nuestro comportamiento basándose en acciones reales, no simplemente en análisis de datos masivos. Así pues, sólo debe hacernos responsables de nuestras acciones pasadas, no de predicciones estadísticas de unas acciones futuras. Y cuando el estado juzgue actos anteriores, no debería basarse exclusivamente en datos masivos"[41].

En la dinámica expuesta en este punto entra en juego una de las contradicciones de la "modernidad líquida", esto es, la dificultad de poner el foco de la discusión pública en cuestiones que tienen un carácter eminentemente privado[42]. En este sentido, si bien el *Big data* tiene un alcance público, puesto que afecta a las formas de interacción social, así como a las políticas gubernamentales, las posibles vulneraciones de la privacidad tienen como destinataria la esfera personal de la ciudadanía. De acuerdo con BAUMAN, "los principales obstáculos que deben ser examinados con urgencia se relacionan con las crecientes dificultades que hay para traducir los problemas privados a problemáticas públicas, para galvanizar y condensar los problemas endémicamente privados bajo la forma de intereses públicos que sean mayores que

[41] Cfr. *Big data. La revolución de los datos masivos*. ob. cit., pp. 216-217.

[42] De acuerdo con MONASTERIO ASTOBIZA: "cuando procedimientos o protocolos automatizados (algoritmos) deciden por los seres humanos y encima lo hacen de manera sesgada y en contra de derechos y libertades civiles que las personas poseen se produce un fenómeno ético particular: el daño causado tiene difícil identificación para la rendición de cuentas y/o responsabilidad, la complejidad de la programación de los algoritmos impide corregir o enmendar, y/o dada la ubicuidad e invisibilidad de los algoritmos uno cree que cualesquiera efectos que produzcan (por muy negativos que resulten ser) hemos de aceptarlos porque así es como son las cosas y nada puede hacerse para evitarlo (conformidad y resignación). La falta de transparencia/opacidad, la complejidad/ubicuidad/invisibilidad y la conformidad/resignación ante los efectos de los algoritmos hace imposible aplicar reglas éticas particulares". Cfr. "Ética algorítmica: implicaciones éticas de una sociedad cada vez más gobernada por algoritmos", ob. cit., p. 197.

la suma de sus ingredientes individuales"[43]. En este sentido, se le reconoce al *Big data* una proyección pública, en tanto que supone una modificación en los presupuestos estructurales de determinadas prácticas sociales como el desarrollo de las políticas gubernamentales o la propia interacción social por parte de la ciudadanía. Ahora bien, las posibles vulneraciones ocasionadas por el cálculo algorítmico en la privacidad y el libre desarrollo de los ciudadanos se manifiesta en la esfera personal del sujeto[44]. Así las cosas, resulta del todo indispensable la apertura de una discusión pública sobre los límites de estas prácticas respecto de las vulneración de los derechos y libertades de la ciudadanía, rechazando en todo caso la imposición de valores inmutables u ontológicos basados en un conocimiento técnico que desnaturalice el significado social de las normas jurídicas.

2. *Dataveillance*: la normalización social de la cultura de la vigilancia

El concepto *dataveillance* ha sido acuñado por CLARKE para hacer referencia al uso sistémico de los procedimientos de tratamiento y análisis de datos masivos, con la finalidad de investigar o monitorizar las dinámicas de actuación o interacción social[45]. En este sentido, resulta de utilidad su mención en este apartado, en tanto que, como se está poniendo de manifiesto en este punto, el *Big data* como fenómeno de transformación social, tiene una incidencia transversal en el ordenamiento jurídico. En el presente apartado se analizarán las nuevas dinámicas e itinerarios de control social que se han abierto en este contexto digital.

El tratamiento de datos masivos, así como la preeminencia de las redes sociales en los procesos de comunicación social suponen un nuevo escenario al que han sabido adaptarse los sistemas de vigilancia y disciplina (*surveillance*) emanados del *Big data* (de ahí la adecuación del término *dataveillance*). Así las cosas, si bien un análisis en profundidad sobrepasaría la temática de esta investigación, sí serán ofrecidas unas pinceladas para que pueda efectivamente

[43] Cfr. *Modernidad líquida*, ob. cit., p. 57.

[44] Como apuntan MAYER-SCHÖNBERGER y CUKIER: "si las predicciones basadas en datos masivos fueran perfectas, si los algoritmos pudieran prever nuestro futuro con infalible claridad, no tendríamos elección para obrar en el futuro. Nos comportaríamos exactamente a tenor de lo predicho. De ser posibles las predicciones perfectas, quedaría negada la voluntad humana, nuestra capacidad de vivir libremente nuestras vidas. Y, además, no sin ironía, al privarnos de elección nos librarían de toda responsabilidad". Cfr. *Big data. La revolución de los datos masivos*. ob. cit., p. 200.

[45] Cfr. *Introduction to Dataveillance and Information Privacy*, Australian National University, 2006.

mostrarse el alcance de los procesos de tratamiento y análisis de datos masivos desde la perspectiva del control social, como se verá al desarrollar el concepto de *panóptico digital* como práctica que consolida el control social en las redes sociales como nuevo paradigma de vigilancia. Igualmente, deben considerarse los riesgos que suponen para la cohesión social las posibles prácticas discriminatorias que puedan derivarse de la ideología del algoritmo que orienta el *Big data*. En este sentido, la posible exclusión de colectivos e individuos dentro de este nuevo paradigma, así como las limitaciones en el disfrute de derechos y libertades púbicas pueden derivar en un proceso de segmentación social donde presupuestos estructurales de un Estado democrático de Derecho puedan verse socavados. Como ejemplo práctico de esta dinámica, será analizado el tratamiento por el sistema penal español de los delitos de enaltecimiento del terrorismo en las redes sociales, ámbito donde los riesgos que serán descritos parecen haberse materializado.

2.1. Panóptico digital: control social en la sociedad de la exposición

El concepto de *panóptico* fue originalmente desarrollado por el filósofo utilitarista JEREMY BENTHAM[46] (1748-1832). Básicamente, la doctrina del utilitarismo defendía la idea de que todo acto humano debe ser juzgado según el placer o el sufrimiento que reporta, con el objetivo de lograr la mayor felicidad para el mayor número de ciudadanos[47]. La interpretación del utilitarismo elaborada por este autor, tiene un fuerte arraigo en el entendimiento liberal ofrecido al capitalismo, no sólo en relación con la importancia del placer como baremo para medir la prosperidad del medio social, sino también por lo que respecta a la importancia del libre mercado. Para dicho autor, la mejor manera de maximizar el reparto del placer en sede social es facilitar un contexto de libre intercambio entre los participantes, de manera que, buscando cada uno su propio interés, pueda llegarse a un nivel óptimo de bienestar general. No obstante, para que esta ley mercantil propuesta por el *utilitarismo benthamiano* pueda funcionar

[46] Cfr. *Panóptico,* Círculo de Bellas Artes, Madrid, 2011.

[47] Como sintetiza RENDUELES en el prólogo a la edición reseñada: "Bentham convirtió este lugar común en una fuente de transformaciones políticas radicales. Básicamente, la colectividad máximamente feliz es la que facilita a los individuos que la componen la realización coherente de aquellas actividades que cada uno considera más placenteras". "Prólogo", *Panóptico,* Círculo de Bellas Artes, Madrid, 2011.

correctamente, es indispensable que no exista ninguna intromisión, sea estatal, moral o religiosa, que pueda limitar su funcionamiento[48].

La translación al ámbito del control social del pensamiento de BENTHAM se plasma en el concepto del *panóptico*. Se trata de un diseño arquitectónico y organizativo aplicable a cualquier institución donde sea necesaria la vigilancia: escuelas, hospitales, fábricas y, sobre todo, una prisión[49]. Arquitectónicamente, el *panóptico* es una construcción circular, donde las personas supervisadas habitan celdas individuales dispuestas a lo largo de la circunferencia del edificio, mientras que los vigilantes ocupan un torreón de vigilancia ubicado en el centro. Distintas construcciones dentro del propio *panóptico* (pasillos de distintas alturas, juegos de luces y sombras, desniveles…) permiten que el vigilante pueda observar a todos los reclusos desde la torre de vigilancia, con el valor añadido de que éstos no saben si están siendo efectivamente controlados por el supervisor, gracias a los dispositivos constructivos mencionados, pero también a que el vidrio de la torre de vigilancia es transparente para el observador, pero opaco para los observados. De este modo, el diseño arquitectónico del *panóptico* permite que los presos nunca puedan saber si están siendo vigilados, creándose por tanto un estado de vigilancia permanente, incluso en los supuestos donde no hay nadie en la torre, y por tanto no están siendo efectivamente vigilados[50].

De acuerdo con lo expuesto, la importancia de la propuesta de BENTHAM no es tanto el control efectivo que la torre de vigilancia pueda suponer para los reclusos, sino la *sensación de control permanente* que éstos experimentan mediante el *panóptico* como diseño arquitectónico del espacio de control. Como señala RENDUELES: "Bentham usó este microcosmos como una especia de laboratorio donde reconstruir las relaciones sociales sobre cimientos racionales y no

[48] Cfr. CIGÜELA SOLA. *Exclosos i transparentats. Del panòptic a la pantalla digital*, Institució Alfons el Magnànim, Centre Valencià d'Estudis i d'Investigació, València, 2017, p. 26.

[49] Cfr. RENDUELES. *Sociofobia. El cambio político en la era de la utopía digital*, Capitán Swing, Madrid, 2013, p. 26.

[50] Como señala CIGÜELA SOLA, el diseño arquitectónico propuesto por Bentham no requería siquiera que las personas que habitaran la torre de vigilancia fuera guardias reales. En este sentido, destaca su sugerencia de alojar en dicho espacio a la familia del vigilante, aumentando de este modo las probabilidades de que los reclusos pudieran ver a personas rondando los espacios de control, reforzando así ese permanente estado de vigilancia. Cfr. *Exclosos i transparentats. Del panòptic a la pantalla digital*, ob. cit., p. 27.

comunitarios. La clave tecnológica del panóptico es la permanente visibilidad de los prisioneros que, en cambio, nunca saben en qué momento están siendo observados desde el edificio central de vigilancia. La incertidumbre que provoca esta exposición total genera los mismos efectos que una supervisión con unos costes y una interacción personal mínimos"[51]. En efecto, no importa el número de vigilantes que habiten la torreta (puede incluso no haber ninguno), en tanto que lo que pretende BENTHAM con el *panóptico* desborda el control físico para entrar en el control mental de las personas supervisadas, que se saben permanentemente observadas contra su voluntad[52]. De este modo, lo que pretende con este modelo es una suerte de racionalización del control, de sometimiento de los egoísmos individuales para la satisfacción del interés general que se pretende preservar mediante la *vigilancia panóptica*.

El concepto de *panóptico* es revisitado por el pensador contemporáneo francés MICHEL FOUCAULT (1926-1984). En su obra *Vigilar y castigar. Nacimiento de la prisión*[53], desarrolla una teoría crítica del control social basada en la formalización del castigo a partir de los conceptos de poder disciplinario y vigilancia jerarquizada. En su obra, el autor francés supera las diferencias entre control social formal e informal, entendiendo ambos como parte de un único poder que actúa siguiendo un orden funcional sobre los cuerpos y las mentes de los reclusos.

Así las cosas, en su deconstrucción crítica del poder de vigilar y castigar, FOUCAULT reconoce un modelo de vigilancia jerarquizada funcional, en tanto que no distingue entre control social formal e informal. Esto supone que los dispositivos de policía, prisión, judiciales, actúan de forma conjunta y complementaria con las instituciones clásicas de control social informal, como la familia, escuela, iglesia, ocupación laboral…En suma, la vigilancia

[51] Cfr. *Sociofobia. El cambio político en la era de la utopía digital*, ob. cit., p. 27.

[52] Como se ha expuesto, el *panóptico* es aplicable a cualquier espacio requerido de vigilancia, siendo en todo caso garantía de orden. Como señala FOUCAULT: "si los detenidos son unos condenados, no hay peligro de que exista complot, tentativa de evasión colectiva, proyectos de nuevos delitos para el futuro, malas influencias recíprocas; si son enfermos, no hay peligro de contagio; si locos, no hay riesgo de violencias recíprocas; si niños, ausencia de copia subrepticia, ausencia de ruido, ausencia de charla, ausencia de disipación. Si son obreros, ausencia de riñas, de robos, de contubernios, de esas distracciones que retrasan el trabajo, lo hacen menos perfecto o provocan los accidentes". Cfr. *Vigilar y castigar. Nacimiento de la prisión*, Siglo XXI, Madrid, 2009, p. 204.

[53] *Ibid.*

jerarquizada supone en el pensamiento del pensador una nueva forma de organizar el control social, en tanto que desarrolla una nueva economía del castigo, basada en la distribución de este poder, de forma que no esté demasiado concentrado en algunos puntos privilegiados, ni tampoco dividido entre instituciones opuestas. Gracias a la vigilancia jerarquizada, "el poder disciplinario se convierte en un sistema *integrado* vinculado del interior a la economía y a los fines del dispositivo en que se ejerce. Se organiza también como un poder múltiple, automático y anónimo; porque si es cierto que la vigilancia reposa sobre individuos, su funcionamiento es el de un sistema de relaciones de arriba abajo, pero también hasta cierto punto de abajo arriba y lateralmente. Este sistema hace que *resista* el conjunto, y lo atraviesa íntegramente por efectos de poder que se apoyan unos sobre otros; vigilantes perpetuamente vigilados"[54].

Si bien puede admitirse la abstracción en las tesis del autor francés, la aplicación práctica de su pensamiento es perfectamente coherente. Lo que viene a expresar mediante el concepto de vigilancia jerarquizada es la existencia de una *control permanente,* en tanto que éste no se limita a las instituciones clásicas de control social formal, sino que se entiende extensivo al conjunto del medio social, en todo el proceso de interacción afectiva, espiritual, educativa o laboral del individuo con las instancias propias del control social informal.

En este punto, FOUCAULT refundamenta el *panóptico* de BENTHAM, considerando que el propio medio social puede actuar como el diseño arquitectónico de prisión propuesto por el pensador utilitarista inglés. Sobre esta cuestión, el *panóptico* dejará de ser un espacio cerrado de reclusión, sino que la propia vida, la existencia del individuo, pasará a ser el nuevo *panóptico* donde el poder disciplinario tendrá un alcance funcional gracias al concepto de vigilancia jerarquizada. De acuerdo con lo expuesto, FOUCAULT considera exitoso el concepto de *panóptico* (tanto en la formulación inicial como en su actualización), en tanto que permite "inducir un estado consciente y permanente de visibilidad que garantiza el funcionamiento automático del poder. Hacer que la vigilancia sea permanente en sus efectos, incluso si es discontinua en su acción. Que la perfección del poder tienda a volver inútil la actualidad de su ejercicio […] Panóptico funciona como una especia de laboratorio de poder.

[54] *Ibid*., p. 182.

Gracias a sus mecanismos de observación, gana en eficacia y en capacidad de penetración en el comportamiento de los hombres; un aumento de saber viene a establecerse sobre todas las avanzadas del poder, y descubre objetos que conocer sobre todas las superficies en las que éste viene a ejercerse"[55].

En suma, para FOUCAULT el *panóptico* no actuará únicamente como un espacio permanente de vigilancia, sino que permitirá determinar el comportamiento de los individuos, en tanto que la visibilidad del comportamiento del sujeto, gracias a la vigilancia jerarquizada, llevará a éste a modular sus actos para adecuarlos a lo que el medio social entiende como norma estandarizada. Éste será el propósito último del *panóptico* de acuerdo con la visión crítica del pensador, la *normalización* de las conductas de los ciudadanos, mediante la aplicación funcional en el medio social del poder disciplinario. No obstante, como bien advierte el autor francés, lo que las instituciones disciplinarias terminan consiguiendo mediante este proceso de *normalización*, no es más que una homogeneización basada en la exclusión, mediante la coacción de la libertad que supone entender la vida en sociedad como un espacio de control permanente.

Una vez realizada esta primera aproximación al concepto de *panóptico* en el pensamiento de BENTHAM y FOUCAULT, entramos a analizar cómo, en el contexto del *Big data* es posible apreciar un salto cualitativo que lleve a reconocer el *panóptico digital*. Para ello, puede partirse de lo que el filósofo surcoreano BYUNG-CHUL HAN ha denominado como *sociedad de la transparencia*[56]. Para éste último, la transparencia viene unida al concepto de exposición, elemento estructural de lo que denomina como sociedad positiva. De acuerdo con su pensamiento, "la omnipresente exigencia de transparencia, que aumenta hasta convertirla en un fetiche y totalizarla, se remonta a un paradigma que no puede reducirse al ámbito de la política y la economía. La sociedad de le negatividad se desmonta cada vez más a

[55] *Ibid*., p. 204.

[56] Cfr. *La sociedad de la transparencia*, Herder, Barcelona, 2013.

favor de la positividad. Así, la sociedad de la transparencia se manifiesta en primer lugar como una *sociedad positiva*"[57].

La noción de transparencia elaborada por el filósofo surcoreano desborda el entendimiento habitual referido a la corrupción y la libertad de información, considerando la transparencia como un mecanismo coactivo que, paradójicamente, limita la libertad de pensamiento en el ámbito de una sociedad que, y aquí radica su calificación como *positiva*, desalienta la *negatividad* entendida como disenso con lo establecido. Esto es así porque la *sociedad positiva* basada en la transparencia exige una necesaria plenitud en su construcción, en tanto que todo debe ser observable, analizable y medible. Por el contrario, lo *negativo* representa, en términos *hegelianos*[58], un espacio para la contradicción dialéctica, para la generación del conflicto, inasumible por una *positividad* que niega el pensamiento para terminar convirtiéndose en mero cálculo[59]. Como señala HAN, "la transparencia forzosa estabiliza muy efectivamente el sistema dado. La transparencia es en sí misma positiva. No mora en ella aquella negatividad que pudiera cuestionar de manera radical el sistema económico-político que está dado. Confirma y optima tan solo lo que existe"[60].

Desde esta *sociedad de la transparencia* descrita por HAN se transita fácilmente a lo que se ha denominado como *sociedad de la exposición*[61]. En ésta, se reconoce la necesidad que sienten las personas por exponerse, no sólo inducidos por el fetichismo digital impuesto por las

---

[57] *Ibid.,* p. 11.

[58] La teoría dialéctica de Hegel parte de la contradicción entre dos ideas enfrentadas (tesis y antítesis) para terminar presentando una comprensión hermenéutica del conflicto del que resulta la solución (síntesis). Esta es una contribución fácilmente aplicable a cualquier modificación en el ordenamiento jurídico. Por ejemplo, en los primeros años de la transición española, arrastrando todavía la moral y cultura heredada del franquismo, no se contemplaba la posibilidad de permitir el divorcio, en tanto que esté se consideraba como una unión sagrada e indisoluble en base a su entendimiento religioso (tesis). Ahora bien, los avances sociales, la necesidad de modernizar el ordenamiento jurídico, así como la propia institución del matrimonio entendida en términos laicos, de acuerdo con su regulación en el Código Civil, lleva a determinados sectores a defender la aprobación de una ley que permita el divorcio, en términos de igualdad para las dos personas que integran la relación matrimonial (antítesis). Fruto de la discusión parlamentaria, el 22 de junio de 1981 el Congreso de los Diputados aprueba la Ley del Divorcio, resultado de la comprensión dialéctica de la contradicción entre ambas posturas.

[59] *Ibid*., p. 17.

[60] Cfr. *La sociedad de la transparencia*, ob. cit., p. 22.

[61] *Ibid.,* pp. 25 ss. Asimismo, puede destacarse la siguiente aportación: HARCOURT. *Exposed. Desire and Disobedience in the Digital Age*, Harvard University Press, Cambridge, 2015.

redes sociales, sino porque representa la única forma de existir, de proyectarse en el medio social. De este modo, cada sujeto es su propio objeto de publicidad, todo se mide en su valor de exposición[62]. Como reconoce HARCOURT, "vivimos en unas condiciones políticas y sociales que están transformando radicalmente la forma en que interaccionamos los unos con los otros, nuestro orden socio-político, y a nosotros mismos: la transparencia está reconfigurando dramáticamente el medio social y las políticas públicas, modificando las formas de manifestación del poder. El nuevo poder de la exposición ordena y distribuye de forma ininterrumpida nuestra identidad digital"[63].

¿Cómo se aplica este estado de cosas al concepto de *panóptico*? Como se ha adelantado, en el contexto del *Big data* la noción desarrollada por BENTHAM y FOUCAULT se adapta a la nueva realidad fruto de la revolución digital para constituir una nueva cultura de la vigilancia. El cambio cualitativo más relevante del *panóptico digital* es que sobre la figura del supervisado no se aplica ningún tipo de poder coactivo, como si ocurría en los paradigmas anteriores. No existe aquí una celda, tampoco una torre de vigilancia sobre la que construir el control permanente ideado por BENTHAM. Tampoco el jefe de la fábrica que supervisa a los trabajadores, o el maestro que castiga a los alumnos en el paradigma foucaultiano. En el *panóptico digital* somos los vigilados los que voluntariamente asumimos ese papel. Nos convertimos en actores y víctimas de un modelo de vigilancia *totalizador* que se extiende a todos los aspectos de nuestra vida diaria. De este modo, cada uno termina siendo el *panóptico* de si mismo. De acuerdo con HAN, "lo que garantiza la transparencia no es la soledad mediante el aislamiento, sino la hipercomunicación. La peculiaridad del panóptico digital está sobre todo en que sus moradores mismos colaboran de manera activa en su construcción y en su conservación, en cuanto se exhiben ellos mismos y se desnudan"[64].

En consecuencia, todo queda dentro del *panóptico digital*, de modo que, paradójicamente, la vigilancia sin coacción supone que ésta no sea considerada como un ataque

[62] Cfr. *La sociedad de la transparencia*, ob. cit., p. 29.

[63] Cfr. *Exposed. Desire and Disobedience in the Digital Age*, ob. cit., p. 15.

[64] Cfr. *La sociedad de la transparencia*, ob. cit., p. 89.

a la libertad, facilitando la entrega voluntaria de la ciudadanía a la mirada del *panóptico digital*[65]. Y aquí es donde resulta importante la referencia al *Big data,* así como la construcción de herramientas jurídicas que permitan que este nuevo hábitat de vigilancia pueda al menos atender a un estándar mínimo de protección de la privacidad. Cuando los pasos que damos en el mundo digital pueden suponer una observación perpetua, es necesario dotarse de instrumentos para proteger los derechos de los ciudadanos que, obligados por las propias dinámicas sociales, se prestan voluntariamente para pasar a ser parte de este *panóptico digital*. Como sostiene GALPARSORO, "cada clic que se hace en la Red queda registrado, dejamos constantemente huellas digitales, que pueden ser fácilmente rastreadas. Nuestras vidas pueden ser reproducidas por completo. Por eso, el lugar del *Big Brother* es ocupado por el *Big Data*. Ya vimos cómo los habitantes del panóptico digital no se sienten prisioneros, sino que viven la ilusión de la libertad. Cada uno de ellos es un vigilante en potencia que, voluntariamente, expone todos sus datos con la mayor transparencia posible"[66].

Efectivamente, esta dinámica es correcta; el *Big data* supone el advenimiento de una versión mejorada del Gran Hermano de Orwell, y seria una negación de la realidad considerar que este contexto no vaya a mantenerse y aumentar cualitativamente con el paso de los años. Por esta razón, el desarrollo del derecho al olvido como derecho fundamental supone una necesidad imperante en el avance de la ciencia jurídica, en tanto que ésta requiere de una adaptación al contexto expuesto, para así garantizar la seguridad jurídica y la protección de los derechos y libertades de la ciudadanía. Sólo de este modo podría atenuarse al auge de la cultura de la vigilancia que supondría un *panóptico digital* contra el que no pudiera oponerse de forma concreta un derecho fundamental que respondiera a la situación de necesidad descrita.

[65] Cfr. GALPARSORO. "*Big Data* y Psicopolítica. Vía de escape: de la vida calculable a la vida como obra de arte", ob. cit., p. 28.

[66] *Ibid*., p. 30.

2.2 Exclusión y segmentación social en el *Big data*

Como se ha expuesto anteriormente[67], no puede reconocerse el *Big data*, ni tampoco el proceso técnico seguido para el análisis y tratamiento de datos masivos como un fenómeno neutral o meramente científico. En este sentido, se han desarrollado los argumentos para rebatir este carácter supuestamente apriorístico relativo al empleo de algoritmos para desarrollar la utilización de los datos masivos. Sobre esta cuestión, han sido reconocidos los riesgos de legitimar cualquier tipo de decisión basada en los cálculos algorítmicos por su supuesto carácter científico, y en consecuencia pretendidamente neutral, en tanto que las variables utilizadas como muestras sobre las que inciden los algoritmos pueden responder a una serie de consideraciones motivadas por razonamientos de tipo político, económico o social.

Por lo tanto, si bien los algoritmos se atienen a una lógica científica-matemática, hemos visto como la forma en que éstos sean proyectados al estudio de los procesos sociales responderá a unas coordenadas ideológicas concretas y, por tanto, según hemos advertido ya, existe el riesgo cierto de que se produzca un proceso reduccionista y simplificador de etiquetaje respecto de determinados colectivos, a partir de prácticas discriminatorias de tipo social o económico, que pueden determinar una segregación excluyente de los grupos afectados. La consumación usual de estos procesos da lugar, según ciertos autores, a la creación de una *sociedad de clases digital*[68].

Sobre esta cuestión, puede resultar pertinente el caso presentado por MONASTERIO ASTOBIZA como ejemplo de discriminación social, en tanto que tiene por objeto algo tan cotidiano como el nombre de las personas[69]. La página web francesa *Ton prenom*[70]*,* portal que sirve de enciclopedia para facilitar la elección del nombre de los recién nacidos, utiliza un algoritmo que discrimina en contra de ciertos nombres personales y a favor de otros. Los

---

[67] Vid., *supra* Cap. I. 1. II.

[68] Cfr. HAN. *Psicopolítica*, ob. cit., p. 99.

[69] Cfr. "Ética algorítimica: implicaciones éticas de una sociedad cada vez más gobernada por algoritmos", ob. cit., pp. 198-200.

[70] http://tonprenom.com/bebe

padres primerizos que quieren elegir el nombre para sus hijos pueden recurrir a sus servicios, pero habrán de tener en cuenta que el algoritmo de esta página asume por defecto que se desea evitar un nombre de origen árabe. Como apunta MONASTERIO ASTOBIZA, "el algoritmo deja marcada por defecto la opción de *favorecer* un nombre de origen francés, marca por defecto la opción *indiferente* para los nombres de origen inglés o judío, pero marca la opción *evitar* para nombres de origen árabe"[71]. Como puede verse, este caso presenta de qué manera los algoritmos, si bien son un producto técnico-científico, pueden responder a una determinada opción ideológica que puede predeterminar su incidencia en los procesos sociales. En este sentido, la discriminación social producida por dicho algoritmo no sería asumible, en tanto que muestra de forma explícita un sesgo atendiendo a la procedencia étnica de los nombres.

Además de los casos de discriminación social, el *Big data* también puede incurrir en casos de discriminación económica, si bien en muchos de los supuestos existirá una correlación entre ambas categorías. Piénsese en las personas que viven en los *márgenes* del *Big data*, aquéllas que debido a causas diversas (pobreza, geografía, estilo de vida…), no son *datificados*, distorsionando a favor de las mayorías integradas en el sistema económico y social la orientación de la lógica algorítmica que orienta el tratamiento y análisis de los datos masivos[72].

Siguiendo con esa posible discriminación entre colectivos, consideremos los hábitos de dos personas distintas para poner de manifiesto estas diferencias. La primera es Carlota, joven residente en Madrid, barrio de Malasaña, diseñadora de 28 años que participa del *Big data* en los hábitos comunes que se le pueden atribuir a partir de su posición geográfica y perfil demográfico y profesional. Se comunica diariamente con su Smartphone, consume productos audiovisuales mediante Netflix, escucha música en Spotify y compra en Amazon. Actualiza diariamente su muro de Facebook, opina sobre política en Twitter y su Instagram esta repleto de sus fotografías y vídeos. Utiliza tarjetas de debito y crédito para todas sus compras, además de gestionar desde su Smartphone sus cuentas bancarias. Como puede imaginarse, Carlota genera datos de forma incesante, que tendrán una valoración económica importante para las

[71] Cfr. "Ética algorítimica: implicaciones éticas de una sociedad cada vez más gobernada por algoritmos", ob. cit., p. 199.

[72] Cfr. LERMAN "Big data and its exclusions", *Stanford Law Review*, 66, 2013, p. 57.

empresas encargadas de su explotación, pero que también determinarán ciertos estándares o parámetros que vendrán a orientar el cálculo algorítmico, resultando Carlota beneficiaria indirecta de un sistema económico y social que prima su conducta, en tanto que normalizada a los hábitos propios del *Big data*. No ocurrirá lo mismo, con Manuel, de 38 años, residente en Vallecas, trabajador sin cualificación en distintas empresas asociadas a la construcción, pero parado desde 2007. Manuel sólo cobra dinero sin declarar en trabajos ocasionales de pintura y mantenimiento, de forma que todas sus compras en las tiendas de su distrito suelen ser en efectivo. Si bien tiene un Smartphone, no utilizada aplicaciones por no tener la tarifa de datos contratada, simplemente se limita a llamar por teléfono. Las pocas ocasiones en que utiliza Internet lo hace gracias al WiFi de la biblioteca municipal. En este caso, Manuel no aporta gran cosa al mercado de los datos masivos, pero además, sus patrones o preferencias no son tenidas en cuenta para la gestión de los algoritmos.

Si comparamos ambos casos, puede apreciarse de qué manera el *Big data* prima a determinados colectivos que se encuentran más conectados a los hábitos propios de la revolución digital. No obstante, debe considerarse que en muchas ocasiones esto no será una elección propia de la persona, sino que responderá a la posición económica que ocupe. Los casos de discriminación económica y social pueden llevar en casos extremos a la exclusión, a la creación de colectivos silenciados, en tanto que no se atiende a sus preferencias o comportamientos para la oferta de bienes y servicios por el Mercado e incluso, la atención y asistencia por parte de los poderes públicos. De acuerdo con SOLOVE, esta situación no sólo afecta al desarrollo del medio social, dado que supone una ruptura de las expectativas que determinados colectivos albergan en los poderes públicos, sino que "afecta a la estructura social en tanto que altera la confianza de la ciudadanía en las instituciones, suponiendo una situación de frustración y desamparo"[73].

Por otra parte, existen determinados espacios de participación pública asociados a la democracia representativa que pueden verse afectados por el *Big data*. Sin entrar en los

[73] Cfr. SOLOVE, D. "I've got nothing to hide and other misunderstandings of privacy", *San Diego Law Review*, 2007, p. 757.

supuestos donde el *Big data* puede suponer una limitación a la libertad de expresión, resulta significativa la creciente importancia de los datos masivos en la planificación de las campañas electorales de los partidos políticos. Obviamente, la posibilidad de establecer una comunicación más directa entre candidatos y electores es uno de los puntos fuertes de los cambios que en este ámbito suponen las redes sociales. No obstante, más allá de la posibilidad de aumentar los espacios para la conformación de una discusión pública en el desarrollo de las campañas electorales, resulta preocupante que el tratamiento de los datos masivos aplicado en la contienda política pueda tener como consecuencia la creación de bases de datos conformadas de acuerdo con parámetros ideológicos. Como apunta GARCÍA MAHAMUT, "Si no fortalecemos los aspectos legales referidos a que los partidos puedan a través de la tecnología realizar acopio masivo de datos personales de electores y potenciales votantes, lo que les permitirá sin demasiados problemas realizar una mega base de datos de perfil ideológico, nos encontraremos ante muy serios y graves problemas. El tratamiento de la información personal por nuevas tecnologías que hacen un uso masivo y profundo de los datos personales alcanzará un impacto en la esfera privada sin parangón. Si la información personal a cada minuto que pasa alcanza un mayor valor económico, el de las preferencias políticas resultará incalculable"[74].

Como se puede observar, los datos no son neutrales en la medida en que están sujetos a todo tipo de condicionamientos, desde el diseño tecnológico hasta el soporte digital en el que son utilizados, así como las finalidades para las cuales se emplean. Ello produce sin ningún lugar a dudas, problemas de discriminación de diversa índole, en tanto que su parcialidad, consciente o inconscientemente, parece ser inevitable.

El empleo indiscriminado del *Big data* tiene consecuencias sociales, políticas y económicas reales, hoy en día puestas de relieve, de la mayor actualidad, por el uso de *bots* y por las *Fake news*, abonando un campo de cultivo para la posverdad sin precedentes[75]. Si bien

[74] Cfr. "Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español", *UNED. Teoría y Realidad Constitucional*, nº 35, 2015, p. 334.

[75] Como ejemplo, el *chatbot* Tay (sistema virtual de imitación del comportamiento humano capaz de generar conversaciones que simulan el lenguaje de las personas) diseñado por Microsoft para contestar las preguntas que los internautas quisieran

es cierto que las noticias falsas no son una novedad, sí que lo es su volumen pues la interacción entre la tecnología, los medios de comunicación y el comportamiento social vigentes, han provocado un aumento exponencial de su producción, propagación y alcance. Como ejemplo, la gran incidencia que en el año 2016 tuvo el sembrado intencionado y masivo de *Fake news* tanto en las elecciones presidenciales de EEUU como en el referéndum británico del *Brexit*, posibilitando que el *Big data* influyera decisivamente en la configuración de las democracias liberales[76].

El *Big data* está lleno de prejuicios, ideologías, sesgos e intencionalidades funcionando libremente sin ningún tipo de sometimiento al control democrático. Ello puede observarse en el sesgo ideológico de los buscadores web, que posicionan los resultados en función de sus propios criterios –éstos, además, están abiertos a acuerdos comerciales pues ciertamente existe un mercado donde comprar un mejor posicionamiento web– o de las redes sociales que, mediante el uso de algoritmos, proporcionan a sus usuarios informaciones afines a su ideología así como les sugieren contenido contrastadamente vinculado a sus intereses, limitando con ello la capacidad crítica de los usuarios. Es por ello que puede concluirse, sin margen de error, que ni la tecnología, ni los datos ni los algoritmos son asépticos ni neutrales pues, detrás de ellos se esconden intereses partidistas (políticos, empresariales, etc.) o subconscientes de aquéllos quienes los han desarrollado, ostentan su propiedad o gozan de cualquier otra posición de dominio.

2.3 Límites a la libertad de expresión en la era digital: el caso del enaltecimiento del terrorismo en redes sociales

Como hemos observado, el denominado *panóptico digital* representa un nuevo paradigma en el estudio del control social. En este ámbito, las redes sociales suponen una

---

hacerle así como entablar conversaciones, que tuvo que ser retirado en menos de 24h desde su puesta en funcionamiento al convertirse en un robot machista, homófobo y racista que, entre otras cosas, negaba el genocidio nazi o apoyaba la construcción de un muro entre EEUU y México.

[76] La ICO, organismo británico análogo a la AEPD sobre el que se incidirá en Capítulos posteriores, abrió una investigación sobre la compañía de datos *Cambridge Analytica* para investigar su papel en las elecciones presidenciales norteamericanas así como en la campaña pro-*Brexit,* tras saberse que pudo manipular hasta 50 millones de perfiles de usuarios de *Facebook* con fines propagandísticos.

nueva realidad, una modificación en los usos de una ciudadanía que adapta su forma de comunicarse y expresarse en el medio social. Siguiendo con la tesis de HAN sobre la *sociedad de la transparencia*, la dependencia de la ciudadanía por las redes sociales, así como la exacerbación del individualismo que representan, supone un paso más en el nuevo itinerario de control social representado por el *panóptico digital*. De este modo, la necesidad de la ciudadanía por encontrarse conectados a la Red muestra de forma palpable cómo puede desnaturalizarse algo tan cotidiano como expresar una opinión o un sentimiento, resultado de esta malentendida *transparencia* que en determinados supuestos tiene como consecuencia la banalización de una noción tan básica en un Estado democrático de derecho como la libertad de expresión. La generalización de estos usos entronca con la realidad expuesta en el apartado precedente, en tanto que la normalización social de la cultura de la vigilancia puede facilitar, paradójicamente, una limitación en los derechos y libertades de determinados colectivos, fruto de la exclusión y segmentación social que representa el tratamiento de los datos masivos para la creación de nuevos ámbitos de control social.

Una vez concluida la exposición de este escenario, mostraremos en el presente apartado una dimensión aplicada de cómo el *panóptico digital*, es decir, la existencia de un espacio de vigilancia permanente, facilita la limitación insospechada del ejercicio de derechos y libertades de ciudadanía trasladados al uso de las redes sociales. En ellas, las personas usuarias, en cuanto opinadoras activas que se dirigen a un círculo que consideran afecto (en cierto modo íntimo, enmarcable subjetivamente dentro de su área de privacidad), pero en realidad autoexpuestas ante todo un público indiscriminado, no parecen ser conscientes del ámbito potencialmente extensivo con que su proceder adquiere transcendencia pública y, en consecuencia, las responsabilidades que de ello pueden derivarse. Unas responsabilidades que serán analizadas en relación con el tratamiento ofrecido por el sistema penal español al delito de enaltecimiento del terrorismo y humillación a las víctimas.

Afirmaremos, ya de partida, que resulta harto discutible la dilatación de este comportamiento delictivo, con la pertinente limitación de la libertad de expresión, a la manifestación en redes sociales de opiniones políticas, humor negro o cualquier otro parecer

que pueda resultar ofensivo según qué estándares morales. Sobre esta cuestión, será comentada la preocupante modificación introducida por la Ley Orgánica 2/2015, de 30 de marzo, de reforma del Código Penal en materia de delitos de terrorismo, en tanto que introduce una modalidad agravada de los delitos de enaltecimiento del terrorismo y humillación a las víctimas cuando estos comportamientos sean llevados a cabo mediante el uso de redes sociales.

De acuerdo con la redacción vigente tras la reforma operada por la LO 2/2015, el artículo 578 CP dispone lo siguiente en sus dos primeros apartados:

> **1.** *El enaltecimiento o la justificación públicos de los delitos comprendidos en los artículos 572 a 577 o de quienes hayan participado en su ejecución, o la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares, se castigará con la pena de prisión de uno a tres años y multa de doce a dieciocho meses. El juez también podrá acordar en la sentencia, durante el período de tiempo que él mismo señale, alguna o algunas de las prohibiciones previstas en el artículo 57.*
>
> ***2.*** *Las penas previstas en el apartado anterior se impondrán en su mitad superior cuando los hechos se hubieran llevado a cabo mediante la difusión de servicios o contenidos accesibles al público a través de medios de comunicación, internet, o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información.*

Si bien la redacción del apartado primero mantiene la conducta típica respecto de los actos de enaltecimiento o justificación del terrorismo, además de aquéllos que suponen un menosprecio o humillación para las víctimas de actos terroristas, la LO 2/2015 ha introducido una modificación cualitativa que debe ser tenida en cuenta respecto del análisis de este precepto. En la redacción inicial del delito de enaltecimiento del terrorismo y humillación a las víctimas, de acuerdo con la LO 7/2000 que modifica el Código Penal, se entiende cometida la conducta típica de enaltecimiento correspondiente al art. 578.1 CP cuando dicha exaltación o justificación de la actividad terrorista, así como la humillación a las víctimas sea realizada "por cualquier medio de expresión pública o difusión". De este modo, se entendía que la modalidad

genérica del delito de enaltecimiento debía cometerse utilizando medios de expresión o difusión públicos que faciliten así dicha exaltación o justificación de la actividad terrorista. Por lo tanto, se le atribuía al delito de enaltecimiento un necesario carácter público, para que así fuera posible reconocer los elementos objetivos del tipo genérico, esto es, la difusión exitosa en la esfera pública de un mensaje que ensalzara la actividad terrorista.

Sin embargo, con la reforma operada se produce una redefinición conceptual en la acotación típica del delito de enaltecimiento del terrorismo que supone una modificación cualitativa en su tratamiento, tanto político-criminal como penológico. Pese a mantener el enunciado que se castigará "el enaltecimiento o la justificación públicos" de los delitos de terrorismo, ha desaparecido de esta definición típica la referencia a que esta expresión pública deba ser llevada a cabo "por cualquier medio de expresión pública o difusión", como quedaba recogido en la formulación original fruto de la LO 7/2000. En su lugar, el legislador penal ha optado por redactar un apartado segundo, donde se establece que la pena prevista en el art. 578.1 CP para el delito de enaltecimiento del terrorismo y humillación a las víctimas (prisión de 1 a 3 años y multa de 12 a 18 meses), se impondrá en su mitad superior "cuando los hechos se hubieran llevado a cabo mediante la difusión de servicios o contenidos accesibles al público a través de medios de comunicación, internet, o por medio de servicios de comunicaciones electrónicas o mediante el uso de tecnologías de la información", lo que revela una voluntad del legislador básicamente centrada en las redes sociales de consumo masivo.

De acuerdo con lo expuesto, como señala CORRECHER MIRA, el punto de crítica a la modificación del art. 578 CP mediante la LO 2/2015 parece claro: "prácticamente ha quedado desvirtuado el contenido del art. 578.1 CP, en la medida en que difícilmente podrán hacerse públicos aquéllos actos de enaltecimiento o humillación a las víctimas que no sean expresados mediante el uso de servicios o contenidos puestos a disposición del público a través de medios de comunicación (televisión, prensa, radio), internet (redes sociales) o cualquier otro tipo de servicio derivado de las tecnologías de la información. Así las cosas, el apartado primero quedaría limitado a la difusión de opiniones emitidas públicamente ante una concurrencia de personas o, aunque pueda sonar paradójico, a la expresión pública de una opinión en un ámbito

privado. Por lo demás, el tipo agravado del art. 578.2 CP pasaría a convertirse *de facto* en la modalidad genérica del delito de enaltecimiento del terrorismo y humillación a las víctimas, tanto por la necesaria proyección pública establecida en los requisitos objetivos del tipo, como teniendo en cuenta que el contexto socio-comunicativo resultante de la revolución digital facilita que puedan apreciarse los delitos de enaltecimiento o humillación a las víctimas a través de la expresión de opiniones mediante las redes sociales. En consecuencia, el tratamiento jurídico-penal de este delito supondría llegar a una situación tal de absurdo que para reconocer los elementos objetivos del tipo genérico fuera necesario aplicar la modalidad agravada del delito"[77].

A través de esta cita, puede reconocerse en la crítica realizada por su autor la confusión entre las fronteras de lo *público* y *privado* expuesta por BAUMAN como uno de los rasgos más reconocibles de la "modernidad líquida". Esto es así porque la reforma introducida en el art. 578.2 CP supone una modalidad agravada que encuentra su fundamentación en el papel de preeminencia de las redes sociales en los procesos de interacción social, en tanto que reconoce ésta como la vía más adecuada para la propagación del supuesto mensaje enaltecedor, pese al carácter personal que puede tener la información emitida en las redes. El comentario reseñado es sólo una de las muchas muestras de incoherencia del legislador penal español en la regulación de estas conductas, como también lo es la posibilidad de que en aplicación de este tipo agravado se imponga la pena prevista para el art. 578.1 CP (prisión de 1 a 3 años) en su mitad superior, lo que podría suponer la entrada en prisión sin siquiera existir antecedentes penales por parte del ciudadano que comete este delito de opinión, en tanto que no sería aplicable la institución de la suspensión de la pena privativa de libertad[78].

---

[77] Cfr. "El delito de enaltecimiento del terrorismo y humillación a las víctimas tras la reforma de la LO 2/2015 en materia de delitos de terrorismo", *Revista General de Derecho penal*, nº 27, 2017, p. 5.

[78] *Ibidem*. La suspensión de la pena se encuentra regulada en el art. 80 CP, siendo uno de sus requisitos que la pena sea inferior a 2 años. Para el caso comentado, la aplicación en su mitad superior de una pena de 1 a 3 años sería necesariamente superior a 2 años, dado que el límite mínimo seria de 2 años y 1 día. De acuerdo con el art. 80 CP: **1.** Los jueces o tribunales, mediante resolución motivada, podrán dejar en suspenso la ejecución de las penas privativas de libertad no superiores a dos años cuando sea razonable esperar que la ejecución de la pena no sea necesaria para evitar la comisión futura por el penado de nuevos delitos. Para adoptar esta resolución el juez o tribunal valorará las circunstancias del delito cometido, las circunstancias personales del penado, sus antecedentes, su conducta posterior al hecho, en particular su esfuerzo para reparar el daño causado, sus circunstancias familiares y sociales, y los efectos que quepa esperar de la propia

Con este panorama, la agravación contenida en el art. 578.2 CP muestra de qué manera el contexto definido como *panóptico digital*, es decir, en la habitual autoexposición en las redes, genera un nuevo espacio de control social donde, a tenor de esa norma, es posible la aplicación del Derecho penal en supuestos donde no está suficientemente claro que la conducta exhibida pueda ser efectivamente constitutiva de delito. Ciertamente, la interpretación extensiva del delito de enaltecimiento del terrorismo y humillación a las víctimas en los supuestos realizados mediante el uso de las redes sociales plantea fundadas dudas en tanto que cercenar y penar su exteriorización implica una limitación de la libertad de expresión que no podría justificarse por mucho que en dichas conductas el contenido de la manifestación pudiera causar un daño o indignación social. Esto debe ser así porque de lo contrario, si se permitiera una extensión del bien jurídico protegido en los delitos de enaltecimiento a cláusulas generales del tipo "daño social", o incluso a la propia supresión del concepto de bien jurídico[79], se terminaría legitimando el castigo del propio contenido político o ideológico que pudiera ser coincidente con el que remotamente pudiera orientar una actividad terrorista[80]. Sobre esta cuestión, podría hacerse referencia al principio de proporcionalidad para analizar la redacción típica del art. 578 CP en relación con la llamada *función dogmática del efecto de desaliento*[81], esto es, considerando las limitaciones en los derechos y libertades fundamentales –libertad de expresión en este caso– que derivan de la sanción desproporcionada de comportamientos

suspensión de la ejecución y del cumplimiento de las medidas que fueren impuestas. **2.** Serán condiciones necesarias para dejar en suspenso la ejecución de la pena, las siguientes:

1.ª Que el condenado haya delinquido por primera vez. A tal efecto no se tendrán en cuenta las anteriores condenas por delitos imprudentes o por delitos leves, ni los antecedentes penales que hayan sido cancelados, o debieran serlo con arreglo a lo dispuesto en el artículo 136. Tampoco se tendrán en cuenta los antecedentes penales correspondientes a delitos que, por su naturaleza o circunstancias, carezcan de relevancia para valorar la probabilidad de comisión de delitos futuros.

2.ª Que la pena o la suma de las impuestas no sea superior a dos años, sin incluir en tal cómputo la derivada del impago de la multa.

3.ª Que se hayan satisfecho las responsabilidades civiles que se hubieren originado y se haya hecho efectivo el decomiso acordado en sentencia conforme al artículo 127.

[79] Cfr. PORTILLA CONTRERAS. "Los excesos del formalismo jurídico neofuncionalista en el normativismo del Derecho penal", *Revista General de Derecho penal*, nº 4, 2000, p. 2.

[80] Cfr. MIRA BENAVENT. "Algunas consideraciones político-criminales sobre la función de los delitos de enaltecimiento del terrorismo y humillación a las víctimas del terrorismo", en *Terrorismo y contraterrorismo en el Siglo XXI. Un análisis penal y político criminal* (Pérez Cepeda Dir.), Ratios Legis, Salamanca, 2016, p. 105.

[81] Siguiendo a CUERDA ARNAU. "Proporcionalidad penal y libertad de expresión: la función dogmática del efecto de desaliento", *Revista General de Derecho penal*, nº 8, 2007.

conectados con la expresión de opiniones en que consiste, en última instancia, el delito de enaltecimiento del terrorismo y humillación a las víctimas.

De acuerdo con lo expuesto, esta extensión permite incluir dentro del tipo del art. 578 CP la mera adhesión política o ideológica a los objetivos perseguidos por la actividad terrorista[82]. Los límites a la libertad de expresión que impone la interpretación extensiva del delito de enaltecimiento pueden ser analizados desde la desproporción y la indeterminación del precepto, circunstancias que pueden favorecer este efecto de desaliento, a sabiendas de la posible sanción que podría acarrear una expresión de opiniones que pudiera ser interpretada como una justificación de actos terroristas. De acuerdo con lo expuesto, puede recordarse la integración realizada por la STC 136/1999, de 20 de julio[83], respecto del efecto de desaliento como parte del juicio de proporcionalidad en sentido amplio, cuestión que como indica CUERDA ARNAU "no persigue privar a las normas penales de su eficacia intimidatoria. Lo que prohíbe es que dicha eficacia intimidatoria se extienda a conductas que son limítrofes con el legítimo ejercicio de la libertad de expresión o que sancione éstas con desproporción manifiesta"[84]. En este sentido la *vis expansiva* representada por el delito de enaltecimiento y humillación a las víctimas supone una colisión con la protección de la libertad de expresión reconocida en el art. 20 CE, tanto por la desproporción en la tipificación de las conductas, como por la coacción a la libre expresión de opiniones que representa el propio precepto desde

[82] Críticamente, PÉREZ CEPEDA, "la finalidad del terrorismo siempre es política y no se castiga solo como terrorista a quien realiza delitos graves indiscriminados contra las personas con fines políticos, sino que como parte de su estrategia de 'lucha' también se persigue la ideología o el pensamiento que lo sustenta cuando utiliza o, simplemente, justifica el medio de la violencia". Cfr. "La criminalización del radicalismo y extremismo en la legislación antiterrorista", en *Terrorismo y contraterrorismo en el Siglo XXI. Un análisis penal y político criminal*, ob. cit., p. 18.

[83] STC 136/1999, de 20 de julio, FFJJ 20º y 29º: "Precisamente por ello, una reacción penal excesiva frente a este ejercicio ilícito de esas actividades puede producir efectos disuasorios o de desaliento sobre el ejercicio legítimo de los referidos derechos, ya que sus titulares, sobre todo si los límites penales están imprecisamente establecidos, pueden no ejercerlos libremente ante el temor de que cualquier extralimitación sea severamente sancionada" (…) "es indudable que las conductas incriminadas son actividades de expresión de ideas e informaciones y constituyen una forma de participación política y, en consecuencia, una sanción penal desproporcionada puede producir efectos de desaliento respecto del ejercicio lícito de esos derechos".

[84] Cfr. "Proporcionalidad penal y libertad de expresión: la función dogmática del efecto de desaliento", ob. cit., p. 22.

la perspectiva del efecto de desaliento, integrado como se ha dicho en la estructura argumental del principio de proporcionalidad[85].

Sobre esta cuestión, la interpretación realizada por los órganos jurisdiccionales parece seguir una línea político-criminal dirigida, más que al tratamiento preventivo-penal de la actividad terrorista, a la criminalización de determinadas opciones políticas o ideológicas que nada tienen que ver de forma directa con la actividad terrorista[86]. En este sentido, la expresión de este tipo de comentarios en las redes sociales, o bien representan muestras de humor macabro descontextualizado, desafortunado y sin duda del todo rechazable -pero que en nada justifica el recurso al Derecho penal-, o bien constituyen una posición de disenso respecto del pensamiento político dominante. Por esta razón, los límites a la libertad de expresión que supone la aplicación extensiva en las redes sociales del delito de enaltecimiento del terrorismo no puede justificarse por el indudable mal gusto de ciertos comentarios proferidos en este ámbito, ni tampoco por la repulsa que pueda causar en las víctimas –entendidas como colectivo–, en la medida en que supone una limitación a los derechos y libertades inasumible por un Estado democrático de Derecho.

Así las cosas, puede apreciarse de qué manera el *panóptico digital* como paradigma de control social propio del *Big data* y, en un contexto donde se expande el recurso al Derecho penal, comporta un castigo del disenso en forma de recorte fáctico de libertades públicas[87]. A este respecto, pueden destacarse las siguientes palabras de HAN descriptivas de los riesgos que supone esta expansión del *panóptico digital* al ámbito del poder punitivo del Estado: "Google y las redes sociales, que se presentan como espacios de la libertad, adoptan formas panópticas. Hoy contra lo que supone normalmente, la vigilancia no se realiza como ataque a la libertad. Más bien cada uno se entrega *voluntariamente* a la mirada panóptica. A sabiendas,

[85] Cfr. CORRECHER MIRA. "El delito de enaltecimiento del terrorismo y humillación a las víctimas tras la reforma de la LO 2/2015 en materia de delitos de terrorismo", ob. cit., p. 8.

[86] Como pueda apreciarse en la Sentencia del Tribunal Supremo 4/2017, de 18 de enero, donde se condenó a Cesar Montaña, cantante del grupo de rap Def Con Dos por un delito de enaltecimiento del terrorismo, o la Sentencia de la Audiencia Nacional 34/2017 de 4 de diciembre, donde se condena al colectivo de rap conocido como *La Insurgencia*.

[87] Cfr. HIJMANS. *The European Union as Guardian of Internet Privacy Law*, Springer International Publishing, Switzerland, 2016, p. 103.

contribuimos al panóptico digital, en la medida en que nos desnudamos y exponemos. El morador del panóptico digital es víctima y actor a la vez. Ahí está la dialéctica de la libertad, que se hace patente como control"[88].

3. La privacidad como negocio: la mercantilización de la protección de datos en el *Big data*

3.1 Lógica economicista del estándar actual de privacidad: los datos personales, el nuevo petróleo

No es inapropiado afirmar que en la actualidad pueda hablarse de una expropiación de la privacidad sin precedentes. Los datos personales se han convertido en un activo patrimonial de gran valor económico en el Mercado, el petróleo del siglo presente, ellos orientan el desarrollo y uso de nuevos productos y servicios[89]. La obtención de información personal cuenta con dos grandes aliados, de una parte las nuevas herramientas tecnológicas y, de otra, la fragmentación legislativa o incluso la desregulación, lo que da rienda suelta al mercadeo de datos personales sin demasiados problemas.

Estos dos factores han convertido a la privacidad en el producto estrella a comercializar por las grandes corporaciones del *Big data*. El negocio resulta más que rentable: los usuarios ceden gratuitamente sus datos personales (a cambio de la instalación de una App, mediante la suscripción a un boletín de ofertas de un grupo empresarial, permitiendo la geolocalización del Smartphone, revelando todo tipo de información personal en una red social…) a empresas que se dedican a almacenarlos, venderlos a terceros o procesarlos para un tratamiento posterior, generalmente con objetivos de marketing.

No puede ignorarse que el uso o la instalación de la mayoría de servicios y aplicaciones informáticas aparentemente gratuitas suponen auténticos contratos de adhesión (sobre los

[88] Cfr. *La sociedad de la transparencia*, ob. cit., p. 95.

[89] De acuerdo con MORENO MUÑOZ: "los datos son hoy el propulsor de crecimiento y transformación, como lo fue el petróleo en su momento. Y los flujos de datos configuran hoy nuevas infraestructuras, nuevos modelos de negocio y nuevas economías, con nuevos actores en posición de monopolio y políticas estatales diferenciadas según las ventajas de partida para beneficiarse de las reglas de mercado". Cfr. MORENO MUÑOZ, M. "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", ob. cit., p. 9.

cuales sus consumidores no tienen capacidad alguna de negociación) que contienen, en su mayoría, un alto número de cláusulas abusivas, dónde los usuarios ceden sus datos personales – en ocasiones sin autorización expresa o incluso sin su conocimiento[90]– en contraprestación por los servicios recibidos, que más tarde se monetizan por dichas empresas dedicadas, en el fondo, al almacenaje, tratamiento, exportación y venta de datos personales. Más flagrante es, sin embargo, el cambio unilateral de las políticas de privacidad (bajo el eufemismo "condiciones o términos de uso") de aplicaciones o programas ya instalados en los dispositivos tecnológicos, y que buscan obtener un mayor número de datos personales, con la consigueinte disminución de la privacidad de los usuarios[91].

También queda patente como las corporaciones de Internet y los operadores de telecomunicaciones han adquirido sobre los usuarios una capacidad de condicionamiento (e, indirectamente, control) sin precedentes. Acceden y patrimonializan nuestra privacidad por medio de la entrega de servicios aparentemente gratuitos que conllevan unilateralmente cláusulas abusivas respecto de los datos personales de los 'beneficiarios', sometidos desde ese momento a una constante vigilancia.

Así, los usuarios de estos servicios ya no somos meros consumidores pasivos sino que, a través de una pérdida considerable de nuestra privacidad, nos hemos convertido en parte del producto cuya ganancia, sin embargo, no percibimos. Sin ser del todo conscientes hemos evolucionado del Internet de las cosas[92] al Internet de las corporaciones, donde las cosas somos

[90] Mientras que la legislación tradicional sobre protección de datos está principalmente basada en aquellos datos qué los usuarios comparten o ceden de manera voluntaria, lo cierto es que en la práctica, éstos son los menos en comparación con el gran volumen de datos y metadatos que se extraen diariamente sin que los usuarios tengan conocimiento y, claro está, dichas acciones no cuentan con su consentimiento.

[91] Esto es lo que sucedió en 2016 con *WhatsApp*, cuando actualizó sus "términos de servicio" y su "política de privacidad" de manera unilateral para conseguir compartir con *Facebook* (que en 2014 compró la empresa de mensajería) y todo su grupo empresarial, los datos de los usuarios de la primera (más de un billón en dicho momento). Esta transfusión masiva de datos revelaba una estrategia puramente comercial que, en principio, parecía explicarse por motivos de publicidad -la llamada "mensajería comercial"- pues las nuevas cláusulas contractuales de *WhatsApp* permiten extraer infinidad de metadatos capaces de establecer patrones de comportamiento prácticamente unívocos -teniendo en cuenta que hoy en día llevamos el móvil prácticamente a todos lados-, cómo cuándo y a qué red WiFi se conecta el usuario o cuales son los comercios en los que suele comprar.

[92] Término acuñado por ASHTON. "That 'Internet of Things' Thing", *RFID Journal*, 2009. Se aplica esta denominación a un sistema ciberfísico donde los objetos pueden conectarse a Internet a través de sensores ubicuos, dotándoles de funcionalidades decisivas en términos de disponibilidad, acceso, eficiencia en la distribución y contextualización. Se origina

nosotros y en el que los datos personales son el nuevo producto a comercializar[93]. Como apunta HAN, "el *Big Data* no solo aparece en la forma de *Big Brother*, sino también de *Big Deal*. El *Big Data* es un gran negocio. Los datos personales se capitalizan y comercializan por completo. Hoy se trata a los hombres y se comercia con ellos como paquetes de datos susceptibles de ser explotados económicamente"[94].

La universalización del Mercado ha optado por configurar modelos sociales, económicos y jurídicos únicos que faciliten las relaciones sociales y el libre comercio y las hagan más eficientes, colocando en una posición privilegiada a los regímenes privados frente a los públicos ya que, mientras que los primeros pueden dedicarse a buscar su beneficio propio, el Estado tiene la obligación de velar por los intereses de los ciudadanos, desde una posición teóricamente punto altruista. Este fenómeno se extiende también al ámbito económico y al Derecho[95].

Analizando lo ocurrido con la mercantilización de la privacidad, desde un punto de vista económico habría que considerar las normas jurídicas como precios, los precios como costes de oportunidad y el sistema jurídico como parte del Mercado[96]. Desde tal interpretación, las normas jurídicas se verían instrumentalizadas para incentivar o desincentivar a sus destinatarios por lo que cabría asignarles un precio en la ecuación.

Así, siguiendo esta analogía, podemos decir que las normas jurídicas en materia de privacidad se han convertido -quizás sin pretenderlo- en costes de oportunidad positivos en el sentido de que han conseguido incentivar la comercialización de la privacidad con la

---

ligado al estándar de identificación automática para sensores de identificación por radio-frecuencia. Este sistema permite el almacenamiento y recuperación de datos remotos a través de dispositivos denominados etiquetas (pegatinas, tarjetas, transponedores…). Cfr. MORENO MUÑOZ. "Privacidad y procesado automático de datos personales mediante aplicaciones y bots", ob. cit., p. 7.

[93] Cfr. DEL FRESNO GARCÍA. "Internet como macromedio: la cohabitación entre los medios sociales y los medios profesionales", *Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad*, nº 99, 2014, pp. 107-110.

[94] Cfr. *Psicopolítica*, ob. cit., p. 98.

[95] Cfr. MERCADO PACHECO. *El análisis económico del derecho: una reconstrucción teórica*, Centro de Estudios Constitucionales, Madrid, 1994, pp. 127 ss.

[96] Cfr. BERMEO ÁLVAREZ. "Las normas jurídicas: una aproximación desde el convencionalismo jurídico y el análisis económico del derecho", *Inciso*, Vol. 18, nº1, 2016, p. 104.

desregulación del Mercado. Ni Internet ni la tecnología son neutrales, son una creación humana y, por lo tanto, responden a la ideología de sus creadores o de los agentes intervinientes que, hasta la fecha, han apostado claramente por almacenar la mayor cantidad posible de datos del mismo modo que han tomado la decisión consciente de vender esa información a terceros, en beneficio propio y en el marco de una decisión empresarial[97]. Estas empresas han adoptado un modelo de negocio en torno a la capitalización de la información personal de sus usuarios en vez de a su protección[98], y lo han hecho en connivencia con los Estados que han resultado cómplices de su actuación.

Si bien es cierto que, al menos en territorio europeo, están explícitamente reconocidos una serie de derechos en torno a la privacidad, en la práctica se ha producido un éxodo masivo de las principales empresas de Internet hacia territorio estadounidense, mucho menos garantista en la materia, tratando de extender el modelo norteamericano más allá de sus fronteras. Estandarizar el derecho, recordemos, cumple con los fines de la globalización. En este sentido, puede compartirse la expresión utilizada por CAPELLA, *"soberano privado interestatal difuso"*, para referirnos a las dudas que desde el principio de soberanía supone la existencia de poderes privados que de forma encubierta, pero en connivencia con las instituciones, inciden en las dinámicas públicas mediante la imposición de sus intereses económicos[99]. Partiendo de esta concepción del proceso de la globalización, en su lógica resulta evidente que no desea verse secundada voluntariamente por una universalización de los derechos, puesto que éstos también están sometidos a los imperativos de la economía, del libre mercado y de la competencia mundial, elementos que, al mismo tiempo, han producido una disminución considerable de la

[97] Cfr. DOMENECH PASCUAL. "Por qué y cómo hacer análisis económico del Derecho", *Revista de administración pública*, nº 195, 2014, pp. 99-133

[98] No obstante, es cuestionable la eficiencia de este régimen que impone a los usuarios la carga de proteger su privacidad ya que, en Internet, la información sobre un individuo nunca es absolutamente cierta o completa y al no tener el usuario control sobre ésta, no hay manera de corregir hechos erróneos que pueden determinar la decisión de la contraparte, lo que puede llevar a una conducta económicamente ineficiente. También ello aleja a potenciales clientes que, por temor a la exposición ilimitada y a la publicidad no deseada, dejan de participar en ciertos comportamientos online.

[99] El significado de la noción desarrollada por CAPELLA se encuentra ligado al reconocimiento de entes de naturaleza privada que con sus actuaciones producen efectos en la esfera pública. Cfr. "Estado y Derecho ante la mundialización: aspectos y problemáticas generales", en *Transformaciones del Derecho en la mundialización*, Consejo General del Poder Judicial, Madrid, 1999, pp. 107-109.

soberanía de los propios Estados, que resultan permeables a su interacción. Ello tiene una mayor visibilidad en el entorno de Internet, dominado principalmente por la autorregulación y la iniciativa privada y poco acostumbrado a la intervención de los Estados.

Así por ejemplo, las páginas web contienen un sinfín de datos personales cuyo acceso está abierto a los motores de búsqueda, y con ello el peligro de vulneración del ámbito sensible, la privacidad, de sus titulares, en clara repercusión –negativa– sobre sus derechos fundamentales. En la práctica, aprovechándose de la tentación o dependencia digital de las personas, empresas como *Google* o *Facebook* están llevando a cabo un tratamiento masivo de datos personales. Los usuarios firman un cheque en blanco sobre sus datos al aceptar los términos y condiciones de uso que ellas imponen siendo que, una vez dado su consentimiento a la política de privacidad que se ofrece en un paquete compacto e indesligable, resulta verdaderamente difícil seguirles la pista[100]. Esta situación escapa al control del usuario y es más que evidente la inseguridad jurídica que le acarrea como ciudadano, sujeto de irrenunciables derechos fundamentales. ¿Cómo puede solicitar la cancelación de una información sensible, puede que la más privada, si no tiene a quién dirigirse ni siquiera conoce a ciencia cierta qué saben de su vida? Pese a tener reconocidos explícitamente en nuestro ordenamiento derechos fundamentales como la intimidad o la protección de datos, éstos se convierten *de facto* en papel mojado.

Parece ser que tanto usuarios -obligados a pleitear en jurisdicción estadounidense- como gobiernos -que ven como las grandes corporaciones esquivan el cumplimiento de su ordenamiento jurídico- están tomando consciencia de los peligros de comercializar con la información más personal, escenario que ha dado lugar a la creación de un nuevo Reglamento Europeo de Protección de Datos. Esta nueva normativa, que pretende consolidar los estándares de protección a todo el territorio europeo, da un giro en la trayectoria reciente al intentar erradicar estos comportamientos empresariales, convirtiéndose en costes de oportunidad

[100] Sobre esta cuestión, ALBERTO GONZÁLAEZ plantea sus dudas sobre la legitimidad de la reutilización de los datos previamente cedidos para la realización de una compra o transacción, en tanto que la finalidad de elaborar perfiles de consumo para luego ser ofertados a terceros resulta ajena a la relación contractual inicial. En este sentido, considera que "esto constituye una desviación de la finalidad, para cual se necesitaría una nueva legitimación en base al consentimiento". Cfr. "Responsabilidad proactiva en el tratamiento de datos masivos", ob. cit., p. 121.

negativos al prever sanciones para supuestos de incumplimiento. Y es que sería deseable que un sistema jurídico pudiera proteger bienes con independencia de su transcendencia económica, pues es indudable que ciertos valores o principios en nuestra sociedad resultan jurídicamente relevantes y son susceptibles de tutela legal con independencia de su provecho económico. La privacidad pues, debe empezar a percibirse de este modo y pasar a protegerse legislativa y jurisdiccionalmente de una forma real, sin pensar en otros factores economicistas.

No obstante, mucho tendrá que cambiar el *modus operandi* de dichas empresas que solicitan la aceptación de unos términos y condiciones infinitos e indescifrables para contratar la mayoría de los servicios y que no informan con claridad sobre cual es el destino de nuestros datos personales ni de si éstos cambian de manos. La transparencia debe aumentar necesariamente para hacer efectivos nuestros derechos, pero, así y todo, va a ser muy difícil controlar, por ejemplo, la actividad de los *Data Brokers* que trabajan prácticamente en la clandestinidad. Además, acuerdos como el *Privacy Shield*, que permite las transferencias transatlánticas de datos personales por "motivos comerciales" eludiendo el tenor literal de la normativa europea, evidencian la visión contrapuesta acerca de la privacidad en los sistemas jurídicos respectivos y no contribuyen a disipar el escepticismo.

3.2 Los *Data Brokers*: mercaderes de la privacidad

El *Big data* de una empresa puede llegar a ser su activo más valioso y juega un papel muy importante en la toma de decisiones de mercado pero ¿Quién compra nuestros datos? Los *Data Brokers* son empresas que se encargan directamente de hacer negocio con nuestra privacidad, son vendedores de información que se dedican a recolectar datos de los consumidores (la mayoría de veces sin su consentimiento) y vendérselos a un tercero. Pese a que este mercadeo es opaco y actúan encubiertos en el anonimato, se calcula que estas empresas no llegan ni a la decena pero, sin embargo, controlan todo el tráfico de Internet[101].

[101] Un informe de 2013 de la Comisión Federal de Comercio del Senado de los Estados Unidos (*Federal Trade Comission*) identificó a nueve empresas como *Data Brokers*, a las que sacó del anonimato para alertar del peligro que supone esta mercadotecnia. El informe disponible, en inglés: https://www.commerce.senate.gov/public/_cache/files/0d2b3642-6221-4888a63108f2f255 b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.

Estos datos se filtran, analizándolos y cruzándolos, hasta crear catálogos con perfiles o patrones de comportamiento y posteriormente se venden a otras empresas que los usarán, por ejemplo, para verificar identidades, detectar fraudes, pero, sobre todo, para fines publicitarios. Como señalan MAYER-SCHÖNBERGER y CUKIER, "dos fondos de inversión, Derwent Capital de Londres y MarketPsych de California empezaron a analizar el texto datificado de los tuits como indicios para la inversión en el mercado de valores (sus estrategias comerciales reales fueron mantenidas en secreto; en lugar de invertir en firmas a las que se daba mucha publicidad, puede que apostaran en su contra). Ambos fondos venden ahora la información a sus propios inversores"[102]. Como puede inferirse de este supuesto, la *datificación* como práctica de explotación de datos masivos no se limita al aislamiento de patrones sobre las actitudes o estados de ánimo, sino que abarca de forma amplia el comportamiento humano[103]. De este modo, los *data brokers* pueden terminar facilitando a los terceros interesados, una muestra del comportamiento humano en un contexto concreto del medio social, obteniendo como se ha expuesto un valor económico por ello.

¿Cómo llevan a cabo su actividad? Recogen información tanto de fuentes públicas (Hacienda, Registro Mercantil, DGT…) como privadas (*cookies*, redes sociales, tarjetas de fidelización, tarjetas de compras…) y gracias a ellas obtienen datos no sólo acerca de cómo nos llamamos o dónde vivimos, sino que son perfectamente capaces de averiguar qué compañía aérea preferimos para viajar, el tipo de cine que solemos ver, la asiduidad con la que visitamos determinados videos de *YouTube*, el presupuesto de nuestras futuras vacaciones, las enfermedades que hemos padecido, si estamos pensando en cambiar de coche…

El marketing personalizado no es nada nuevo, pero la tecnología ha abierto nuevas vías de explotación y los *Data Brokers* están haciendo negocio con ello. Sus últimas prácticas consisten en la instalación de sensores en lugares estratégicos, como por ejemplo centros comerciales, capaces de monitorizar la señal WiFi de nuestros Smartphones, de este modo saben en qué tiendas compramos, en qué escaparates sólo nos fijamos, cuánto tiempo

[102] Cfr. *Big data*. *La revolución de los datos masivos*, ob. cit., p. 117.

[103] *Ibid*., p. 119.

dedicamos a ello[104]… y así retratan nuestros hábitos de consumo. No cabe duda de la revolución que para la mercadotecnia esto supone y de cómo esta información es de gran valor para muchas empresas[105].

3.3 Los ciudadanos como contribuyentes en la hacienda privada de los datos personales

Si bien es cierto que parte de la información personal que se encuentra en bases de datos no cuenta con nuestro consentimiento o nuestro conocimiento, hay mucha otra información que es revelada conscientemente por los directamente "afectados" mediante tarjetas de fidelización, suscripciones gratuitas, obtención de cupones de descuento…

Como si de vender el alma al diablo se tratara, cedemos nuestra biografía digital a cambio de servicios gratuitos, desde el historial de búsqueda hasta nuestras preferencias políticas, pasando por nuestra localización. Cada vez que *Google Now* nos indica el tiempo que nos queda para llegar a casa, lo hace porque sabe dónde vivimos, dónde está nuestro trabajo, cuales son nuestros horarios e incluso a qué velocidad media solemos desplazarnos. Esta es otra de las características de la "modernidad líquida" que viene a orientar los presupuestos estructurales de este trabajo. De acuerdo con BAUMAN, "para el individuo, el espacio público no es mucho más que una pantalla gigante sobre la que son proyectadas las preocupaciones privadas sin dejar de ser privadas ni adquirir nuevos valores colectivos durante el curso de su proyección: el espacio público es donde se realiza la confesión pública de los secretos e intimidades privados"[106]. Siguiendo esta tesis, la exposición a la que se somete la ciudadanía en el marco de la revolución digital, sin entrar en si ésta es realizada de forma plenamente libre o por pulsiones determinadas por el medio social, es una muestra de cómo la "modernidad

[104] Esta práctica recibe el nombre de *wifi tracking* o medición de audiencias en tiendas físicas. Apple tiene implantadas este tipo de balizas llamadas *iBeacon* en muchas de sus tiendas físicas desde el año 2014, mediante unos transmisores de bajo consumo, se envían señales a los dispositivos móviles más cercanos que tengan activado el WiFi, pese a no estar conectados a ninguna red, midiendo la actividad y el movimiento de cada cliente por la tienda.

[105] En algunos casos incluso, mediante este uso de la información personal, se producen prácticas comerciales desleales ya que, empleando de forma sesgada la información personal de usuarios, se elaboran campañas de marketing dirigidas a explotar psicológicamente el consumidor con la intención de influir en su capacidad de decisión y en su comportamiento económico, tratando de imponerle preferencias respecto de la contratación de determinados bienes o servicios

[106] Cfr. *Modernidad líquida*, ob. cit., p. 45.

líquida" supone un contexto propicio para la confusión entre los ámbitos público y privado, con el consiguiente riesgo a la desprotección de los datos personales que esto supone.

Algunas veces por pura pereza, no cambiamos la configuración de fábrica de nuestros dispositivos, no leemos las condiciones generales de contratación o no desmarcamos las casillas que permiten usar nuestros datos para "recibir ofertas o descuentos", otras veces sí que se nos exige una conducta más proactiva al requerirnos enviar cartas (¡en pleno 2018!) a un apartado de correos para manifestar nuestra oposición al tratamiento de datos que se aplica por defecto. Por no hablar de la información que puede extraerse de las redes sociales, con un breve vistazo al perfil de usuario podemos saber la ciudad en la que vive una persona, dónde y con quién estudió, cual es su situación sentimental, sus gustos musicales, sus tendencias políticas, sus preferencias de ocio y consumo…

Todo esto se debe al desconocimiento o quizás indiferencia del usuario de lo que se hace con toda esta información. La masificación de las redes sociales ha supuesto una nueva era de sobreexposición que los expertos han convenido en llamar "extimidad", como concepto clarificador de este cambio de paradigma en la privacidad[107]. Lo curioso es que esta "extimidad" está suponiendo la vulneración de nuestros derechos, muchas veces por la renuncia del propio titular. Renunciamos a nuestra privacidad para tener una cuenta en *Facebook*, para que *Google Maps* nos diga qué camino es el más rápido para llegar a casa, para que la compañía hotelera nos aplique un 10% de descuento sobre el precio… y así nos damos cuenta de que en el mundo online no tenemos intimidad ninguna.

La información que se revela en muchos casos puede parecer inofensiva, pero no es disparatado pensar que en algún momento pueda resultar perjudicial para la persona en

[107] El término "extimidad", pese a ser originariamente acuñado por el psicoanalista francés Jacques Lacan en 1958 con diferentes propósitos, se emplea hoy en día para referirse a la tendencia de los individuos a hacer pública su intimidad y vida privada. Al hacer gala de esta extimidad, los sujetos desvirtúan su propia esfera privada y, de manera intencional, arrojan su intimidad y vida privada a la arena pública. Mediante la exposición voluntaria a través de las tecnologías digitales, los sujetos pervierten la naturaleza propia de la esfera privada, valorando su publicidad por encima de su salvaguarda. NOAIN SÁNCHEZ. *La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)*, Boletín Oficial del Estado, Madrid, 2016, pp. 194-195.

concreto, aunque sea en términos de reputación online que se añade hoy a nuestra biografía[108]. En Internet, el tiempo siempre es lineal: el pasado sigue estando presente y será siempre accesible en el futuro.

Es perfectamente posible defender que el avance imparable –y la mayoría de veces positivo, no puede negarse– de las nuevas tecnologías no tiene porqué ser inversamente proporcional a la vulneración del derecho a la privacidad de sus usuarios, y desde luego no es excusa suficiente para quebrantar derechos fundamentales.

3.4 Valor monetario de los datos personales

Las nuevas formas de explotación económica que permite el mercado digital, como la propia vida moderna, están llenas de contradicciones. Si como se ha visto, a medida en que aumenta la demanda de los servicios gratuitos que necesitan de nuestros datos personales para su funcionamiento incrementa también la preocupación por la privacidad, otra paradoja se produce en torno a este fenómeno. Y es que, mientras empresas como *Facebook* o *Google* ganan millones de dólares a partir de los ingresos que obtienen de los anunciantes a los que venden nuestros datos personales, la estimación del valor que se deriva de éstos en relación a cada uno de los usuarios es más bien baja. Se calcula que los usuarios estiman su información personal online entre los 2.000€ y los 3.000€, un valor desorbitado si tenemos en cuenta el precio que un anunciante pagaría por usarla: unos céntimos de euro[109].

Todos los datos personales tampoco son igual de valiosos, el mercado digital no cotiza del mismo modo nuestra localización que nuestro nivel de estudios. De entre toda esta

[108] Como muestra el caso de la tuitera Cassandra Vera, una joven de 21 años que hace más de cinco años hizo comentarios irónicos y humorísticos en su perfil Twitter acerca de Carrero Blanco (Sentencia nº 9/17 de 29 de marzo, de la Audiencia Nacional. MP: Juan Francisco Martel Rivero). Sin entrar a comentar la desproporción de dicha resolución, es innegable que la reputación online se añade hoy a nuestra biografía y que, por tanto, estamos más expuestos públicamente. En este caso en concreto, Cassandra ha sido condenada a un año de prisión y a siete de inhabilitación absoluta lo que, en su caso, le ha comportado graves perjuicios económicos y profesionales. Pese a que el posterior recurso de casación supuso la absolución de Vera por el Tribunal Supremo (STS 493/2018, de 26 de febrero de 2018), no podrá negarse que el daño en su biografía digital será difícilmente reparable con las herramientas jurídicas actuales.

[109] En la página web, http://www.totallymoney.com/personal-data/, mediante la realización de un test, se puede comprobar la diferencia entre el valor que cada uno le otorgamos a nuestra información personal más básica y el valor real por el que una empresa anunciadora pagaría por ella.

información, la que tiene un valor económico superior es la relativa a la salud cuyos datos, especialmente sensibles por razones obvias, cotizan al alza en el mercado negro[110].

Es muy difícil calcular el valor de nuestra información personal, en primer lugar, por la falta de datos al respecto, pues es un mercado opaco lleno de secretismo y dónde las fluctuaciones económicas del producto escapan a nuestro entender. No obstante, se han llevado a cabo diversas estimaciones, como la que realizó el *Financial Times*[111], creando una calculadora digital para poner valor a nuestra información personal mediante la realización de un test. Según los resultados, la información básica como la edad, el sexo y la ubicación tendrían un valor de 0,0005$ mientras que si se añade más información como la marca de coche utilizando, el lugar de vacaciones o información financiera, esta cifra aumentaría exponencialmente.

No obstante, el hecho que los datos personales singularmente considerados tengan un valor relativamente bajo, no implica que su explotación global por parte de empresas como *Google* o *Facebook* no les esté reportando cuantiosos beneficios económicos. Debe tenerse en cuenta que el valor de la información personal varía en función del volumen de datos que se comercialice, cuanta más información y cuantas más variables al respecto, más alto es el precio y mayores son los ingresos[112].

Los datos de cada persona no son en sí los más relevantes, lo más valioso es obtener información sobre la totalidad de nuestra actividad online que permita rastrear nuestras

[110] Los ciberdelincuentes se están especializando cada vez más en el robo de datos de hospitales, farmacéuticas y asegurados de salud, de hecho, el sector sanitario ha sido el más afectado por ataques informáticos destinados al robo de información sensible. Como ejemplo, el pasado febrero se produjo un ciberataque al Hollywood Presbyterian Medical Center de los Ángeles robando los historiales médicos de sus pacientes así como los correos electrónicos de sus trabajadores, por el que se solicitó un rescate de 3,7 millones de euros. Lo mismo ocurrió ese mismo mes en dos hospitales alemanes, el Lukas Hospital y el Klinikum Arnsberg Hospital, ambos sufrieron el ataque de un virus informático en su sistema que bloqueó los archivos exigiendo dinero para liberar los datos previamente cifrados. Fuentes de las noticias disponibles, respectivamente, en https://www.theguardian.com/technology/2016/feb/17/los-angeles-hospital-hacked-ransom-bitcoin-hollywood-presbyterian-medical-center y http://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030 .

[111] Herramienta disponible en: https://ig.ft.com/how-much-is-your-personal-data-worth/?ft_site=falcon#axzz4g6IgV7zg

[112] Investigadores de la Universidad de Carlos III de Madrid han desarrollado "FDVT: Facebook Data Valuation Tool", una herramienta para saber cuánto dinero gana *Facebook* con los datos personales de sus usuarios. Así, mientras se está utilizando *Facebook*, aparece una ventana en la que se detallan los ingresos que genera el usuario a dicha red social mientras se navega por ella, en tiempo real y en relación al valor económico de la publicidad. Éstos van aumentando a medida en que la interacción en la navegación es mayor, cuantos más Me Gusta o más reacciones se produzcan por el usuario en cuestión.

reacciones, pautas y preferencias y catalogar de este modo nuestro patrón de comportamiento en base a una visión comercial[113]. Así, los datos individualmente considerados van cobrando relevancia en la medida en que se cruzan con otros datos y permiten una reconstrucción de la personalidad online capaz de predecir nuestros pasos o intereses en la vida real.

Un aspecto a tener en cuenta es que no todos los bancos de datos tienen un destino comercial, la información personal se vende como cualquier otra mercancía, a quien tenga interés y dinero para comprarla con independencia de la finalidad que vaya a darle, precisamente este es el riesgo más inquietante de especular con la privacidad. Así, por ejemplo, en el mercado de los seguros, hoy en día un historial clínico tiene más valor que una tarjeta de crédito.

Recientemente la prensa se hacía eco de *Exact Data*, una empresa *Data Broker*, que cuenta con un banco de datos de más de 200 millones de contactos de Estados Unidos y que se pueden filtrar entre más de 450 categorías, entre ellas algunas tan sensibles como religión y etnia, además de contar con otras categorías preconfiguradas como "estadounidenses hispanos no asimilados". Es más, dicha empresa publicita la oferta de los datos de 1,8 millones de musulmanes por 126.851€, a razón de 7 céntimos de euro por persona.

Esta posibilidad, ilegal en países como el nuestro pero cuyo reproche de moralidad va más allá de nuestras fronteras, pone en peligro derechos fundamentales de los más básicos como la intimidad o la prohibición de discriminación, cosa que ya han puesto de relieve algunas organizaciones en defensa de los derechos humanos[114]. Si comercializar con estos datos para meros propósitos de marketing ya suscita dudas más que razonables, éstas aumentan

[113] AGUILAR, define este fenómeno como "la invivible transparencia", en la que las personas son expuestas tras las vitrinas de las redes sociales como un objeto de museo y junto a una leyenda explicativa que le añade significados. De la mayor o menor acumulación de significados, depende que cada personalidad virtual sea más o menos susceptible de convertirse en un potencial cliente de las empresas que se enuncian en dicha plataforma. De igual modo, cuanto mayor sea la interacción que alimenten o produzcan dichos sujetos, mayor será el valor que le darán a la compañía. Sin embargo, esta transparencia no se predica desde la óptica de los usuarios que, en términos generales, no son conscientes del destino de sus datos personales recolectados ni siquiera de las condiciones en que éstos se recolectan. Cfr. AGUILAR. "La opacidad necesaria" en *La transparencia engaña*, (Albergamo ed.), Biblioteca Nueva, Madrid, 2014, p. 85.

[114] http://tecnologia.elpais.com/tecnologia/2017/05/03/actualidad/1493835469_309268.html.

conforme imaginamos los numerosos usos que pueden darse a los mismos en manos malintencionadas, con propósitos claramente discriminatorios y vulneradores de derechos.

3.5 Un ejemplo de modelo empresarial: Facebook en cifras

Facebook, se configura como un servicio sin coste económico para los usuarios de su red social, sin embargo, ni ésta ni las otras grandes compañías que operan en el ámbito de Internet son ajenas a la lógica del Mercado, no actúan por motivos filantrópicos ni para acercar la tecnología a los ciudadanos sin pretender obtener nada a cambio. *Facebook* es una empresa que cotiza en bolsa, que pone a disposición de sus usuarios una serie de infraestructuras cuyo mantenimiento le comporta ciertos costes y, en consecuencia, tiene como finalidad obtener beneficios económicos.

¿Y cómo lo logra? Sus ingresos los aporta la publicidad pero su activo empresarial lo forman la gran cantidad de datos y metadatos –datos sobre los datos- que almacena en sus servidores y que los usuarios de *Facebook* ceden gratuitamente y en propiedad[115]. El negocio es redondo, sus usuarios donan gratuitamente información de carácter personal (nombre, sexo, localización, dirección de correo electrónico, estado civil, nivel de estudios, hábitos de consumo, preferencias de todo tipo…) que se filtra y clasifica por grupos y se ofrece a anunciantes que la emplearán para el marketing personalizado (el llamado *targeting*[116]).

[115] *Facebook* es, de facto, una plataforma dedicada a la creación de perfiles mediante las acciones de sus usuarios, sus deseos, sus preferencias, sus Me Gusta, sus no acciones… transformando toda esta información en datos: en ceros y unos que a menudo reconfiguran nuestra identidad digital. Aunque no se conocen los algoritmos que usa *Facebook* para ello, se han creado herramientas como "What Facebook Thinks You Like" que permiten hacerse una idea de cómo funciona el sistema y como avanza éste según vamos navegando en la web.

[116] La publicidad personalizada no es una nueva técnica comercial así como tampoco lo es que los gobiernos espíen a sus ciudadanos, pero el entorno digital contemporáneo amplia dichas posibilidades hasta el infinito, lo que en muchos casos roza la distopía Orwelliana. Este es el caso de las últimas filtraciones llevadas a cabo por WikiLeaks, llamadas "Year Zero" y que ponen de manifiesto las técnicas utilizadas por la CIA para el ciberespionaje entre 2013 y 2016. Según parece no sólo utilizaban las vulnerabilidades técnicas de ciertos aparatos electrónicos estadounidenses y europeos sino que infectaban dispositivos de última generación para acceder a información personal. Así, por ejemplo, mediante *malware* se conseguía acceder a los Smartphones y, entre otros fines, georastrear al usuario o, mediante las Smart TV, grabar el sonido ambiente, convirtiéndolas en micrófonos y hasta en algunos casos cámaras, encubiertas.

Facebook, en la práctica se ha convertido en un software masivo de datos cuyo destino, por el momento, se limita a fines publicitarios[117].

Mediante este proceder se van configurando perfiles y etiquetas[118] para las personas, que pueden usarse para recibir ofertas de productos y servicios que sean de su interés pero que también puede convertirse en la razón por la que no les concedan un préstamo o un trabajo. Habría que reflexionar también sobre la selección de los hechos relevantes para tal categorización, lo que inevitablemente refleja cierta ideología, así como sesgos y prejuicios.

Facebook es el gigante de la publicidad comportamental en línea, lo explota y no tiene ningún reparo a la hora de ofrecerse a los anunciantes como mediador entre ellos y los usuarios a cambio de una contraprestación económica. Ha hecho un negocio de ello, presumiendo de poder desglosar a los usuarios de la red social en segmentos potenciales de consumidores según los datos obtenidos por la plataforma: su ubicación, fragmento demográfico, intereses, nivel de conexión o según los *Me Gusta*[119].

Ello, sin embargo, se adecúa *a priori* a la legalidad pues todo usuario de *Facebook* debe, como requisito para crearse una cuenta, prestar su consentimiento –se presupone que previa lectura– sobre sus términos y condiciones de uso que, si bien consisten en unas cláusulas de adhesión más que abusivas, el usuario parece estar de acuerdo a aceptar cuando crea su perfil[120]. Por lo tanto, dejando de lado la ética empresarial y el mercadeo de la privacidad de sus usuarios, el inconveniente principal del almacenamiento masivo de datos es su opacidad[121].

---

[117] MAYER-SCHÖNBERGER y CUKIER señalan la posición de preeminencia en el mercado de datos adoptada por *Facebook*, empresa que no existía diez años atrás, gracias a la interacción social de sus *clientes* registrados: "sus usuarios hacen clic en el botón de *me gusta* o insertan un comentario casi tres mil millones de veces diarias, dejando un rastro digital que la compañía explota para descubrir sus preferencias". Cfr. *Big data. La revolución de los datos masivos*, ob. cit., p. 19.

[118] En un reciente artículo del Washington Post, se creó una lista de los 98 datos personales que *Facebook* maneja sobre sus usuarios, sin que éstos sean muchas veces conscientes de ello, y que permiten catalogarlos de muchas y variadas formas. Artículo disponible en https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/?utm_term=.079af4e1045f

[119] https://www.facebook.com/business/learn/facebook-ads-choose-audience.

[120] No obstante como señala NOAIN SÁNCHEZ ello podría discutirse ya que Facebook utiliza el sistema de consentimiento pasivo (*Opt-out*), lo que implica que el interactor no es preguntado sobre si se pueden usar sus datos, sino que se da por hecho que si no manifiesta lo contrario y sigue usando el servicio, otorga su aquiescencia. Y, dado que dicho consentimiento no es explícito en la mayoría de redes sociales, al firmar el acuerdo de usuario y aceptar las condiciones del

Está demostrado que los datos personales tienen un importante valor de mercado y también que hay empresas dedicadas única y exclusivamente al almacenamiento masivo de datos. Y, si bien hasta ahora se están empleando con fines exclusivamente publicitarios, puede ser que en el futuro no se generen suficientes beneficios y decida emplearse la información personal para otros usos.

Por ejemplo, ¿qué ocurriría si una compañía acumula una deuda impagable y para evitar un concurso de acreedores o una bancarrota, decide vender la información más sensible para generar ingresos?, ¿las aseguradoras privadas de salud estarían interesadas en saber de antemano el historial médico de aquéllos que solicitan contratar con ellas?... o, en un escenario peor, son muchos los usos que podrían darse a los datos personales en manos de la economía criminal. El *Big data* en connivencia con Internet, se está convirtiendo en un mercado opaco dónde la materia prima es la vida íntima de las personas, y cuyos ingresos y utilidades son cada día mayores e inversamente proporcionales a la privacidad y a la seguridad jurídica de las personas. Sin embargo, la preocupación debería recaer en las aplicaciones futuras que dicha información personal tendrá y que aún se desconocen.

De lo que no hay duda es que se está comercializando con nuestros datos personales así como que hay empresas dedicadas -única y exclusivamente- al mercadeo de éstos, sin embargo, dada la falta de transparencia del sector es imposible extraer cifras concretas del negocio de la privacidad. No obstante, para hacerse una idea aproximada de las ganancias que se generan en torno a ello, basta con examinar la cuenta de resultados de una empresa dedicada a este negocio. Así, siguiendo con el ejemplo de *Facebook*, cuyos últimos resultados presentados son

---

servicio, también se está dando el asentimiento para el uso y disfrute de sus informaciones. "Rizando el rizo, veremos que en el caso de *Facebook* ni siquiera es necesario dar la aprobación sobre las condiciones del servicio, sino que éstas se dan por asumidas una vez que el individuo decide abrir una cuenta en su plataforma". Cfr. *La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)*, ob. cit., p. 291.

[121] No obstante lo anterior, uno de los problemas que presenta la plataforma es el cambio unilateral de su "política de privacidad", práctica habitual mediante la cual, pese a pretender adoptar estándares más protectores de la privacidad de sus usuarios –bien por las presiones sociales, bien por la necesidad de adaptarse a ciertas normativas- a quienes hace creer que tienen el poder de decidir y controlar su información personal, el resultado final, gracias a la redacción ambigua de sus "términos y servicios", el uso de cláusulas ambiguas y el aumento de las opciones de publicidad por defecto, es que los usuarios han visto como ha disminuido notablemente el control sobre sus propios datos que, en la práctica, no pueden ejercer de manera efectiva.

los relativos al último trimestre de 2016, se observa que entre julio y septiembre de 2016, sus ingresos[122]superaron los 7 millones de dólares (unos 6.100 millones de euros), una cifra récord desde el nacimiento de la compañía. Para hacerse una idea de la magnitud de dichas cifras, según el Fondo Monetario Internacional, éstas superarían el Producto Interior Bruto de más de 40 países.

El motivo de dicho negocio son sus usuarios, cuyo crecimiento parece no tener límites (en la actualidad está a punto de alcanzar los 1.800 millones, el equivalente a casi la cuarta parte de la población mundial) y los datos personales de los mismos, *vis atractiva* de empresas publicitarias que compran espacios en la red social para anunciarse. De hecho, de estos 7 millones de ganancias, 6.820 millones (su 97%) corresponden a ingresos por publicidad. Si dividimos dichos ingresos trimestrales entre los usuarios de la red, *Facebook* habría obtenido un promedio mundial de unos 4 dólares de ganancia por cada uno de sus usuarios, lo que multiplicado por 12, se convierte en 16 dólares anuales[123].

Facebook cerró el año 2016 con una media de unos cinco dólares más por cada uno de sus usuarios, con unos ingresos totales de más de 27.500 millones de dólares, un incremento de casi un 650% respecto a los cinco años anteriores dado su incremento constante de usuarios, lo que hace del *targeting* un filón para las empresas anunciadoras cuyo número ha aumentado también exponencialmente[124]. Otra manera de calcular el valor de los datos sería ponerlo en relación con su valor de cotización en bolsa. Siguiendo con *Facebook*, si se compara su valor bursátil con el número de usuarios de la red social, la cifra resultante es un total de 227 dólares por usuario. Precisamente *Facebook* alcanzó el récord de 375.000 millones de dólares en bolsa, consolidándose como la cuarta empresa más valiosa del Mundo.

[122] http://www.bbc.com/mundo/noticias-37871331.

[123] Obviamente estas cifras varían en función del ámbito geográfico (a la cabeza, Estados Unidos y Canadá, mientras que Europa se sitúa ligeramente por encima de la media mundial) y del valor de la oferta y la demanda en cada momento.

[124] *Facebook*, junto con *Google*, controla la mitad del mercado de la publicidad en Internet. Estas empresas ven incrementados cada vez más sus ingresos por publicidad online, cuyas cifras han desbancado los medios tradicionales como la televisión que han visto como se retiraban en paralelo los recursos de los anunciantes, seducidos por las nuevas oportunidades de marketing que presenta el *Big data*.

Este modelo de negocio gira exclusivamente en torno a la explotación publicitaria de la información de sus usuarios que, paradójicamente, no se ven repercutidos económicamente de ninguna manera[125]. Ante estas cifras, parece lógico preguntarse si no deberían de cobrar a *Facebook* por el uso de sus datos, activo principal de su negocio. Sobre esta cuestión, es importante tener en cuenta que, si bien la actividad empresarial del *Facebook* se circunscribe al ámbito privado, ésta tiene una indudable relación de complementariedad con las políticas públicas, en tanto que las condiciones en que se desarrolle el negocio de *Facebook* estará determinado por el marco legal correspondiente. En este sentido, resulta instructiva la observación realizada por O'NEIL, apuntando de qué manera los beneficios obtenidos por empresas como *Facebook*, *Apple* o *Google* se encuentran estrechamente ligados al desarrollo de según qué políticas gubernamentales: "el Gobierno los regula o deja de hacerlo, aprueba o bloquea sus fusiones y adquisiciones y define las políticas fiscales (a menudo haciendo la vista gorda a los miles de millones de dólares depositados en paraísos fiscales). Esta es la razón por la que las empresas de tecnología, al igual que el resto de las grandes empresas estadounidenses, inundan Washington con grupos de presión e inyectan silenciosamente cientos de millones de dólares como donaciones al sistema político"[126].

4. Resituación: la necesidad de repensar el concepto de privacidad en el contexto *Big data* para la construcción del derecho al olvido digital como derecho fundamental

4.1 Intimidad vs. privacidad: la comprensión dialéctica del debate para construir una perspectiva integradora en el contexto del *Big data*

a) Delimitación conceptual

A menudo se confunden los términos "intimidad" y "privacidad", los cuales suelen emplearse de forma errónea como sinónimos tanto en el ámbito jurídico como en el lenguaje

[125] De hecho el dueño de *Facebook*, Mark Zuckerberg, ha afirmado categóricamente proclamas que evidencian, sin ningún tipo de reparos, su apuesta por un modelo de negocio dedicado a la explotación de la privacidad de las personas, como por ejemplo, "*la era de la vida privada ha muerto*" o "*si volviera a crear Facebook lo haría todo público por defecto*". Cfr. JOINSON. "Looking at, Lookinf up, or Keeping up with People? Motives and uses of Facebook, en *CHI 2008 Proceedings: Online Social Networks*, 2008.

[126] Cfr. *Armas de destrucción masiva. Cómo el Big data aumenta la desigualdad y amenaza la democracia*, ob. cit., p. 225.

cotidiano, pese a que ambos divergen en su significado y alcance, estando impregnados de muy diversas connotaciones. Ello se debe, principalmente, a razones históricas y filológicas pues, como más tarde se analizará, la protección de la vida privada tiene su origen en la construcción anglosajona *privacy*[127] que ha sido incorporada en nuestra tradición jurídica indistintamente como "lo privado" o "intimidad". Sin embargo, ambos términos tienen raíces distintas en la lengua latina, mientras que la palabra "privacidad" deriva del latín *privatus*, la "intimidad" procede del latino *intimus* que es una variación de *intumus*, forma superlativa del verbo *intus* cuyo significado es "dentro", por lo que se puede advertir una primera diferenciación entre ambos conceptos, y es que "intimidad" alude a aquello que está lo más dentro posible del ser humano, el ámbito más reservado de su personalidad[128].

La intimidad se circunscribe al ámbito más personal del individuo, al reducto o refugio de cada ser humano libre de toda injerencia externa y en el que se fraguan las decisiones más propias e intransferibles, desarrollándose la propia personalidad en toda su extensión[129]. Ésta forma parte de la esencia misma de la personalidad y, por ende, es inherente a todos los seres humanos, constituyéndose como una suerte de "derecho de secreto" sobre lo que somos, pensamos o hacemos[130].

En la privacidad, por su parte, aunque también integra un ámbito de protección del individuo libre de injerencias externas, la esfera de protección es mucho mayor en tanto que supera el perímetro circunscrito de lo estrictamente íntimo para abarcar otras conductas y facetas cotidianas y personales sujetas al control de la soberanía individual. A diferencia de la intimidad, el ámbito de protección de la privacidad es flexible y está sujeto a cambios pues

---

[127] Aunque se ahondará en ello en el siguiente Capítulo, brevemente procede comentar que comúnmente se ha acordado en situar el origen de la protección del derecho a la vida privada en los planteamientos llevados a cabo en el siglo XIX por SAMUEL WARREN y LOUIS BRANDEIS, que defendieron la existencia en el *common law* de un derecho a no ser molestado "*the right to be let alone*".

[128] DESANTES GUANTER. "Intimidad e información, derechos excluyentes" en *Nuestro tiempo*, nº 213, Pamplona, 1972.

[129] "La idea de intimidad se refiere a todos aquellos pensamientos, deseos, sueños, intenciones, fantasías, imaginaciones y creencias que solo una persona sabe o conoce, algo que no se comunica a nadie y que uno se lleva consigo tras su muerte", NOAIN SÁNCHEZ. *La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)*, ob. cit., p. 80.

[130] GARCÍA SAN MIGUEL. *Estudios sobre el derecho a la intimidad*, Tecnos, Madrid, 1992, p. 17.

depende del contexto, de las pautas de comportamiento e interacción respecto de un lugar, de unas costumbres o de unas necesidades individuales y sociales[131].

Así, mientras que sobre el concepto de intimidad existe cierto consenso en la doctrina[132], no existen criterios uniformes para determinar aquello que constituye la "vida privada", pues dicha concepción varia sustancialmente según las circunstancias en las que se someta a examen e incluso en función de las expectativas personales.

Con la misma orientación, se elabora la *Teoría de los círculos concéntricos o las tres esferas* en la doctrina alemana[133], según la cual debe diferenciarse entre tres niveles de confidencialidad o secretismo: primeramente, la esfera más íntima del individuo (*Intimsphäre*) impermeable a cualquier intromisión, a continuación la esfera privada (*Privatsphäre*) más permeable, en la que se incluyen aspectos personales y familiares menos íntimos y asemejada al *right to privacy* del *common law* y, finalmente, en un tercer nivel se delimita la esfera más pública pero aún protegida (*Privatsphäre*) en la que se incluyen aspectos relativos al honor y a la propia imagen[134].

---

[131] "*Because privacy involves protecting against a plurality of different harms or problems, the value of privacy is different depending upon which particular problem or harm is being protected. Not all privacy problems are equal; some are more harmful than others. Therefore, we cannot ascribe an abstract value to privacy. Its value will differ substantially depending upon the kind of problem or harm we are safeguarding against. Thus, to understand privacy, we must conceptualize it and its value more pluralistically. Privacy is a set of protections against a related set of problems. These problems are not all related in the same way, but they resemble each other*", SOLOVE. "I've Got Nothing to Hide and Other Misunderstandings of Privacy" en *San Diego Law Review*, Vol. 44, 2007, p. 763.

[132] Las definiciones que proporcionan la mayoría de los autores no difieren sustancialmente entre ellas, aunque ciertamente pueden apreciarse matices. Como muestra, ALBALADEJO entiende la intimidad personal como "el poder concedido a la persona sobre el conjunto de actividades que forman un círculo íntimo, personal y familiar, poder que le permite excluir a los extraños de entrometerse en él y de darle una publicidad que no desee el interesado", Cfr. *Derecho Civil I. Introducción y Parte General*, Edisofer, Madrid, 2009, p. 460; DÍEZ PICAZO Y GULLÓN lo definen como "la esfera secreta de la propia persona que debe ser protegida contra las intromisiones e indagaciones ajenas", Cfr. *Sistema de Derecho Civil*, Tecnos, Vol. 1, Madrid, 1992, p. 340; Para LÓPEZ GUERRA se trata de "el reducto más privado de la vida del individuo, esto es, aquellos extremos más personales de su vida y su entorno familiar", Cfr. *Derecho Constitucional*, Tirant lo Blanch, València, 2007, p. 231.

[133] Dicha doctrina tiene su origen en las disertaciones de HUBMANN aunque posteriormente fue acogida y reelaborada por el Tribunal Constitucional Alemán. Cfr. *Das Persönlichkeitsrecht*, Böhlau, Colonia, 1967.

[134] Esta teoría ha sido acogida en nuestra tradición jurídica, entre otros, por DESANTES GUANTER y SORIA quienes defienden: "La esfera de la vida pública puede y debe ser siempre objeto de la información: la esfera de la vida privada puede ser siempre objeto del mensaje, pero debe serlo tan solo cuando la actuación privada trascienda a la vida pública; la vida íntima no solo no es informable, sino que ni siquiera es investigable. No puede, ni debe ser objeto de la información.

Así, como si de una muñeca rusa se tratare, el Tribunal Constitucional alemán entiende que sólo el ámbito más "íntimo" de una persona está libre de cualquier injerencia externa, mientras que ampliando un poco más el círculo deben ponderarse los intereses en juego en el caso concreto para examinar sí cabe o no vulneración en este segundo nivel de "privacidad". Por último, el nivel más bajo de protección vendría conformado por "lo público", mínimamente sometido a hermetismos individuales y permeable a todo tipo de intervenciones[135].

Sin embargo, dicha teoría ha sido ampliamente criticada principalmente por la imposibilidad de objetivar la intimidad, pues dichos niveles de privacidad no son uniformes sino que cada individuo, en función de sus circunstancias personales y de sus pretensiones sociales, configura libre o inconscientemente los diámetros de dichas esferas, lo que plantea numerosos problemas a la hora de delimitar los ámbitos de protección[136].

La distinción entre lo "íntimo" y lo "privado" ha sido llevada a cabo también por GARZÓN VALDÉS que entiende que aquello íntimo viene formado por los pensamientos de cada cual y por tanto es el origen de la formación de las decisiones, circunscribiéndose a un ámbito exento de la intervención de terceros a quienes tampoco afecta la intimidad de lo ajeno, tratándose de "un velo de total opacidad que sólo puede ser levantado por el individuo mismo"[137].

Es un núcleo totalmente reservado". Cfr. *Los límites de la información. La información en la jurisprudencia del Tribunal Constitucional: las 100 primeras sentencias*, APM, Madrid, 1991, p. 108.

[135] El *Bundesverfassungsgericht* construyó dicha teoría en torno a los derechos de la personalidad y destacando los vínculos de éstos con el derecho de dignidad de la persona, ambos reconocidos respectivamente, en los artículos 2.1 ("*Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt"*) y 1.1 ("*Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt"*) de la *Grundgesetz für die Bundesrepublik Deutschland*, de la Constitución de la República Federal Alemana.

[136] Como más adelante se profundizará, en la tradición jurídica del *common law*, COOLEY diferenció también entre distintos niveles de privacidad, de mayor a menor: la intrusión sobre la reclusión o los asuntos privados de una persona, la divulgación pública de hechos privados que puedan comprometer el honor, la publicidad de hechos falsos que comporten un daño al sujeto y la apropiación de la identidad personal de alguien. Cfr. *The law of torts*, Callaghan, Chicago, 1930.

[137] Lo íntimo se integra también por "las dudas que escapan a una clara formulación, de lo reprimido, de lo aún no expresado y que quizás nunca lo será, no sólo porque no se desea expresarlo sino porque es inexpresable". Cfr. GARZÓN VALDÉS. "Lo íntimo, lo privado y lo público", en *Claves de la razón práctica*, nº 137, Madrid, 2003, p.15.

Por el contrario, la privacidad, pese a ser condición necesaria para el ejercicio de la libertad individual, tiene unos límites altamente difusos, pues dependen en todo caso del contexto cultural y social. Esta esfera se desliga de la total opacidad de lo íntimo así como de la transparencia inherente a lo público, situándose entre ambos extremos, en función de las reglas de comportamiento imperantes en un determinado contexto.

Así, la intimidad es el ámbito en el que el individuo ejerce plenamente su autonomía personal, el confín último de la personalidad, donde uno es plenamente soberano para decidir sus formas de comportamiento social, privado o público. Y la privacidad puede presentar diversas características según la naturaleza de las relaciones interpersonales que se desenvuelvan en dicho ámbito -así, cuanto más connotaciones públicas adquiera el papel que un individuo desempeñe en la sociedad, menor será la esfera de su vida privada-, constituyéndose por reglas de convivencia que tienden a preservar la intimidad personal y se erigen como barreras a la invasión de lo público.

De ello se desprende que la intimidad no se opone a lo privado, y a pesar de que comparte ciertas atribuciones, se distingue de ésta por su dimensión, mucho menor. Sin embargo, el origen de ambos radica en la defensa liberal de la autonomía y la necesidad de un dominio reservado para la plena realización de los individuos, aunque con distinta intensidad[138], siendo justificada su protección y garantía por idénticas razones.

Podría decirse que, mientras que el derecho a la intimidad se relaciona con el poder que cada individuo tiene para controlar la injerencia externa en su esfera más íntima, el derecho a la privacidad permite controlar el acceso, el alcance y la difusión de los demás a ese dominio íntimo. Igualmente, mientras que la intimidad es necesaria para salvaguardar la autonomía personal y el libre desarrollo de la personalidad, la privacidad abarca una dimensión mayor en el contexto de las relaciones interpersonales, proporcionando un espacio libre para llevar a cabo una multiplicidad de actos entre los que se incluye el intercambio de información personal[139].

[138] Cfr. BÉJAR. *El ámbito íntimo. Privacidad, individualismo y modernidad*, Alianza, Madrid, 1989.

[139] "*The content of privacy cannot be captured if we focus exclusively on either information, access, or intimate decisions because privacy involves all three areas* […] *privacy's content covers intimate information, access, and decisions. The*

De este modo, intimidad y privacidad son realidades distintas aunque relacionadas y tienen un objetivo común: la ausencia de difusión -resguardarse de la publicidad no deseada-, reservando al individuo una parcela libre de injerencias.

b) Consecuencias prácticas del debate: la privacidad como estándar y garantía de la protección de datos personales

La protección constitucional de lo privado se circunscribe al ámbito de la intimidad, como se deduce del tenor literal del artículo 18 de la Constitución española. Se considera así que en dicho precepto hay tres derechos fundamentales distintos, el derecho al honor, a la intimidad personal y familiar y a la propia imagen[140], al que se le puede hoy en día añadir uno más: la protección de datos personales.

Nótese que dicho artículo constitucional habla de "intimidad" y no de "privacidad" y, ello tiene gran relevancia en cuanto al desarrollo doctrinal y jurisprudencial que ha producido dicho concepto, mediante el cual se ha circunscrito su ámbito de garantía al "ámbito propio y reservado" de las personas cuya efectiva existencia es necesaria para alcanzar una "calidad mínima de vida humana"[141].

Pese a que por razones de extensión no se desarrollará un exhaustivo examen doctrinal y jurisprudencial acerca del concepto constitucional de intimidad, más adelante se incidirá en las cuestiones de mayor importancia[142], sí que puede avanzarse cómo dicho tratamiento ha supuesto en la práctica una disminución considerable del alcance de la garantía de dicho precepto, limitando su protección a aquellos aspectos más íntimos de los sujetos, y dejando sin tutela determinadas conductas que, si bien constituyen una intromisión en la privacidad

---

problem with understanding privacy as intimacy, however, is that not all private information or decisions we make are intimate"". Cfr. INNES. *Privacy, Intimacy and Isolation*, Oxford University Press, New York, 1992, p. 56.

[140] O'CALLAGHAN MUÑOZ. *Libertad de expresión y sus límites: honor, intimidad e imagen*, Edersa, Madrid, 1991, p. 96.

[141] STC 231/1988, de 2 de diciembre, FJ 3º.

[142] Vid. *infra* Cap. III.

personal, no vulneran el estricto ámbito de la intimidad[143]. Ello se ha intentado paliar con el reconocimiento del derecho a la protección de datos personales, sin embargo aquí podría decirse del legislador que ha incurrido en ciertas inconsistencias y confusiones terminológicas, como se expone a continuación.

Si bien el derecho a la protección de datos, como más adelante se ahondará, está hoy en día reconocido como un derecho fundamental y autónomo, ello no se deriva del texto constitucional, sino de la jurisprudencia del Tribunal Constitucional, que lo ha considerado incluido dentro del párrafo cuarto del artículo 18. Así se reconoció inicialmente por la STC 94/1998, de 4 de mayo y más profundamente por la STC 292/2000, de 30 de noviembre en la que, por primera vez, se habla de la existencia de un "derecho fundamental a la protección de datos" y se preocupa de diferenciarlo del derecho a la intimidad, señalando que, si bien comparte con él "*el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar*", se distingue del mismo porque "*atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley*" (FJ 2º).

Así las cosas, su protección formal se ha llevado a cabo mediante leyes orgánicas, y es aquí dónde encontramos la disparidad de criterios. Resulta curioso como en la Exposición de Motivos de la derogada Ley de Protección de Datos Personales de 1992[144] (LORTAD), se diferenciaba expresamente entre el concepto de intimidad y privacidad, precisamente para extender la protección de dicha ley cualquiera que fuese el grado de lesión, sin distinguir entre el ámbito privado y el ámbito íntimo[145]. En este sentido, decía la LORTAD que, mientras que

[143] Se ha desarrollado una protección constitucional de la intimidad en base a determinados supuestos de hecho, entre los que se procede reseñar: inviolabilidad del domicilio, integridad corporal, casos de especial sujeción, secreto de las comunicaciones, protección de la salud, libertad sexual, libertad informática y conflicto de derechos.

[144] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD).

[145] De acuerdo con la exposición de motivos: "*Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona -el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo-, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad*

la intimidad personal queda garantizada constitucionalmente por los tres primeros apartados del artículo 18 CE, el último párrafo del precepto es el que da cobijo legal a todo el resto de conductas que, mediante el uso de la informática y sin hacer injerencia directa en el ámbito íntimo de una persona, tienen incidencia en la esfera privada de las personas.

Sin embargo, la vigente Ley Orgánica de Protección de Datos[146] (LOPD), pese a ampliar su ámbito de aplicación a cualquier tratamiento de datos personales con independencia de los medios utilizados en el mismo, abandona toda referencia a la privacidad y dispone como ámbito de su protección la intimidad personal y familiar[147], produciendo una confusión terminológica en cuanto al ámbito de protección[148].

El ordenamiento jurídico, cada vez más garantista con los aspectos privados de los ciudadanos, debería ir en consonancia con la delimitación de los ámbitos privados del sujeto en orden a facilitar su protección. El artículo 18.4 CE toma un cariz protagonista en las demandas de la sociedad que ven como la informática y las nuevas tecnologías se apoderan de sus recodos más personales, cobrando una entidad propia más allá de la estricta intimidad.

Suscribimos así las palabras de ÁLVAREZ-CIENFUEGOS SUÁREZ[149] que distingue, junto con la intimidad, "una esfera más amplia y quizá de protección menos enérgica que recibe el nombre de privacidad, siguiendo el anglicismo de la *privacy*. La cual viene referida a datos o informaciones no íntimos, pero que el individuo desea que sólo sean conocidos por determinadas personas, queriendo sustraer su conocimiento a núcleos más amplios de la sociedad".

---

que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado".

[146] Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (LOPD).

[147] Artículo 1 LOPD: "*La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*".

[148] El Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, por su parte, sigue con dicha línea argumental haciendo mención de la "privacidad" sólo respecto de las comunicaciones electrónicas, en su Disposición adicional decimocuarta.

[149] Cfr. *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, Pamplona 1999, p. 71.

Defendemos pues la adopción del término "privacidad" como el más idóneo para describir la realidad presente, en la que el *Big data* en concurrencia con la revolución informática y tecnológica, ocasionan riesgos y lesiones para ciertos ámbitos personales de los individuos que, sin penetrar necesariamente en su estricta intimidad, calan en su ámbito más privado, suscitando igualmente molestias y perjuicios[150].

De acuerdo con lo expuesto, entendemos la privacidad como aquella esfera personal, integrada por informaciones y comportamientos no íntimos, que el individuo desea que sólo sean conocidos por él o por determinadas personas con las que voluntariamente quiera compartirlos, sustrayendo su conocimiento a núcleos más amplios de la sociedad. Se pretende así adoptar una postura más garantista de la esfera privada de las personas, ciertamente necesaria tiendo en cuenta las circunstancias concurrentes.

c) Toma de postura: una refundamentación de la privacidad desde la protección de la libertad frente a los riesgos del Big data

Gracias a Internet todo es público -todo está al alcance de todos-, incluso lo privado, y además es permanente en el tiempo, lo que indudablemente ha repercutido mermando nuestros derechos fundamentales. La realidad tecnológico-digital ha convertido en lesiones potenciales y crecientes algunas conductas que antaño se consideraban remotas o de mínimo riesgo[151]. Así por ejemplo, como se ha visto en apartados anteriores, con la recolección, almacenamiento y tratamiento en masa de los datos personales de los ciudadanos, la privacidad personal está más expuesta que nunca y, en consecuencia, el riesgo de sufrir un daño es ciertamente real.

---

[150] Nuestra intimidad quizás no quede vulnerada cuando *Google Maps* solicita tener acceso a nuestra localización ni tampoco cuando las *cookies* de Internet almacenan nuestras preferencias a la hora de navegar por la Red pero, ¿acaso ello no afecta a nuestra privacidad? Aspectos secundarios de nuestra personalidad quedan expuestos en el uso de las nuevas tecnologías online y, según el alcance de su exposición y su puesta en relación, sin duda puede verse afectada nuestra vida privada.

[151] Si bien es cierto que la privacidad engloba facetas personales que, por si mismas pueden carecer de relevancia, cuando éstas se relacionan entre ellas, pueden perjudicar seriamente los derechos fundamentales de un individuo. Como ejemplo, las conductas de agregación y triangulación de datos personales que, si bien por si mismos pueden no ser relevantes, puestos en relación permiten identificar perfectamente a una persona.

Con el desarrollo de las nuevas técnicas informáticas se han roto las fronteras físicas que protegían la privacidad de las personas y además han supuesto un efecto multiplicador para las lesiones de los derechos de la personalidad. Paralelamente, también se ha producido una aparente democratización –por equiparación del riesgo sin diferencias de clases, aunque cualitativamente sus consecuencias puedan ser distintas- de la esfera privada, al menos en nuestro entorno más inmediato, en el que las posibilidades de la mayoría de la ciudadanía de acceder a las nuevas tecnologías, hace que ésta se exponga por igual a sufrir injerencias en su vida privada[152].

La sociedad avanzada requiere repensar los términos y los medios de protección de las esfera privada de sus ciudadanos, como consecuencia lógica del desarrollo garantista de la intimidad personal frente a los desafíos que la nueva coyuntura ofrece para los bienes jurídicos. Las nuevas facetas de la vida privada requieren nuevos medios de tutela jurídica que deben ampliar su rango de protección en tanto que la esfera privada ha sido exponencialmente puesta en riesgo. En este sentido, las intromisiones en la privacidad de las personas, cada vez más frecuentes gracias a la intermediación de los fenómenos anteriores, no pueden quedar impunes por no cumplirse todos los requisitos que para la protección de la intimidad se requieren. El ordenamiento debe dar respuesta a dichas conductas que lesionan otros derechos fundamentales y suponen conductas discriminatorias.

Como se ha argumentado, la privacidad abarca un espectro mucho más amplio de la esfera personal que la clásica intimidad, pero a la vez, mucho más accesible y vulnerable. La esfera de privacidad incluye muchos otros aspectos aparte de la intimidad personal, entre ellos la facultad de toda persona de ejercer un autocontrol sobre su información personal. Ello

[152] No obstante, dicha democratización es sólo aparente, porque dicha cuestión sólo concierne a la población occidental "desarrollada" -empleando la terminología usual en la cuestión- que tiene a su alcance Internet y los medios tecnológicos en torno a él. Una muestra de ello, y en relación con el derecho al olvido digital que se tratará más adelante, es el hecho de que las personas con gran nivel adquisitivo, pueden interferir en la lógica del mercado y deshacerse de la inercia mayoritaria, por ejemplo, contratando servicios de borrado de huella digital o influyendo en los posicionamientos de los buscadores web.

conlleva una extensión de la libertad individual, pues la privacidad implica control[153], autodeterminación.

Así, en el contexto del *Big data*, hablamos de privacidad para referirnos a la esfera de libertad que todo ser humano tiene respecto de sus datos de carácter personal, información que, si bien no en todas las ocasiones puede lesionar su intimidad, afecta a otra esfera menos restringida pero igualmente protegida por el Derecho[154]. En consecuencia, ante esta casuística, es preciso abandonar la concepción tradicional de la vida privada como un *status* negativo pues la protección de la privacidad sin duda es un derecho activo de control, de defensa si se prefiere, que permite a cada individuo controlar el ámbito de privacidad deseado, concediéndole asimismo herramientas efectivas para reaccionar frente a cualquier intromisión.

De este modo, la estrecha conexión que liga el derecho a la autodeterminación informativa con el derecho a la intimidad no tiene por qué traducirse en una concepción individualista de ésta, en la medida en que la propia intimidad ha dejado de ser un privilegio del hombre aislado para devenir en un valor constitucional de la vida comunitaria[155]. Lo que se pretende es reconocer la pluralidad de manifestaciones que tiene la esfera privada, concediendo a todas ellas protección jurídica, cuyo contenido no obstante, variará de mayor a menor, en función de la cercanía al núcleo más íntimo de la personalidad. Las circunstancias sociales, culturales e históricas aconsejan ampliar el concepto y la garantía de lo privado de la "intimidad" a la "privacidad", siempre desde una concepción integradora y comprensiva.

Somos conscientes, no obstante, de que la privacidad no es un valor absoluto. De hecho su mutabilidad y la indefinición de su concepto dificultan en ocasiones su protección. Ciertamente no se puede ignorar que se trata de un concepto subjetivo también susceptible de influencias externas. Por una parte, el espacio privado lo define el propio sujeto que en cierta

[153] WESTIN fue un pionero al examinar la privacidad desde un punto de vista positivo, no como una libertad negativa del individuo, identificando la privacidad con la facultad de control sobre nuestras propias informaciones. Cfr. *Privacy and freedom*, Athenaeum, New York, 1967.

[154] Así, cuanto mayor sea el control que sobre nuestros datos tengamos, mayor será nuestra esfera de privacidad y viceversa.

[155] PÉREZ LUÑO. *Los derechos humanos en la sociedad tecnológica*, Universitas, Madrid, 2012, p. 94.

manera decide los límites de su privacidad, pero al mismo tiempo, la privacidad debe ponerse en relación con el contexto histórico-social, el entorno cultural, el bien común y el *status* de la autonomía individual[156].

Compartimos pues la visión de LÓPEZ JACOISTE[157] cuando, al definir los derechos de la personalidad, les atribuye cierto carácter de mutabilidad pues la personalidad está en constante evolución y varia en función del contexto social, ya que es muy sensible a las conceptualizaciones del momento así como voluble respecto de las amenazas que en cada situación pueden peligrar la integridad de los derechos personales.

Sin embargo, ello no obsta para que el ordenamiento jurídico reconozca, como le es exigible, la realidad social actual y actúe en consonancia para dotar a los ciudadanos de herramientas jurídicas adecuadas para preservar este ámbito de la vida privada de los sujetos definido como "privacidad" pues de ello depende la garantía unitaria de los derechos fundamentales.

Así lo consideró CONSTANT siglos atrás cuando, estableciendo una diferenciación entre la libertad de los antiguos -basada en la participación activa y constante en el ejercicio del poder colectivo- y la libertad de los modernos -basada en el disfrute apacible de la

[156] La diversidad cultural y las infinitas vertientes de moralidad existentes, convierten en una tarea extremadamente difícil estudiar la privacidad desde una perspectiva universal. Partiendo de la base de que la colectividad hace las normas y que el Derecho, al menos en las sociedades democráticas, es un conjunto de pautas de comportamiento comúnmente aceptadas, podemos concluir que éstas varían en función del contexto cultural. Así por ejemplo, en nuestra sociedad se valora positivamente la privacidad, como una extensión de nuestra libertad, por lo que se procura reservar una parcela libre de injerencias externas, en la que desenvolverse con plena autonomía para el desarrollo de la personalidad. En nuestra tradición jurídica, la privacidad se convierte en un derecho y una excepción al régimen general de libertad a la que se le imponen ciertos límites cuando colisiona con anteriores derechos, entre ellos el derecho a la vida privada y familiar. Sin embargo, en otras culturas, por ejemplo la iraní, en la que las mujeres tienen prohibido enseñar su cuerpo y cabello en cualquier lugar excepto en su propia casa -existiendo incluso la Policía de la Moral que se encarga de controlar que la indumentaria y comportamiento de las mujeres se ciñe a unos codificados valores islámicos- la privacidad no es un derecho sino una imposición social. En este caso, la privacidad no se percibe siempre como un valor de libertad sino todo lo contrario, como una obligación.

[157] LÓPEZ JACOISTE. "Una aproximación tópica a los derechos de la personalidad", en *Anuario de Derecho Civil*, Vol. 39, nº14, 1986, pp. 1059-1120.

independencia privada-, defendió que la privacidad era presupuesto indispensable para la protección de la gran mayoría de los derechos individuales[158].

En consonancia con todo lo anterior, a lo largo de la presente investigación se emplea el término "privacidad", de forma consciente y en contraposición al concepto de intimidad, en base a la distinción que se ha razonado y con la intención de mantener una coherencia argumental en todo el trabajo.

4.2 La construcción del derecho al olvido digital como derecho fundamental: una exigencia para la protección de la libertad en el Estado social y democrático de Derecho

Desde hace un tiempo venimos asistiendo a un vertiginoso cambio tecnológico-social hasta el punto de que impera la sensación de transición constante que, sin embargo, no se ha traducido significativamente al Derecho, incapaz de adaptarse con agilidad al nuevo paradigma ni de anticiparse a realidades futuras. Un ejemplo claro sería la noción de "Estado" o "frontera", totalmente superado por la realidad de Internet, de jurisdicción mundial si cabe, cuyo poder territorial carece de sentido hoy día, por ejemplo, ante casos de vulneraciones de derechos en las transferencias internacionales de datos personales. En relación con la sociedad globalizada a la que hoy pertenecemos, parece interesante contraponer dos perspectivas distintas acerca de su incidencia en los derechos humanos. Hay autores como PÉREZ LUÑO que sostienen la existencia de una relación estrecha entre globalidad y universalidad de los derechos, señalando que "en la esfera jurídica, la globalización ha potenciado que se difunda la exigencia humanista y cosmopolita de situar los valores y derechos de la persona por encima de la coyuntura de las fronteras nacionales. La erosión de la soberanía de los Estados en la era de la globalización ha favorecido la defensa del valor de la universalidad de los derechos humanos, que ha tenido, las más de las veces, una de sus quiebras y límites más implacables en el ejercicio de la soberanía estatal"[159].

[158] Cfr. CONSTANT. *Cours de Politique Constitutionelle*, Didier, París, 1836.

[159] Cfr. "Los derechos humanos en la sociedad global", en *La tercera generación de derechos humanos*, Thomson-Aranzadi, Cizur Menor, 2006, p. 247.

La modernidad líquida y la mutabilidad que conlleva originan en la sociedad la sensación permanente de volatilidad, lo que ciertamente supone incertidumbre y claro está, inseguridad jurídica. Esta nueva realidad incita a repensar y reconfigurar conceptos que indudablemente han adquirido un nuevo significado, como "intimidad", "vida privada" o de "lo público" y "lo privado". De acuerdo con BAUMAN, "ya no es cierto que lo *público* se haya propuesto *colonizar* lo *privado*. Es más bien todo lo contrario: lo privado coloniza el espacio público, dejando salir y alejando todo aquello que no puede ser completamente expresado sin dejar residuos en la jerga de las preocupaciones, las inquietudes y los objetos privados. Cuando se le ha dicho repetidamente al individuo que es el arquitecto de su propio destino, tiene pocas razones para dar *relevancia tópica* a nada que se resista a ser engullido por el yo o a ser manejado dentro de sus instalaciones; pero tener un razón para ello y actuar en consecuencia es precisamente la marca distintiva del ciudadano"[160].

Ni las nuevas tecnologías ni Internet han creado nuevos bienes jurídicos protegidos, ni sustanciales cambios en los principios y valores del ordenamiento jurídico, pero sin embargo, sí que han aumentado exponencialmente las vulneraciones de derechos creando, incluso, nuevas formas de lesión. Frente a este nuevo escenario, se exige una reacción proporcionada por parte del Derecho que dote de mecanismos jurídicos adecuados para atender nuevas realidades que reconozcan nuevos derechos capaces de reflejar nuevas necesidades, si fuera necesario. En la relación entre la tecnología y el Derecho, se parte de presupuestos contrapuestos. Este último se caracteriza, desgraciadamente, por su lentitud a la hora de reaccionar ante el surgimiento de fenómenos sociales y jurídicos intempestivos, de raíz tecnológica, de modo que, cuando finalmente lo hace, pronto queda superado por el devenir de los acontecimientos ya que la informática y la tecnología están en continua evolución, conduciendo los procedimientos de tutela jurídica al anacronismo.

Internet ha condicionado sobremanera la privacidad de las personas y sus derechos derivados en tanto que tiene un efecto multiplicador de los atentados que contra éstos puedan tener lugar. La exposición masiva de información, accesible desde cualquier punto del planeta,

[160] Cfr. *Modernidad líquida*, ob. cit., p. 45.

ha creado un ambiente propicio para perpetrar vulneraciones de derechos fundamentales como la igualdad, la intimidad, la dignidad, la libertad, la propia imagen o el honor. Sobre esta cuestión, es curioso cómo se tiene la creencia generalizada de que Internet incrementa la libertad de las personas mientras que, ante un supuesto de vulneración de derechos, esas "virtudes" se convierten en impedimentos para lograr la restitución de lo afectado y, aún más, para exigir responsabilidades por su causa. Esa es la gran paradoja de Internet, la contraposición entre la facilidad con la que la información fluye por la Red de forma ilimitada -paradigma de la libertad de expresión e información- y la dificultad de eliminar aquél contenido que produce una lesión de derechos fundamentales, por la propia lógica de funcionamiento del sistema.

En este sentido, cuanto más extensa es la innovación tecnológica y cuanto mayor sea su generalización, menor es el ámbito de privacidad reservado a los individuos y menores son sus armas para proteger. Lo cierto es que deviene una fuerza de ataque en lo que PÉREZ LUÑO[161] ha denominado "asalto tecnológico de los derechos y libertades", donde resulta difícilmente negable la injerencia de la informática de control individual y colectivo que comprometen gravemente valores como la identidad, dignidad e igualdad, así como respecto de la propia seguridad jurídica[162]. La deseable concepción extendida de los derechos que auspició DWORKIN[163] no parece compatible con el devenir de la realidad económica, social y cultural actual cuyas estructuras jurídicas y políticas no están suficientemente bien articuladas como para que dicha universalidad sea una realidad jurídica. Así, la comprensión contextualizada de los derechos y de las condiciones de efectividad reales y presentes en los mismos nos lleva a considerar como utópicas o prematuras algunas teorías en torno a ellos.

[161] Cfr. PÉREZ LUÑO. *Los derechos humanos en la sociedad tecnológica*, Universitas, Madrid, 2012, p. 23.

[162] Siguiendo con la obra de PÉREZ LUÑO, se parte de las dos exigencias desarrolladas por el autor para la construcción del concepto de seguridad jurídica. En primer lugar, se entendería como *corrección estructural*, en cuanto garantía de disposición y formulación regular de las normas e instituciones integradoras de un sistema jurídico. En segundo lugar, parte de la exigencia de *corrección funcional*, que supone la garantía de cumplimiento del Derecho por todos sus destinatarios, así como una regularidad en la actuación de los órganos encargados de su aplicación. Cfr. *La seguridad jurídica*, Ariel, Barcelona, 1991, pp. 23-26.

[163] Cfr. *Los derechos en serio*, Ariel, Barcelona, 1984.

Ahora bien, podemos plantear dicha cuestión siguiendo la idea de ANSUÁTEGUI ROIG, según el cual, hablar de universalidad de los derechos "*no supone describir una realidad sino más bien intentar cambiarla*"[164]. Desde este punto de vista, la universalidad de los derechos se nos presenta como un ideal regulativo, por lo que la regulación del derecho al olvido puede ser un punto de inflexión para conseguir una efectividad jurídica como derechos fundamentales asociados al entorno digital.

De forma consecuente con los objetivos de esta investigación, reconocida la transformación en términos cualitativos que ha experimentado la protección de datos personales -privacidad en última instancia- en el ámbito del *Big data*, será necesario desarrollar una propuesta doctrinal coherente que armonice la protección de los derechos y libertades de la ciudadanía con este panorama digital. Una vez asumida como una de las muchas realidades conflictivas resultantes de la *posmodernidad*, la postura que esta tesis adopta no supone negar el uso de los datos masivos, pues este escenario, además de ser irreversible, puede ser muy beneficioso para la ciudadanía, sólo precisa que su desarrollo se encuentre inspirado por los presupuestos estructurales de un Estado social y democrático de Derecho[165].

Éstos no son otros que el disfrute de los derechos y libertades públicas, garantías que, incluso en el caso de los derechos fundamentales, no han tenido un carácter ontológico, no responden a estructuras lógico-objetivas o valores inmutables. Todo lo contrario, han sido objeto de un desarrollo histórico diferenciado atendiendo a las dinámicas de transformación social propias de una realidad conflictiva. En este sentido, los derechos fundamentales emergen como respuesta a dichos conflictos, para así garantizar en última instancia el respeto a la dignidad de la persona, a su propia capacidad para desarrollarse de acuerdo con el principio general de libertad. No puede obviarse la necesidad de asegurar el respeto a las condiciones

[164] Cfr. "La cuestión de la universalidad de los derechos: de las instituciones a los problemas" en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. IV, Dykinson, Madrid, 2013, p. 118.

[165] Así, MAYER-SCHÖNBERGER y CUKIER señalan de qué manera "los datos masivos señalan el momento en que la *sociedad de la información* por fin cumple la promesa implícita en su nombre. Los datos son el eje del todo. Todos esos fragmentos digitales que hemos reunido pueden explotarse ahora de formas novedosas para servir a nuevos propósitos y liberar nuevas formas de valor. Pero esto requiere una forma de pensar nueva, y supondrá un desafío para nuestras instituciones e incluso para nuestro sentido de la identidad. La única certeza radica en que la cantidad de datos seguirá creciendo, igual que la capacidad de procesarlos todos". Cfr. *Big data. La revolución de los datos masivos*, ob. cit., p. 233.

materiales que permiten el disfrute de esta libertad de forma plena, o dicho de otro modo: no es lo mismo ser libre que tener la capacidad de serlo.

Sería ésta una postura deudora del *garantismo* elaborado por FERRAJOLI[166], en relación con su defensa de la subordinación de la legitimidad del ordenamiento jurídico al aseguramiento de las condiciones efectivas de disfrute de los derechos fundamentales. Se trata de una doctrina de legitimación denominada por el autor italiano como *democracia sustancial*, entendida como sistema dotado de garantías efectivas, tanto liberales como sociales, donde se manifiestan los derechos fundamentales de los ciudadanos frente a los poderes del Estado[167].

Partiendo de estos presupuestos ideológicos, la respuesta desarrollada en este trabajo respecto del conflicto que representa el *Big data* para el libre desarrollo de la personalidad, en relación con los riesgos para la protección de la privacidad, se concretará en la construcción desde los derechos fundamentales de un modelo garantista de derecho al olvido que permita, sin renunciar al disfrute de los avances tecnológicos, proteger la esfera de privacidad, libertad en última instancia, de la ciudadanía. De acuerdo con O'NEIL, "los procesos del *big data* codifican el pasado. No inventan el futuro. Para inventar el futuro hace falta imaginación moral y eso es algo que solo los seres humanos pueden ofrecer. Debemos integrar de forma explícita mejores valores en nuestros algoritmos y crear modelos de *big data* que sigan nuestro ejemplo ético. Y a veces eso significa dar prioridad a la justicia antes que a los beneficios"[168]. Efectivamente, la crítica[169] contenida en estas páginas no supone una impugnación, una enmienda a la totalidad del *Big data* como fenómeno social, sino únicamente respecto de aquellas cuestiones que puedan suponer un retroceso en materia de derechos y libertades.

---

[166] Para FERRAJOLI, "el garantismo opera como doctrina jurídica de legitimación y sobre todo de deslegitimación interna". Cfr. *Derecho y razón. Teoría del garantismo penal*, Trotta, Madrid, 2009, p. 852.

[167] *Ibid*., p. 864.

[168] Cfr. *Armas de destrucción masiva. Cómo el Big data aumenta la desigualdad y amenaza la democracia*, ob. cit., pp. 252-253.

[169] Como afirma GARCÉS, en relación con la necesaria vocación crítica necesaria para defender y actualizar los postulados de la Ilustración: "lo que la ilustración radical exige es poder ejercer la libertad de someter cualquier saber y cualquier creencia a examen, venga de donde venga, la formule quien la formule, sin presupuestos ni argumentos de autoridad. Este examen necesario, sobre la palabra de los otros y, especialmente, sobre el pensamiento propio, es a lo que empiezan a llamar entonces, de manera genérica, la crítica". Cfr. *Nueva ilustración radical*, ob. cit., pp. 36-37.

Asimismo, el desarrollo del derecho al olvido como derecho fundamental es una exigencia derivada del espacio de previsibilidad objetiva que el Estado debe ofrecer a la ciudadanía para conocer los límites en el ejercicio de sus derechos y libertades, pero también las restricciones establecidas antes las posibles injerencias de terceros, como ocurriría en el caso de la privacidad. En este sentido, DÍAZ apunta de qué manera "la mera existencia de un derecho produce seguridad; puede decirse, desde esta perspectiva, que el *valor* seguridad, aunque sólo sea en ese momento incipiente, es algo que aparece irremediablemente cuando comienza a hablarse de lo que el Derecho *es* y de lo que el Derecho *hace* en la sociedad. Y algo similar podría decirse de la justicia, o de la libertad, y en general de los valores jurídicos. De momento, lo que se constata es que el *Derecho*, en cuanto sistema de *legalidad*, produce *seguridad*"[170].

Aplicando esta argumentación a la construcción del derecho al olvido, considerado como derecho fundamental, puede aportar un espacio de seguridad a la propia regularidad estructural del ordenamiento jurídico, necesitado de respuestas ante el desafío del *Big data* en relación con la protección de la privacidad de ciudadanía[171]. Por lo tanto, su aplicación en el medio social vendría a subsanar la falta de seguridad jurídica producida por la lenta respuesta legislativa a uno de los más importantes cambios estructurales de nuestrahistoria reciente, en este caso fruto del contexto de la "modernidad líquida", siendo la consecución de la seguridad jurídica un estadio necesario para garantizar la propia legalidad en el disfrute de los derechos y libertades de la ciudadanía.

5. Recapitulación

I. Vivimos en una época de continua expansión tecnológica, donde la revolución digital ha producido un cambio sustancial en las pautas de comportamiento de la ciudadanía. En este

[170] Cfr. DIAZ. *Sociología y filosofía del derecho*, Taurus, Madrid, 1989, p. 42.

[171] Como sostienen MAYER-SCHÖNBERGER y CUKIER: "¿cómo se regula un algoritmo? En los albores de la computación, los legisladores advirtieron que la tecnología podía usarse para socavar la privacidad. Desde entonces, la sociedad ha erigido un conjunto de reglas para proteger la información personal. Sin embargo, en la era de los datos masivos, esas leyes constituyen una línea Maginot en buena medida inútil. La gente comparte gustosamente información online: es una característica central de los servicios en red, no una vulnerabilidad que haya que evitar". Cfr. *Big data. La revolución de los datos masivos*, ob. cit., pp. 29-30.

estado de cambio constante, la técnica no se detiene, y el conocimiento deviene vanguardia o anacronismo de forma acelerada. En lo que se ha denominado como "modernidad líquida", se produce un cambio radical en la cohabitación humana, en el condicionamiento social de las políticas de vida.

Conceptos como la velocidad del movimiento o el espacio han dado un giro radical hasta diluir sus fronteras, llegando incluso a desaparecer. Así por ejemplo, los avances tecnológicos han logrado una instantaneidad en la comunicación que ha supuesto la eliminación de la concepción del espacio como límite de las relaciones sociales, pues nuestros actos ya no se circunscriben al entorno más inmediato, sino que van más allá del espacio físico. Del mismo modo, la interacción de las personas en el ciberespacio es tan real como frecuente, por lo que éste ha pasado a convertirse en una prolongación de la sociedad física.

En este contexto, cada uno de los movimientos en la Red genera información que se digitaliza en código binario y se almacena masivamente para, con técnicas de lo más complejas, analizarlos y extraer nuevas referencias que en el futuro puedan aplicarse a la transformación del mundo real. En este sentido, ello supone un uso y tratamiento masivo de datos destinados a inferir, a partir de su análisis, nuevas percepciones o indicadores, los cuales tienen una dimensión valorativa o axiológica que puede servir como fundamento para la transformación de los mercados, organizaciones o entes, e incluso la propia forma de relacionarse entre el Estado y la ciudadanía.

II. Así las cosas, llamamos *Big data* al almacenamiento, tratamiento y transferencia de datos a gran escala a través de las tecnologías de Internet. En la globalización del siglo XXI, las innovaciones tecnológicas junto con el nuevo modelo económico y social, han hecho proliferar enormes cantidades de bases de datos relativos a realidades tangibles (datos físicos) o intangibles *a priori* pero convertidos mediante algoritmos en información digital. Entre los unos y los otros hay un número descomunal de datos de carácter personal. La relevancia de estos datos masivos no sólo afecta a cuestiones directa e indirectamente vinculadas a nuestra privacidad, sino que tiene una trascendencia que abarca la propia configuración del tejido social.

El *Big data* no sólo se trata de acumular datos, sino de interrelacionarlos entre sí para lograr aumentar exponencialmente la información a obtener y sacarle así un mayor partido. Este proceso ha sido denominado como *agregación*: conformar el perfil de una persona a través de la triangulación y organización de la información que se ha adquirido sobre ella, obteniendo así nuevos datos sobre un individuo. Este proceso, al alterar las expectativas de las personas, supone una amenaza para la privacidad, ya que el sujeto no ostenta control alguno sobre el conocimiento que está generando su información personal.

Mediante la filtración de los datos (*data mining*) llevada a cabo por software específicos que funcionan atendiendo a los parámetros que para una finalidad concreta decidan emplearse, una misma información se recicla y almacena en bancos de datos siguiendo diversos crietrios por lo que, unos mismos datos pueden clasificarse según distintos parámetros y, en consecuencia, pueden formar parte de infinidad de bases de datos. De acuerdo con esta técnica, cualquier fenómeno social puede terminar siendo *datificado*, lo que lleva a reconocer un segundo estadio en el proceso de filtración de datos, próximo a su correlación con el medio social. Se denomina *reality mining* a la técnica consistente en procesar datos masivos procedentes de dispositivos móviles para extraer inferencias y predicciones sobre el comportamiento humano. En este segundo estadio, los datos previamente obtenidos tienden a situarse en correlación con distintas variables de aplicación en el medio social, con la finalidad de desarrollar una serie de criterios o pautas para el estudio de determinados comportamientos o fenómenos de alcance sociológico.

III. Como en toda dinámica de transformación social, el *Big data* se caracteriza por una serie de prácticas políticas, sociales o culturales que definen el estado actual del conocimiento y su proyección en las pautas de comportamiento en el medio social. En este contexto, es indudable la importancia del cálculo algorítmico como presupuesto estructural sobre el que se sustenta gran parte del marco de referencia acontecido con el *Big data*. Sobre esta cuestión, la utilización del algoritmo ha sido defendida desde la neutralidad asignada al pensamiento científico, en tanto que se trata de un lenguaje codificado mediante el uso de las matemáticas,

pero ello no resulta impermable a la posición de preeminencia adoptada por la hegemonía del pensamiento neoliberal propio de las sociedades capitalistas.

En consecuencia, se discute la idoneidad de la utilización del algoritmo como tércnica de ordenación social en los términos actuales, considerando las dificultades con las que se ha encontrado el capitalismo, como forma político-estatal, para adaptarse a los presupuestos estructurales de la *posmodernidad*. Así lo evidenció, la vacuidad de las soluciones aportadas para responder a la crisis de 2008, con la consecuente repercusión en el ámbito de las Unión Europea.

IV. En este sentido, no puede considerarse el *Big data*, ni tampoco su desarrollo mediante el cálculo algorítmico, como una realidad social neutra pues, pese a su carácter científico-técnico, la forma de orientar esta evolución, por ejemplo respecto al valor monetario atribuido a los datos masivos, muestra una opción ideológica concreta. Esta posibilidad de desnaturalizar una posición ideológica no es más que una demostración de que todo proceso social se encuentra orientado por un marco de referencia ideológico.

Por mucho que los algoritmos puedan responder a razonamientos matemáticos fruto de una lógica científico-numérica, esto no obsta para que puedan tener determinados sesgos o limitaciones cuando traspasan el ámbito del *deber ser ideal* propio del pensamiento científico, para aplicarse en el *ser conflictivo* de los procesos sociales. Como se evidencia en la posibilidad de establecer variables relacionadas con el nivel económico o la procedencia social de los sujetos destinatarios del cálculo algorítmico, no pudiendo en consecuencia, negarse los riesgos discriminatorios que pueden derivarse así como el posible etiquetaje de la ciudadanía en función de su acceso a los recursos.

V. Se considera necesario impugnar aquéllas formas de pensamiento que, amparadas en la técnica o la neutralidad y excusándose en valores que se presentan como inmutables, suponen una limitación de la capacidad crítica. Es por ello que deviene imprescindible una discusión pública del modelo algorítmico que permita reformular aquellos aspectos que puedan limitar el libre desarrollo de la personalidad de los sujetos.

Especial examen requiere el ámbito de las ciencias jurídicas, no sólo por la propia dinámica de reforma del ordenamiento jurídico en base a las necesidades sociales, sino también debido a la aplicación práctica de las normas jurídicas por los órganos jurisdiccionales. En este sentido, si consideráramos como irrefutable cualquier predicción desarrollada de acuerdo con el cálculo algorítmico, existirían dudas acerca de la posibilidad de afirmar el libre albedrio como característica inherente del ser humano.

VI. El concepto *dataveillance* ha sido acuñado para hacer referencia al uso sistémico de los procedimientos de tratamiento y análisis de datos masivos, con la finalidad de investigar o monitorizar las dinámicas de actuación o interacción social. En este sentido, la referencia al concepto *dataveillance* supone la normalización de una nueva cultura de la vigilancia a partir de los parámetros del *Big data*.

Para describir este nuevo estado de cosas, se ha recurrido al concepto de *panóptico digital*. Éste es construido de acuerdo con el *panóptico* originalmente desarrollado por BENTHAM que diseñó un sistema aquitectónico y organizativo, aplicable a cualquier institución requerida de vigilancia, en base a una construcción circular, donde las personas supervisadas habitan celdas individuales dispuestas a lo largo de la circunferencia del edificio, mientras que los vigilantes ocupan un torreón de vigilancia ubicado en el centro. Ello permite al vigilante observar a todos los habitantes sin que éstos sepan si están efectivamente siendo vigilados, creándose así un estado o percepción de vigilancia permanente, incluso en los supuestos donde no haya nadie en la torre.

El concepto de *panóptico* fue revisitado por FOUCAULT, quien desarrolló una teoría crítica del control social basada en la formalización del castigo a partir de los conceptos de poder disciplinario y vigilancia jerarquizada. En su deconstrucción crítica del poder de vigilar y castigar, reconoce un modelo de vigilancia jerarquizada funcional, que no distingue entre control social formal e informal. Esto supone que los dispositivos de policía, prisión, judiciales, actúan de forma conjunta y complementaria con las instituciones clásicas de control social informal (familia, escuela, iglesia…), desarrollándose una nueva economía del castigo, basada en la distribución de este poder.

En este punto, FOUCAULT *refundamenta* el *panóptico* de BENTHAM, considerando que el propio medio social puede actuar como el diseño arquitectónico propuesto por este último, donde el poder disciplinario tiene un alcance funcional gracias a la vigilancia jerarquizada, entendiendo ésta como *control permanente,* haciéndose extensivo a las instancias propias del control social informal.

VII. Partiendo de estos presupuestos, el concepto de "panóptico digital" forma parte de lo que se ha denominado por HAN como *sociedad de la transparencia*, cuya noción de "transparencia" desborda el entendimiento habitual referido a la corrupción y la libertad de información, considerándola como un mecanismo coactivo que, paradójicamente, limita la libertad de pensamiento en el ámbito de una sociedad que, y aquí radica su calificación como *positiva*, desalienta la *negatividad* entendida como disenso con lo establecido. Esto es así porque la *sociedad positiva* basada en la transparencia exige una necesaria plenitud en su construcción, en tanto que todo debe ser observable, analizable y medible.

Desde esta *sociedad de la transparencia* se transita fácilmente a lo que se ha denominado *sociedad de la exposición* para describir la necesidad que sienten las personas por exponerse, no sólo inducidos por el fetichismo digital impuesto por las redes sociales, sino porque representa la única forma de existir, de proyectarse en el medio social. De este modo, cada sujeto es su propio objeto de publicidad, todo se mide en su valor de exposición.

En el contexto del *Big data* el concepto de *panóptico* desarrollado por BENTHAM y FOUCAULT se adapta a la nueva realidad fruto de la revolución digital para constituir una nueva cultura de la vigilancia. El cambio cualitativo más relevante del *panóptico digital* es que sobre la figura del supervisado no se aplica ningún tipo de poder coactivo, como si ocurría en los paradigmas anteriores, sino que son los propios vigilados quienes voluntariamente asumen dicho papel, convirtiéndose en actores y víctimas de un modelo de vigilancia *totalizador* que se extiende a todos los aspectos de la vida diaria.

Sobre estos presupuestos, deben construirse herramientas jurídicas que permitan garantizar un estándar mínimo de protección de la privacidad en este nuevo hábitat de

vigilancia donde los ciudadanos, obligados por las propias dinámicas sociales, se someten a la observación perpetua y forman parte del *panóptico digital*. El desarrollo del derecho al olvido responde a la necesidad imperante del Derecho de adaptarse al contexto expuesto, para garantizar con ello la seguridad jurídica y la protección de los derechos y libertades de la ciudadanía.

VIII. El tratamiento ofrecido por el sistema penal español al delito de enaltecimiento del terrorismo en las redes sociales ejemplifica cómo funciona el *panóptico digital* en la práctica, como medio de vigilancia permanente. La interpretación realizada por los órganos jurisdiccionales en estos casos parece seguir una línea político-criminal dirigida, más que al tratamiento preventivo-penal de la actividad terrorista, a la criminalización de determinadas opciones políticas o ideológicas que nada tienen que ver de forma directa con la actividad terrorista. En este sentido, la expresión de este tipo de comentarios en las redes sociales, pese a que constituyan opiniones desafortunadas y rechazables, no justifican el recurso al Derecho penal.

La aplicación extensiva del delito de enaltecimiento a muchos de los comentarios vertidos en las redes sociales que, en la mayoría de casos, constituyen muestras de humor macabro o una posición de disenso respecto del pensamiento político dominante, pueden suponer una limitación de las libertades expresivas inasumible por un Estado democrático y de Derecho.

IX. No puede reconocerse el *Big data*, ni tampoco el proceso técnico seguido para el análisis y tratamiento de datos masivos como un fenómeno neutral o meramente científico. En este sentido, se han desarrollado los argumentos para rebatir este carácter supuestamente apriorístico relativo al empleo de algoritmos para desarrollar la utilización de los datos masivos. Sobre esta cuestión se ha razonado que, si bien los algoritmos responden a una lógica científica-matemática, es indudable que la forma en que éstos sean proyectados al estudio de los procesos sociales responderá a unas determinadas coordenadas sesgadas en función de razonamientos de tipo político, económico o social. En consecuencia, existe el riesgo de que pueda producirse un proceso de etiquetaje respecto de determinados colectivos, que pueden

resultar discriminatorias para los grupos afectados así como excluyentes para aquellas personas que, debido a causas diversas (pobreza, geografía, estilo de vida…), no son *datificadas*, pudiendo dar lugar a la creación de una *sociedad de clases digital,* distorsionando a favor de las mayorías integradas en el sistema económico y social la orientación de la lógica algorítmica que orienta el tratamiento y análisis de los datos masivos.

X. En la actualidad, puede hablarse de una expropiación de la privacidad sin precedentes. Los datos personales se han convertido en un activo patrimonial de gran valor económico en el Mercado, el petróleo del siglo presente, ellos orientan el desarrollo y uso de nuevos productos y servicios. La obtención de información personal cuenta con dos grandes aliados, de una parte las nuevas herramientas tecnológicas y, de otra, la fragmentación legislativa o incluso la desregulación, lo que da rienda suelta al mercadeo de datos personales sin demasiados problemas.

Estos dos factores han convertido a la privacidad en el producto estrella a comercializar por las grandes corporaciones del *Big data*. El negocio resulta muy rentable pues son los usuarios quienes ceden gratuitamente sus datos personales a empresas que se dedican a almacenarlos, venderlos a terceros o procesarlos para un tratamiento posterior, generalmente con objetivos de marketing. Sobre esta cuestión, el uso o la instalación de la mayoría de servicios y aplicaciones informáticas aparentemente gratuitas suponen auténticos contratos de adhesión que contienen, en su mayoría, un número considerable de cláusulas abusivas, mediante los cuales, los usuarios ceden sus datos personales en contraprestación por los servicios recibidos, que más tarde se monetizan por dichas empresas.

Así, los usuarios de dichos servicios han dejado de ser simples consumidores pasivos pues, a través de una pérdida considerable de su privacidad, se han convertido en parte del producto cuya ganancia, sin embargo, no perciben. Parece pues, que se ha evolucionado de un Internet de las cosas a un Internet de las corporaciones, donde las cosas son los usuarios y en el que los datos personales se han convertido en el producto a comercializar.

XI. El *Big data* de una empresa puede convertirse en su activo más valioso y juega un papel muy importante en la toma de decisiones de mercado. En este escenario, los *data brokers* aprovechan la coyuntura para lucrarse con la venta de los datos personales de los usuarios, llevando a cabo un filtrado de datos, esto es, desglosándolos y cruzándolos entre ellos, hasta crear catálogos con los perfiles o patrones de comportamiento deseados, para ser vendidos posteriormente a otras empresas que los usarán para su propio beneficio, principalmente para el marketing personalizado.

La *datificación,* como práctica de explotación de datos masivos, no se limita al aislamiento de patrones sobre las actitudes o estados de ánimo, sino que abarca de forma amplia el comportamiento humano. De este modo, los *data brokers* pueden terminar facilitando a los terceros interesados una muestra del comportamiento humano en un contexto concreto del medio social, obteniendo como se ha expuesto un valor económico por ello.

XII. La intimidad se circunscribe al ámbito más personal del individuo, al reducto de cada ser humano libre de toda injerencia externa y en que se fraguan las decisiones más propias e intransferibles, desarrollándose la propia personalidad en toda su extensión. Ésta, forma parte de la esencia misma de la personalidad y, por ende, es inherente a todos los seres humanos, constituyéndose como una suerte de "derecho de secreto" sobre lo que somos, pensamos o hacemos.

En la privacidad, por su parte, aunque también integra un ámbito de protección del individuo libre de injerencias externas, dicha esfera de protección es mucho mayor en tanto que supera el perímetro circunscrito de lo estrictamente íntimo para abarcar otras conductas y facetas cotidianas y personales sujetas al control de la soberanía individual. A diferencia de la intimidad, el ámbito de protección de la privacidad es flexible y está sujeta a cambios, por lo que depende de cada persona, del contexto, de las pautas de comportamiento de un lugar, de las costumbres o de las necesidades sociales.

Podría decirse que, mientras que el derecho a la intimidad se relaciona con el poder que cada individuo tiene para controlar la injerencia externa en su esfera más íntima, el derecho a la

privacidad permite controlar el acceso, el alcance y la difusión de los demás a ese dominio íntimo. Igualmente, mientras que la intimidad es necesaria para salvaguardar la autonomía personal y el libre desarrollo de la personalidad, la privacidad abarca una dimensión mayor en el contexto de las relaciones interpersonales, proporcionando un espacio libre para llevar a cabo una multiplicidad de actos entre los que se incluye el intercambio de información personal. De este modo, intimidad y privacidad son realidades distintas aunque relacionadas y tienen un objetivo común: la ausencia de difusión -resguardarse de la publicidad no deseada-, reservando al individuo una parcela libre de injerencia.

En consecuencia, se defiende la adopción del término "privacidad" como el más idóneo para describir la realidad presente, en la que el *Big data* en concurrencia con la revolución informática y tecnológica, ocasionan riesgos y lesiones para ciertos ámbitos personales de los individuos que, sin penetrar necesariamente en su estricta intimidad, calan en su ámbito más privado, suscitando igualmente molestias y perjuicios. De acuerdo con lo expuesto, entendemos la privacidad como aquella esfera personal integrada por informaciones y comportamientos que, pese a no ser íntimos, el individuo desea que sólo sean conocidos por él o por determinadas personas con las que voluntariamente quiera compartirlos, sustrayendo su conocimiento a núcleos más amplios de la sociedad. Se pretende así adoptar una postura más garantista de la esfera privada de las personas, ciertamente necesaria tiendo en cuenta las circunstancias concurrentes.

XIII. La sociedad avanzada requiere repensar los términos y los medios de protección de las esfera privada de sus ciudadanos, como consecuencia lógica del desarrollo garantista de la intimidad personal frente a los desafíos que la nueva coyuntura ofrece para los bienes jurídicos. Las nuevas facetas de la vida privada requieren nuevos medios de tutela jurídica que deben ampliar su rango de protección en tanto que la esfera privada ha sido exponencialmente puesta en riesgo. En este sentido, las intromisiones en la privacidad de las personas, cada vez más frecuentes gracias a la intermediación de los fenómenos anteriores, no pueden quedar impunes por no cumplirse todos los requisitos que para la protección de la intimidad se

requieren, el ordenamiento debe dar respuesta a dichas conductas que lesionan otros derechos fundamentales y suponen conductas discriminatorias.

Así, en el contexto del *Big data*, hablamos de privacidad para referirnos a la esfera de libertad que todo ser humano tiene respecto de sus datos de carácter personal, información que, si bien no en todas las ocasiones puede lesionar su intimidad, afecta a otra esfera menos restringida pero igualmente protegida por el Derecho. En consecuencia, debe abandonarse la concepción tradicional de la vida privada como un *status* negativo pues la protección de la privacidad, sin duda es un derecho activo de control, de autodeterminación, que permite a cada individuo controlar el ámbito de privacidad deseado, concediéndole asimismo herramientas efectivas para reaccionar frente a cualquier vulneración.

Se reconoce así la pluralidad de manifestaciones que tiene la esfera privada, concediendo a todas ellas protección jurídica, partiendo de las circunstancias sociales, culturales e históricas que aconsejan ampliar el concepto y la garantía de lo privado desde la "intimidad" hacia la "privacidad", desde una concepción unitaria y global.

En consecuencia, a lo largo de la tesis doctoral se emplea el término "privacidad", de forma consciente y en contraposición al concepto de intimidad, en base a la distinción llevada a cabo en páginas anteriores y con la intención de mantener una coherencia argumental en todo el trabajo.

XIV. La modernidad líquida y la mutabilidad que conlleva originan en la sociedad la sensación permanente de volatilidad, lo que indudablemente supone cierta inseguridad jurídica. Esta nueva realidad incita a repensar y reconfigurar conceptos que indudablemente han adquirido un nuevo significado, como "intimidad" o "vida privada". De igual modo, una vez ha quedado acreditada la transformación experimentada por la privacidad en el ámbito del *Big data*, deviene necesario desarrollar una propuesta doctrinal coherente capaz de armonizar la protección de los derechos y libertades de la ciudadanía en este nuevo estado de cosas.

Los derechos fundamentales no responden a estructuras lógico-objetivas o valores inmutables, sino que son objeto de un desarrollo histórico diferenciado, atendiendo a las

dinámicas de transformación de toda sociedad. En este sentido, los derechos fundamentales emergen como respuesta a una conflictividad, para así garantizar en última instancia el respeto a la dignidad de la persona y a su capacidad para desarrollarse conforme al principio general de libertad, de acuerdo con los presupuestos estructurales de un Estado social y democrático de Derecho.

Partiendo de la teoría jurídica del *garantismo* propuesta por FERRAJOLI, en relación con la defensa de la subordinación de la legitimidad del ordenamiento jurídico al aseguramiento de las condiciones efectivas de disfrute de los derechos fundamentales, se concibe en este trabajo una respuesta al conflicto que plantea el *Big data* para el libre desarrollo de la personalidad y la privacidad de los sujetos, desde el punto de vista de los derechos subjetivos, que permita a los ciudadanos disfrutar de los avances tecnológicos sin renunciar a la protección de sus derechos y libertades.

En este sentido, se construye un modelo garantista de derecho al olvido como derecho fundamental idóneo para paliar las exigencias derivadas del espacio de previsibilidad objetiva que el Estado debe ofrecer a la ciudadanía para aportar un espacio de seguridad a la propia regularidad estructural del ordenamiento jurídico, necesitado de respuestas ante el desafío del *Big data* en relación con la protección de la privacidad de ciudadanía. Por lo tanto, su aplicación en el medio social vendría a subsanar la falta de seguridad jurídica producida por la lenta respuesta del ordenamiento jurídico a uno de los más importantes cambios estructurales fruto del contexto de la *posmodernidad*, siendo la consecución de la seguridad jurídica un estadio necesario para garantizar la propia legalidad en el disfrute de los derechos y libertades de las personas.

CAPÍTULO II. EL CONCEPTO DE PRIVACIDAD EN EL ÁMBITO JURÍDICO DEL *COMMON LAW*: DESARROLLO DEL *RIGHT TO PRIVACY* EN REINO UNIDO

1. Notas preliminares

1.1 *Right to privacy* como estándar y garantía de la esfera personal del sujeto: una aproximación desde el Derecho comparado a partir de la refundamentación de la privacidad

En este capítulo será estudiado el tratamiento en el Reino Unido de la protección de los datos personales, como parte de la garantía jurídica de la intimidad y la vida privada. Para ello, además de presentar, desde una perspectiva amplia, el orden de un sistema jurídico de la cultura legal anglosajona, serán consideradas una serie de cuestiones inherentes al desarrollo diferenciado de la salvaguarda de la esfera personal del sujeto en el ordenamiento jurídico británico.

Sobre esta cuestión, puede partirse de una serie de aspectos que acreditan la pertinencia de ofrecer una exposición sobre la protección legal de la privacidad en el orden jurídico británico, como representante del sistema legal del *common law*, principalmente, la propia importancia del Derecho comparado, especialmente en lo relativo a la cultura legal anglosajona. Esto es así porque, desde la perspectiva de la doctrina española, de raigambre continental, se ha tendido de forma generalizada a dirigir la mirada *iuscomparativa* al estudio de sistemas legales propios de nuestra propia tradición jurídica, como Alemania o Italia, desatendiendo realidades jurídicas igualmente próximas como acontece con el Reino Unido, teniendo en cuenta además, que la permeabilidad entre las distintas culturas legales es una cuestión transversal al estudio científico del Derecho, más si cabe en una realidad tan fuertemente sometida a las tensiones derivadas de la *posmodernidad* como lo es la privacidad y la protección de datos en el contexto del *Big data.* En este sentido, si bien esta investigación tiene como punto de partida un ordenamiento jurídico propio de la cultura legal continental, como lo es el español, la necesidad de profundizar desde una perspectiva *iuscomparativa* en el

estudio de la protección de datos permite ampliar el ámbito del objeto de estudio[172], resultando aquí de interés el ordenamiento jurídico británico como representante de lo que se ha conocido como cultura legal anglosajona o *common law*[173].

Dado que la investigación propuesta en este trabajo pretende circunscribirse al contexto europeo, como se pone de manifiesto en el estudio de la normativa comunitaria[174], se ha considerado coherente con la voluntad integradora de esta disertación, dedicar un capítulo a la protección de la privacidad en el Reino Unido. De este modo, no sólo se amplia la proyección comparativa del estudio, enriqueciendo el mismo, sino que permite además conocer una realidad jurídica en ocasiones ignorada por la doctrina continental. En este sentido, serán considerados los rasgos inherentes del sistema de fuentes propio de un ordenamiento jurídico del *common law*, especialmente teniendo en cuenta el desarrollo pionero de la legislación británica en materia de protección de datos personales, mediante las *Data Protection Act 1984* y *Data Protection Act 1998*, así como la promulgación por Reino Unido de la *Human Rights Act 1998*, que incorpora y positiviza el Convenio Europeo de Derechos Humanos en el ordenamiento jurídico británico.

De acuerdo con lo expuesto, una primera razón para el análisis del marco legal y doctrinal sobre la cuestión objeto de estudio en el Reino Unido, responde a la importancia de ampliar el enfoque *iuscomparativo* de esta investigación. No obstante, la elección del sistema jurídico británico se justifica teniendo en cuenta los presupuestos estructurales de este trabajo expuestos en el Capítulo anterior[175]. En éste, además de describir la incidencia multidisciplinar

---

[172] De acuerdo con ESER, debe reconocerse la importancia del Derecho comparado desde una perspectiva académica, considerando así su valor para permitir el avance de una disciplina jurídica concreta. Cfr. "The importance of comparative legal research for the development of criminal sciences", en *Law in Motion: recent developments in Civil procedure, Contract, Criminal, Environmental, Family & Successions, Intellectual Property, Labour, Medical, Social Security and Transport Law*", Kluwer Law International, 1997, p. 498.

[173] Hacer referencia al *common law*, cultura legal anglosajona o tradición jurídica anglosajona puede incurrir en una posible generalización, en tanto que dentro de este ámbito jurídico-cultura se entienden incluidos desarrollos diferenciadores por los distintos Estados que la integran, siendo distinta la evolución en el caso británico, norteamericano, australiano, sudafricano, etc. De acuerdo con GEERTZ, no admitir este reconocimiento podría llevar a un reduccionismo que dificultaría el estudio de sus rasgos inherentes. Cfr. "Fact and law in comparative perspective", en *Local knowledge: further essays in interpretative anthropology*, New York, Basic Books, 2000, p. 167 ss.

[174] Vid. *infra* Cap. III. 3.

[175] Vid. *supra* Cap. I. 4.

del *Big data* como presupuesto ideológico o político sobre el que se descansa este estudio, se ha descrito el marco metodológico al que se adscribe la presente disertación para desarrollar el derecho al olvido como derecho fundamental. Sobre esta cuestión, se ha partido de la comprensión dialéctica de los conceptos de intimidad y privacidad, con la finalidad de *refundamentar* el debate a partir de una construcción de la esfera personal de privacidad del sujeto que integre ambos conceptos, permitiendo así la creación de un estándar garantista que responda a las demandas de legalidad y seguridad jurídica propias de la *posmodernidad*, especialmente desde los riesgos que para éstas supone el *Big data*.

Así las cosas, la toma de postura expuesta en páginas anteriores, supone un reconocimiento de la esfera personal del sujeto ligada a un modelo de garantismo que permita el libre desarrollo de la personalidad de los sujetos, siendo decisiva la importancia conferida a la protección jurídica de la privacidad como condición material previa para asegurar la libertad del sujeto. Asumiendo el concepto de privacidad ofrecido como presupuesto estructural de este trabajo, se ha reconocido la relación de semejanza que presenta éste con el *right to privacy* propio del ámbito jurídico del *common law*.

Por esta razón, y pese a que se ha considerado nuestro marco constitucional de referencia como el más pertinente para la construcción del derecho al olvido, se ha estimado conveniente conocer el desarrollo del *right to privacy* en la cultura legal anglosajona, concretamente en el Reino Unido, por ser parte del Convenio Europeo de Derechos Humanos propio del Consejo de Europea, en tanto que en su articulado (art. 8) queda reconocida la protección de la intimidad y la vida privada. A partir de su estudio, se pretende reconocer el desarrollo doctrinal y jurisprudencial del concepto, además de la elaboración de los marcos legales pertinentes en el Reino Unido para su protección. De este modo, se considera que puede dotarse a este trabajo, además de la proyección *iuscomparativa* previamente mencionada, de las referencias necesarias para estudiar la protección de la esfera personal del sujeto desde una perspectiva amplia, consecuente con los presupuestos estructurales de este estudio. A partir de éstos, será posible desarrollar con garantías la construcción del derecho al olvido como derecho fundamental.

1.2 Marco de referencia del ordenamiento jurídico británico como integrante de la cultura legal anglosajona

La privacidad en el Reino Unido es un caso de estudio realmente interesante por diversas razones. En primer lugar, porque Reino Unido aúna en un mismo sistema legal dos corrientes aparentemente contrapuestas, esto es, de un lado su tradición jurídica del *common law* [176] íntimamente ligado al precedente judicial -de modo que, sin constar ciertos derechos expresamente escritos desde un inicio, éstos se convierten en ejercitables una vez así se determine por los tribunales a través del *case law*-, y de otro, el positivismo jurídico creciente, adoptando el principio de soberanía nacional mediante el cual se legitima al Parlamento para legislar en cualquier ámbito del Derecho – así, cuando una ley es promulgada por el Parlamento británico, los tribunales la aplicarán independientemente de su contenido o el parecer de los jueces-. La reciente incursión de la doctrina de la soberanía parlamentaria, se enmarca en el contexto del acceso de Reino Unido al Espacio Económico Europeo el 1 de enero de 1973, que impulsó la evolución de su sistema legal, principalmente por la necesidad de incorporar la normativa europea a la legislación y los tribunales domésticos que, a partir de entonces, se comprometen a interpretar el derecho anglosajón de conformidad con el europeo. Este proceso comporta una progresiva positivización del sistema anglosajón con la finalidad de armonizar el derecho como consecuencia de la integración europea, cuyo exponente máximo de este proceder se consuma con la aprobación de la *Human Rights Act* el 9 de noviembre de 1998.

En segundo lugar, este particular fenómeno se une al hecho de que Reino Unido no cuenta con una constitución escrita, lo que no impide tener una constitución no codificada, esto es: un intrincado de leyes, sentencias judiciales y tratados internacionales cuyo valor se equipara al de una constitución material. Las concretas circunstancias del sistema constitucional anglosajón, le dotan de una capacidad de aclimatación francamente asombrosa,

[176] Conviene señalar desde el principio, que a lo largo de este Capítulo se hace mención al *common law* anglosajón en un sentido general, esto es, reduciendo su aplicabilidad a Inglaterra, Gales e Irlanda del Norte. El sistema legal y parlamentario británico es de una gran complejidad, dada la estructura multinivel y las relaciones competenciales territoriales, lo que ocasiona que Escocia goce de un status particular en la gran mayoría de los aspectos que se tratan en este trabajo, cuya pormenorización se omite al considerar que ello incrementaría innecesariamente la extensión y haría engorrosa su lectura.

adaptando sus reglas y principios a las estructuras de poder y a los convencionalismos sociales vigentes, así como a las necesidades económicas, los patrones culturales u otras circunstancias determinantes en cada momento histórico.

El sistema de fuentes anglosajón, descrito muy someramente, es eminentemente jurisprudencial, fundamentado en origen en la costumbre (*common law*) y en el precedente legal (*case law*). Éste ha ido paulatinamente codificándose, principalmente mediante la promulgación de leyes y otras normas reglamentarias (*statutory law*) que complementan y actualizan las primeras[177], así como incorporan a la legislación doméstica las exigencias derivadas de la integración europea. En todo este intrincado normativo, destaca la centralidad del concepto *rule of law*[178] como clave de bóveda del ordenamiento constitucional británico, en tanto que a partir de éste terminan desarrollándose una serie de principios específicos, de alcance político-constitucional, como criterio orientador para garantizar los derechos y libertades propios de un sistema donde se reconoce en las disposiciones normativas de origen parlamentario, en la fuerza vinculante otorgada al *common law* y el respeto a los tratados internacionales lo que se ha venido a llamar como *unwritten constitution*[179].

La volatilidad del sistema de valores anglosajón queda patente en la configuración de los derechos y libertades ciudadanas así como en su sistema de garantía, lo cual también se plasma en la evolución del modelo británico de protección de la privacidad, a cuyo examen se procederá en el presente Capítulo. Se pueden distinguir tres etapas importantes en este sentido: un primer estadio, marcado por la promulgación de la *Data Protection Act 1984* (cuyo contenido se amplió mediante la *Data Protection Act 1998*, que incorporaba las exigencias

[177] Éstas tienen distinta denominación según el órgano que las dicta: *Act of Parliament* (leyes parlamentarias), *Ministerial orders* (órdenes ministeriales), *Local by-laws* (ordenanzas municipales), *Statute* (normas reglamentarias)…

[178] El concepto *rule of law* es de una complejidad enorme, pues es un concepto "vago en lo que respecta a su contenido y promiscuo" en lo relativo a las funciones a desarrollar en un sistema constitucional que tiene la peculiaridad de no tener una norma constitucional. Cfr. RAZ, J. "The rule of law and its virtue" en *The authority of law. Essays on law and morality*, Oxford Clarendon Press, Oxford, 1979, p. 211. Por lo que respecta a la vaguedad, pueden recogerse las palabras de BINGHAM, cuando señala cómo, pese a ser una noción frecuentemente utilizada por los juristas en distintas instancias, sería difícil ofrecer por parte de éstos una definición clara de su significado. Cfr. *The rule of law*, Penguin Group, London, 2011, vii.

[179] Serán estas instituciones, siguiendo el contenido de la *rule of law* como criterio orientador, las que determinen el respeto a los derechos y libertades públicas.

europeas de la Directiva 95/46/CE claramente influenciada por la normativa británica, pionera en la defensa de la información personal) que reconoce un derecho a la protección de datos -como algo intrínsecamente ligado a la identidad y a la privacidad- e introduce un sistema adecuado para su garantía, proporcionando herramientas jurídicas a los tribunales que, hasta el momento, sólo concedían exigua protección a la privacidad a través de algunas figuras tradicionales del *common law* como la *breach of confidence*, la *defamation* o la *nuisance*.

La segunda fase de este eje histórico se consagró con la aprobación de la *Human Rights Act 1998*, mediante la cual se incorporaron a la legislación británica los derechos y libertades garantizadas por el Convenio Europeo de Derechos Humanos de 1950 que ahora resultan directamente aplicables, así como la jurisprudencia del Tribunal Europeo de Derechos Humanos interpretando dichos preceptos, dejando éste de ser un órgano de segunda instancia. La aprobación de dicha norma, supuso el hito jurídico más relevante para el Reino Unido desde la aprobación del Tratado de Roma, evidenciando un cambio social, cultural e ideológico de la sociedad británica que apostó por un desarrollo de la sociedad basado en los derechos humanos y cuyo impacto jurídico se aprecia no solo en el derecho público y penal, sino también en el *common law*.

El artículo 8 del Convenio Europeo de Derechos Humanos así como de la *Human Rights Act 1998*, reconocen el derecho a la vida privada, lo que supuso un punto de inflexión para su protección, cuya ejecución principalmente se ha llevado a cabo adaptando las causas tradicionales de acción existentes en el *common law* que ahora amplían su contenido pues, como se verá más adelante, pese a todo, el derecho anglosajón no reconoce explícitamente el derecho a la privacidad al no prever ninguna "*tort law*" ni ninguna "*civil wrong*" en relación a ésta.

La tercera y última de las fases que ha incidido en la cuestión de estudio viene integrada por múltiples acontecimientos y, de hecho, su futuro está aún por determinar. Puede destacarse aquí, por un lado, como, con el paso de los años, se ha producido una disminución del alto estándar de protección del que gozaba la privacidad en el Reino Unido –unido quizás a la deriva neoliberal de las políticas del Gobierno británico de los últimos quince años- que se ha

proyectado en leyes como la *Anti-Terrorism Crime and Security Act 2001* o la *Data Retention Regulation and Investigatory Powers Act 2014* que, bajo la excusa de la amenaza terrorista o el control de los mercados financieros, permiten de facto la vigilancia masiva de los ciudadanos y que claramente abogan por la limitación del espacio privado de las personas, lo que le ha supuesto a Reino Unido más de una reprimenda por parte del Tribunal de Estrasburgo.

Por otro lado, el creciente euroescepticismo británico que se consagró el 23 de junio de 2016 con el referéndum celebrado y que dio como resultado la victoria al *Brexit* y, en consecuencia, conlleva la salida de Gran Bretaña de las instituciones comunitarias en un futuro próximo. Fruto de esta decisión, y entre otros muchos efectos, el gobierno británico aboga por la salido de Reino Unido del Convenio Europeo de Derechos Humanos que dejará de someterse a la jurisprudencia del Tribunal Europeo de Derechos Humanos, deshaciéndose del espíritu y el camino recorrido hasta ahora por la *Human Rights Act 1998*.

Entre tanto, y dentro de este contexto, ha entrado en vigor el Reglamento General de Protección de Datos 2016/679 (publicado dos meses antes de dicho referéndum), directamente aplicable en Reino Unido y que, hasta el momento en que se produzca la desconexión total con la Unión Europea, supone la obligación de adaptar la legislación británica al nuevo articulado europeo (como parece se está haciendo mediante la *Data Protection Bill*, en tramitación parlamentaria en el momento de redacción de estas líneas), determinando en un futuro inmediato la naturaleza de las relaciones que tendrán lugar entre la Unión Europea y el Reino Unido, que podría pasar a considerarse un tercer estado a efectos de la normativa europea de protección de datos.

Por todo ello, en el presente Capítulo procura presentarse la panorámica actual del sistema de protección de la privacidad en el Reino Unido, haciendo hincapié en aquéllas etapas que, de un modo u otro, han supuesto un punto de inflexión en la materia, integrando y comentando la jurisprudencia más relevante al respecto (como el caso *Campbell*[180], dónde se estipula la vulneración de la privacidad personal con la publicación relativa al sometimiento a

[180] *Campbell v. Mirror Group Newspapers Ldt*, de 27 de marzo de 2002 [2002] EWHC 499, Court Queen's Bench Division.

un tratamiento de rehabilitación, por sus conexiones con la dignidad y el desarrollo de la propia personalidad; el caso *Douglas*[181], en el que los tribunales se pronunciaron sobre el derecho a la explotación de la propia imagen como potestad inherente al derecho de privacidad; o el caso *Peck*[182] donde se estimó que la difusión de las grabaciones de las cámaras de seguridad de un intento de suicidio vulneraban la privacidad), y aventurándose a extraer posibles soluciones de futuro frente a los retos inmediatos, como consecuencia de los acontecimientos políticos más recientes.

2. Desarrollo evolutivo de la protección de la privacidad en el Reino Unido

2.1. Consideraciones preliminares

Se ha convenido en situar la creación del derecho a la privacidad en el *common law*, en el artículo que en 1890 escribieron WARREN y BRANDEIS en el *Harvard Law Review* titulado "The right to privacy"[183]. A raíz de la aparición de las cámaras instantáneas, se intensificó la actividad de la prensa amarillista y en consecuencia, la exposición pública, lo que dio lugar a que estos abogados bostonianos construyesen el derecho a la privacidad –al que llamaron "*right to be let alone*"- sobre los presupuestos jurídicos del *common law*, al que exigían un reconocimiento expreso y específico de la "*privacy*" -que, según defendían, ya se protegía bajo diferentes formas y denominaciones-[184], como respuesta a la nueva realidad tecnológica, política, social y económica

Así, WARREN y BRANDEIS identificaron un derecho a la privacidad, implícito en el derecho anglo-americano del *common law* que ofrecía a los ciudadanos plena protección en su persona y en su propiedad, reexaminando el concepto de "*privacy*" en base a las posibilidades

[181] *Michael Douglas & Catherine Zeta-Jones v. Hello! Ldt*, de 7 de noviembre de 2003 [2003] EWHC 2629 (Ch), Court Chancery Division.

[182] *Peck v. United Kingdom*, de 28 de enero de 2003, (App. 44647(98), [2003] ECHR 44, (2003) 36 EHRR 41, [2003] 36 EHRR 719.

[183] WARREN/BRANDEIS. "The Right to Privacy", *Harvard Law Review*, vol. IV, nº 5, 1890.

[184] Entendían los autores que hasta el momento, las figuras jurídicas prevista por el *common law* (*defamation, breach of confidence, nuisance*…) eran soluciones parciales que se basaban en un mismo principio con derecho a un reconocimiento específico y una sustancialidad propia: el derecho a la privacidad. Y recuerdan el carácter evolutivo del *common law*, y su eterna juventud ("*eternal youth*") que le otorga capacidad de crecer para satisfacer las demandas cambiantes de la sociedad, que el derecho debe actualizar.

que el *common law* les ofrecía en relación a otros derechos, asumiendo que los cambios del momento, debían de comportar asimismo, un cambio en la legalidad existente.

En base al derecho de propiedad, crearon una doctrina capaz de dar respuestas jurídicas a la sociedad del momento, empoderando a los ciudadanos con derechos ejercibles, como el famoso "*right to be let alone*" que, como defendían sus autores, partía de un derecho más general a la inmunidad personal, en sus propias palabras "*the right's to one's personality*".

Y lo hicieron siendo fieles al pasado legal e histórico con el que contaban, sin romper radicalmente con la legislación del momento, sino evolucionándola para ponerla de actualidad[185]. Estos dos abogados son el ejemplo de la interpretación extensiva del Derecho con la que revolucionaron la forma de entender la privacidad a finales del siglo XIX, adaptando cuidadosamente el *common law* a su más inmediata actualidad, creando las bases de lo que hoy la doctrina asume como indiscutible. Esta es la primera fase de gestación de un nuevo derecho, cuya evolución tomó caminos divergentes en la jurisdicción americana e inglesa de la tradición jurídica del *common law*. Sobre esta cuestión, si bien no se entrará en el estudio del desarrollo evolutivo de la jurisdicción americana[186], puede mencionarse la existencia de dos elementos diferenciadores entre ambas jurisdicciones.

Por un lado, la naturaleza de las constituciones existentes a ambas partes del atlántico: mientras que Estados Unidos cuenta con una Constitución rígida y escrita en la que se reconoce explícitamente algunas de las facetas del derecho a la privacidad, la Constitución de Reino Unido no está codificada y como se ha explicado anteriormente, su naturaleza intrínseca permite la volatilidad de su contenido en función de la modificación de las reglas y principios que, sobre el ejercicio del poder por parte del Estado, la forma de organización política y los derechos de los ciudadanos británicos, estén vigentes en cada momento[187].

---

[185] La evolución del Derecho, no tiene porqué encontrar límites en tanto que el comportamiento humano está en permanente evolución, es una cuestión de voluntad política y demanda ciudadana.

[186] Respecto del estudio de la privacidad en el ordenamiento jurídico norteamericano, véase, PROSSER/KEETON. *On the Law Of Torts*, West, St. Paul, 1984.

[187] Este fenómeno viene aparejado al desarrollo del concepto *rule of law* por la doctrina anglosajona, caracterizado por la dicotomía entre la perspectiva formal y sustantiva de su significado. En cuanto a la primera, la importancia de la *rule of law*

Ahora bien, como más tarde se evidenciará, la existencia de un marco constitucional para el derecho a la privacidad no es directamente proporcional a su garantía efectiva, pues el modelo constitucional se articula con otros muchos factores que inciden en el estándar de protección.

En segundo lugar, e íntimamente relacionado con lo anterior, sucede que, mientras que en Estados Unidos existe un marco sustantivo para el reconocimiento del derecho a la vida privada -ampliamente definido por la doctrina y la jurisprudencia[188]-, en Reino Unido no existe un reconocimiento legal ni tampoco un consenso doctrinal ni jurisprudencial acerca del concepto de privacidad[189].

Conviene tener en cuenta ambos elementos ya que, frecuentemente, se cae en el error de pensar que el Derecho americano y británico son equivalentes al compartir un origen único, pero lo cierto es que sus ordenamientos jurídicos han evolucionado hasta conseguir sustantividad propia, pese a compartir elementos comunes pertenecientes al sistema del *common law*.

---

radica en el procedimiento formal de aprobación de las normas jurídicas que regulan el ejercicio de un derecho o libertad, siendo éstas coherentes cuando respetan el procedimiento previsto para su aprobación y promulgación. Cfr. DICEY. *Introductory to the study of the law of the constitution* (The Oxford Edition of Dicey), Oxford University Press, Oxford, 2013; RAZ. "The rule of law and its virtue", en *The authority of law. Essays on law and morality*, Oxford Clarendon Press, Oxford, 1979; Críticamente, UNGER. *Law in modern society: towards a criticism of social theory*, Free Press, New York, 1976. En cambio, desde la perspectiva sustantiva, se exigen además, unos atributos materiales para garantizar que la norma sea respetuosa con los derechos y libertades que pudieran entrar en contradicción con su regulación desde una perspectiva estrictamente formal. Cfr. ALLAN. *The sovereignty of law*, Oxford University Press, Oxford, 2013; *Constitutional Justice, A liberal theory of the rule of law*, Oxford University Press, Oxford, 2011. Así las cosas, la perspectiva sustantiva se muestra crítica con la visión excesivamente procedimental de la vertiente formal, en tanto que parece reducir el concepto *rule of law* a categoría ontológica. Cfr. DWORKIN. *A matter of principle*, Hardvard University Press, Cambridge, 1985, p. 11. En cambio, los defensores del formalismo consideran que los postulados que defienden una interpretación sustantiva del concepto pueden llevar a relativizar su significado, el cual puede verse disperso en el amplio abanico de intereses cambiantes que pueden esgrimirse para desarrollar un entendimiento del concepto desde la perspectiva sustantiva, a partir de la remisión a ciertas referencias teleológicas o epistemológicas en la orientación del concepto rule of law. Cfr. CRAIG. "Formal and substantive conceptions of the rule of law: an analytical framework", *Public Law*, Sweet and Maxwell, London, 1997, p. 469. Puede así reconocerse una primera concepción más próxima al positivismo jurídico, mientras que la perspectiva sustantiva presenta una mayor incidencia en la dimensión discursiva y argumentativa de las normas jurídicas.

[188] Cfr. PROSSER/KEETON. *On the Law Of Torts*, ob. cit.

[189] Cfr. MARKESINIS/O'CINNEIDE/FEDTKE/HUNTER-HENIN. "Concerns and ideas about the developing English Law of Privacy (And How Knowledge of Foreign Law Might Be of Help)", en *American Journal of Comparative Law*, nº 52, 2004.

El factor principal que ha incidido sustancialmente en la evolución del modelo jurídico británico ha sido la entrada del Reino Unido en la Unión Europea, que ha supuesto un compromiso armonizador -de los derechos y libertades de los europeos así como de los instrumentos para su protección y garantía-, entre todos los Estados miembros, la mayoría de los cuales pertenecen a la tradición jurídica continental. Si bien la integración europea ha forzado al Reino Unido a evolucionar hacía un sistema más intervencionista y de abundante codificación, éste no ha perdido los valores y principios jurídicos asociados tradicionalmente al *common law*, convirtiendo al Reino Unido en un sistema dual cuya dicotomía resulta tremendamente atractiva para su estudio.

Por las razones explicadas anteriormente, esta disertación se va a centrar en el ordenamiento jurídico británico como representante del ámbito legal del *common law*, el cual presenta varias fases en la protección del derecho a la privacidad. Su evolución ha sido eminentemente ascendente[190], siendo sus hitos más relevantes los que se presentan a continuación, destacando la protección de datos personales como la faceta más visible de la protección de la privacidad en el derecho británico.

2.2. Fundamentos de la privacidad en el ámbito jurídico del *common law*

Históricamente, el *common law* inglés no reconocía ningún derecho a la intimidad ni tampoco contemplaba un derecho a la responsabilidad civil[191], sino que en sus inicios se limitaba su protección a la dispuesto por la doctrina de la "*breach of confidence*" -que podríamos traducir como revelación de secretos- a la que más tarde nos referiremos.

Aunque no había en Reino Unido una regulación específica en materia de privacidad, indirectamente se abordaba ya la cuestión desde algunas normas sectoriales tanto en Derecho

[190] Sin embargo, dada la situación política planteada por el *Brexit* así como las últimas reformas legislativas en materia de privacidad, no se descarta una futura reversión del estándar de protección alcanzada, tal como se profundizará más adelante. Esto añade aún más interés al estudio del sistema jurídico británico, cuyos horizontes más inmediatos están aún por determinar.

[191] En el derecho anglosajón se emplea el término "*tort law*" o "*civil wrong*" (ilícito civil). El concepto de "*tort*" en *common law* es muy difícil de definir dada la falta de equivalencia entre nuestros sistemas jurídicos, por lo que sus matices varían en función del contexto que, en el presente caso, se ha convenido traducir por "responsabilidad civil".

privado como desde la perspectiva del Derecho penal, en base al *common law*[192]. Así, se consideraba delito el acoso por parte de los cobradores de deudas o se preveían acciones civiles en contra de la atribución de una falsa autoría, mediante la *Copyright Act 1956*.

El *common law* ha ofrecido tradicionalmente, remedios parciales y limitados para la protección de la privacidad de los ciudadanos británicos, principalmente a través de las figuras de la *breach of confidence* (revelación de secretos), el *trespass* (allanamiento), la *nuisance* (perjuicio, molestias) o la *defamation and malicious falsehood* (difamación), figuras que se examinarán más adelante[193].

Sin embargo, la normativa, o mejor dicho, las pinceladas jurídicas de lo que en la actualidad conocemos como derecho a la privacidad, en el Derecho británico están íntimamente relacionadas con la protección de la información personal de los ciudadanos, esto es, el derecho a la protección de datos, y tuvieron sus comienzos en los años setenta, a raíz de la incipiente introducción de los ordenadores en la sociedad.

No obstante, la implementación de los ordenadores empezó siendo muy sectorial y reservada principalmente al ámbito profesional. Los inicios de lo que ahora se conoce como Derecho a la protección de datos se limitaban a regular ciertos aspectos de la confidencialidad en la empresa en relación con la información personal introducida en las computadoras.

Las reacciones en la materia se propiciaron en 1972 con la publicación, por parte del *Younger Committee on Privacy*[194], de unas recomendaciones sobre el uso de las computadoras que empleaban datos personales en su funcionamiento y que, a grandes rasgos, sugerían supeditar el empleo de información personal a la obtención de una autorización previa por parte de su titular, así como limitar su uso o destino al fin concreto, así como su duración[195]. Es

[192] Ya en el siglo dieciocho se encuentran sentencias estimatorias de ciertos espacios de privacidad, como es el caso de la inviolabilidad del domicilio. *Entick v. Carrington* [1765] EWHC KB J98 95 ER 807, King's Bench, 2 de noviembre de 1765.

[193] Vid. *infra* apartado 4.1 a) del presente Capítulo.

[194] Cmnd 5012, 1972.

[195] Los puntos principales establecían:

asombroso como en este documento se asientan de manera incipiente derechos hoy tan asimilados como el de información, acceso o rectificación de la información personal contenida en un fichero automatizado.

Las propuestas del *Younguer Committee*, más allá de sugerir medidas de control administrativas así como instrumentos de autorregulación (*Self-discipline measures*) según el caso, pasaban también por adoptar cambios en la legislación criminal[196], sugiriendo crear una figura agravada para el tipo de delito de vigilancia -cuando se lleve a cabo mediante un dispositivo técnico- y para el delito de revelación de información obtenida ilegalmente por estos medios. También sugerían cambios en la definición de "*property*" con la intención de que en ella tuviese cabida la "información robada" regulada en la *Theft Act 1908*, en vigor en aquél momento.

En respuesta a estas observaciones, el Gobierno británico publicó años después un *White Paper*[197] en el que se disponían las líneas de actuación del Gobierno en relación con la nueva etapa que estaba por venir, con el objetivo de salvaguardar la privacidad, amenazada entonces

---

a) *"Information should be regarded as held for a specific purpose and should not be abused, without appropriate authorization, for other purposes.*

b) *Access to information should be confined to those authorized to have it for the purpose for which it was supplied.*

c) *The amount of information collected and held should be the minimum necessary for the achievement of a specified purpose.*

d) *In computerized systems handling information for statistical purposes, adequate provision should be made in their design and programs or separating identities from the rest of the data.*

e) *There should be arrangements whereby a subject can be told about the information held concerning him.*

f) *The level of security to be achieved by a system should be specified in advance by the user and should include precautions against the deliberate abuse or misuse of information.*

g) *A monitoring system should be provided to facilitate the detection of any violation of the security system.*

h) *In the design on information systems, periods should be specified beyond which the information should not be retained.*

i) *Data held should be accurate. There should be machinery for the correction of inaccuracy and the updating of information.*

j) *Care should be taken in coding value judgments*".

[196] DWORKIN. "The Younger Committee Report on Privacy", en *The Modern Law Review*, Vol. 36, nº 4, 1973, pp. 399-406.

[197] Cmnd 6353, 1975.

por la forma de proceder de la nueva tecnología emergente. Por primera vez se asienta la necesidad de legislar para preservar un ámbito de privacidad[198] para los ciudadanos así como salvaguardar los intereses industriales y comerciales, disponiendo las bases de lo que en el futuro sería el derecho a la protección de datos, aún en fase embrionaria.

Las reivindicaciones del *Younger Committee* nunca fueron implementadas, principalmente debida al *lobby* ejercido por los medios de comunicación, muy poderosos en la sociedad británica[199], que veían amenazado el derecho a la libertad de expresión y se opusieron frontalmente a cualquier tipo de medida[200]. Sin embargo, ello sirvió para tomar consciencia de la situación y crear el *Lindop Committee* que sugirió[201] la creación de la *Data Protection Authority* así como la elaboración de distintos códigos de buenas prácticas para los diferentes sectores empresariales, definiendo su objeto de protección con el término "*data privacy*"[202].

Sin embargo, ninguna de las propuestas formuladas se tuvo en cuenta, hubo que esperar hasta el Convenio del Consejo de Europa de 1981 para la protección de datos personales[203] para que el Reino Unido estableciese los pilares de lo que sería el derecho a la protección de datos moderno, a través de la *Data Protection Act 1984*. Curiosamente, esta norma vio recogidas muchas de las reivindicaciones que el *Younguer Committee on Privacy* había hecho hacía una

---

[198] Textualmente, dice el párrafo 30: "*the time has come when those who use computers to handle personal information, however responsible they are, can no longer remain the sole judges of whether their own systems adequately safeguard privacy*".

[199] De hecho, en el Reino Unido la prensa escrita, a diferencia de lo que ocurre con los medios de comunicación audiovisuales, se basa en mecanismos de autorregulación cuyos principios éticos están recopilados en un código de buenas prácticas: el *Editors' Code of Practice*.

[200] Como curiosidad, cabe decir que coincidió en el tiempo un hecho que afectó a la imparcialidad del Gobierno: el caso *Lambdon*, por el que dos ministros del gobiernos tuvieron que dimitir al publicarse en la prensa que habían solicitado los servicios de unas prostitutas, asunto que tuvo una gran repercusión mediática, pese a los cuestionables métodos periodísticos empleados.

[201] Cmnd 7341, 1978.

[202] "*The Younger Committee had to deal with the whole field of privacy. Our task has been to deal with that of data protection. In fact, the two fields overlap, and the area of overlap can be called 'information privacy' or, better, 'data privacy' [...] we found it useful to examine the concept of data privacy, and its implications and consequences. For this purpose we have used the term data privacy to mean the individual's claim to control the circulation of data about himself*".

[203] Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

década y que habían sido ignoradas tanto por el Gobierno británico como por el *Lindop Committee*.

2.3. *Data Protection Act 1984*

Esta norma[204], fue una de las primeras leyes en materia substancial de protección de datos en todo el Mundo, cuyo objetivo primero era establecer el régimen jurídico sobre la tenencia y procesamiento automatizado de información[205].

En las disposiciones preliminares de la norma se establecían las definiciones empleadas a lo largo de todo el articulado y que resultan de gran interés por su novedad. Así, por ejemplo, se definen los datos como "información registrada en una forma en la que pueda ser procesada por equipos que funcionan automáticamente en respuesta a las instrucciones dadas con ese propósito", se especifica el procesamiento de datos como la posibilidad de "modificar, aumentar, borrar o volver a organizar los datos o extraer la información de la que consiste los datos y, en el caso de los datos personales, realizar cualquiera de esas operaciones por referencia a la persona sujeto de os datos" y se detallan las posibles formas por las que se produce una tenencia de datos[206].

Uno de los aspectos clave de esta Ley fue el establecimiento de los principios fundamentales en los que se debía fundamentar toda actuación relacionada con los datos personales, asentándose en las bases comunes establecidas en el Convenio del Consejo de Europa de 1981 para la protección de datos personales[207]. Este código de actuación estaba

---

[204] *Data Protection Act 1984, Chapter 35, An Act to regulate the use of automatically processed information relating to individuals and the provision of services in respect of such information*, 12 de Julio de 1984.

[205] El único *statutory instrument* precedente en materia de datos es la *The Medecines (Data Sheet) Regulations 1972*, de 30 de diciembre de 1972. Sin embargo, esta regulación jurídica en materia de protección de datos era escasa y muy sectorial, limitándose a la ordenación de las recetas médicas y de los prospectos de los medicamentos.

[206] *(5) "Data user" means a persona who holds data, and a person "holds" data if (a) the data form part of a collection of data processed or intended to be processed by or on behalf of that person as mentioned in subsection (2) above; and (b) that person (either alone or jointly or in common with other persons) controls de contents and use of the data comprised in the collection; and (c) the data are in the form in which they have been or are intended to be processed as mentioned in paragraph (a) above or (thought not for the time being in that form) in a form into which they have been converted after being so processed and with a view to being further so processed on a subsequent occasion.*

[207] El Convenio, en su artículo 5, disponía los principios a seguir por el tratamiento automatizado de datos de carácter personal: "a) Se obtendrán y tratarán leal y legítimamente; b) se registrarán para finalidades determinadas y legítimas, y no

conformado por ocho puntos de contenido muy general, motivo por el cual dichos principios no podían invocarse directamente frente a los Tribunales[208], salvo por la autoridad de control, la *Data Protection Registrar*, y el *Information Rights Tribunal*, órgano jurisdiccional creado *ad hoc* a tal efecto.

Estos principios, a grandes rasgos, disponían[209]:

1. La información que comprenda datos personales debe haberse obtenido de manera justa y legal y así se procesará.
2. Los datos personales se retendrán sólo para el o los propósitos especificados, que en todo caso deberán ser lícitos.
3. Los datos personales no podrán usarse ni divulgarse de ninguna forma en que resulte incompatible con el propósito para el que fue recolectada.
4. Los datos personales almacenados deberán ser adecuados, relevantes y no excesivos en relación con el propósito para el que fueron almacenados.
5. Los datos personales deberán ser precisos y, cuando sea necesario, deberán mantenerse actualizados.
6. Los datos personales obtenidos con un determinado fin no deberán guardarse más tiempo del que éste requiera[210].

---

se utilizarán de una forma incompatible con dichas finalidades; c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; d) serán exactos y si fuera necesario puestos al día; e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado".

[208] Si bien la *Data Protection Act 1984* está vertebrada en torno a estos ocho principios, sorprende la poca valentía legislativa al catalogar a éstos como "principios", sin fuerza jurídica vinculante aunque, en la práctica, sí que tuvieron cierta trascendencia, como por ejemplo, respecto de las notificaciones de ejecución. CAREY. *Data Protection: a practical Guide to UK and EU Law*, Oxford University Press, Oxford, 2015, p. 5.

[209] Resulta curioso como el texto distingue entre los primeros siete principios, los cuales dice, se aplicarán a los datos personales almacenados por los *data users*, y el último y octavo, cuyo contenido será, además, aplicable cuando los servicios sean prestados por personas que trabajen con máquinas computadoras (párrafo segundo de la Disposición Preliminar segunda).

[210] Ahora bien, se preveían excepciones por razones históricas, estadísticas o de investigación.

7. Toda persona tendrá derecho, sin demoras ni gastos indebidos, a ser informado acerca de sus datos personales almacenados, así como el derecho de acceso, corrección y borrado de los mismos.

También se hacía mención, aunque tangencialmente y abriendo la posibilidad a una modificación o ampliación futura de dichos principios, a determinado tipo de información que por su contenido pudiera resultar especialmente sensible y debiera excluirse de cualquier fichero como regla general: el origen racial, las opiniones religiosas, la salud física o mental, la vida sexual o su historial criminal.

En cuanto a las garantías, la presente norma introdujo dos medidas encaminadas a la protección de datos. Por una parte, dispuso la creación de una autoridad supervisora, *The Office of the Data Protection Registrar*, obligando a todos aquellos que custodiaban datos (*data users*) a formar parte de un registro dependiente de ésta, bajo sanción penal en caso de incumplimiento. Se dispuso el acceso público a este Registro, por lo que todo ciudadano tenía derecho a conocer qué información disponía una empresa sobre su persona, previo pago de una pequeña tarifa, el *data user* estaba obligado a proporcionar esta información en un plazo máximo de 40 días. Este proceso podía instarse ante la *Data Protection Registrar* o directamente ante los Tribunales.

De hecho, el grueso de la norma se dedicaba a tratar todas las cuestiones relativas al Registro: composición, procedimiento, excepciones, sanciones administrativas, delitos penales… No en vano, pues el Registro permite por primera vez a los ciudadanos, saber qué compañías procesan datos personales y con qué propósitos, lo que es un presupuesto básico para ejercitar los derechos subjetivos que se les reconocen.

Por otra parte, esta Ley dispuso las bases para la creación del *Data Protection Tribunal* (que finalmente obtuvo la denominación de *Information Rights Tribunal*), un órgano jurisdiccional *adhoc* para conocer de las cuestiones de ambas partes, al que se le atribuía la obligación de velar por los intereses de los usuarios así como de los *data users*. Se reconocía asimismo un derecho de compensación por daños y perjuicios para los afectados por cualquier

daño sufrido directamente atribuible a la inexactitud, pérdida o divulgación no autorizada de datos, así como el derecho a la rectificación o supresión de la información errónea[211].

En definitiva, la *Data Protection Act 1984*, estableció para el Reino Unido una regulación cuyo contenido era compartido por el resto de sus socios europeos, tratando de unificar un mínimo denominador común[212] en materia de protección de datos personales. Consagró por vez primera derechos de información, acceso, rectificación y borrado de datos personales, obligó a aquellos que almacenaban datos personales a inscribirse en un Registro específico, creó una autoridad de control independiente para su supervisión (*The Office of the Data Protection Registrar*), implantó unos órganos jurisdiccionales especiales para tratar asuntos en materia de protección de datos (el *Information Rights Tribunal*), introdujo sanciones penales para el caso de contravenir sus disposiciones y estableció medidas de responsabilidad civil para indemnizar por los posibles daños y perjuicios sufridos por los usuarios. De hecho, la jurisprudencia que el *Information Rights Tribunal* dictó a resultas de la Ley del 1984 a día de hoy se sigue considerando un marco de referencia en la materia y sirve para interpretar las disposiciones legales en vigor.

En definitiva, la *Data Protection Act 1984* dispuso una de las primeras regulaciones modernas en materia de protección de datos, haciendo frente al contexto de la época pero también avanzándose a la sociedad que estaba por venir, donde los cambios tecnológicos que han revolucionado nuestra forma de comunicarnos estaban aún en fase embrionaria.

Con el objetivo de no incurrir en reiteraciones y lograr así una lectura más amena y comprensiva de la cuestión, se ha optado por no ahondar más profundamente en las

---

[211] *7. Part I, Section 2(1): "An individual shall be entitled – (a) at reasonable intervals and without undue delay or expense – (i) to be informed by any data user whether he holds personal data of which that individual is the subject; and (ii) to access to any such data held by a data user; and (b) where appropriate, to have such data corrected or erased".*

[212] Estas bases comunes fueron establecidas por el Convenio del Consejo de Europa de 1981 para la protección de datos personales que, en su artículo 5, disponía los principios a seguir por el tratamiento automatizado de datos de carácter personal: "a) Se obtendrán y tratarán leal y legítimamente; b) se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; c) serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; d) serán exactos y si fuera necesario puestos al día; e) se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.".

disposiciones legales previstas en la *Data Protection Act 1984* cuyo articulado, prácticamente sin excepción, se reproduce en la *Data Protection Act 1998* –al que, como se verá, se le añaden las modificaciones preceptivas- que a continuación se examina y que estaba vigente en el momento de la redacción de este Capítulo.

2.4. *Data Protection Act 1998*

a) Introducción y contexto de la reforma

Como ya se ha hecho mención, la *Data Protection Act 1998* reproduce íntegramente tanto el planteamiento legal como el esquema organizativo que se empleaba por la normativa anterior, adaptando su articulado a los cambios tecnológicos del momento.

Si bien la *Data Protection Act 1984* fue una legislación precursora en materia de protección de datos y su aplicación estaba produciendo efectos satisfactorios, su derogación por la *Data Protection Act 1998* responde a la necesidad de armonización entre las legislaciones domésticas de los Estados miembros europeos, pues mediante esta Ley se implementó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[213].

Después de dieciséis años reivindicando una regulación que restringiera el procesamiento indiscriminado de los datos personales, se promulgó la Directiva de Protección de Datos el 24 de octubre de 1995, cuyo objetivo era proporcionar a los Estados miembro unas reglas comunes para resolver los problemas que ocasionaba el tratamiento masivo de información personal.

A raíz de su aprobación muchos países, como Italia o Grecia, tuvieron que establecer por primera vez una regulación en materia de protección de datos, mientras que otros países, como Francia o Reino Unido, sólo tuvieron que incorporar a sus legislaciones las novedades

[213] Actualmente derogada por el Reglamento General de Protección de Datos, esto es, 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 datos y por el que se deroga la Directiva 95/46/CE.

proporcionadas por la nueva norma europea. En este último caso, la legislación británica en la materia había sido pionera hasta el punto de que, según defienden algunos autores, llegó a inspirar la propia normativa europea y no al contrario, cosa que podría sustanciarse en la inclusión en la Directiva de los principios inspiradores que se establecieron diez años atrás por la *Data Protection Act 1984*[214].

Podría decirse que la Directiva tenia tres objetivos principales: en primer lugar, garantizar los derechos de las personas individuales a la privacidad en el contexto de la sociedad de la información. En segundo lugar, promover la libre circulación de los datos personales entre los países miembros, introduciendo un marco de integración entre ellos. Y en tercer lugar, prevenir el abuso de los datos personales en territorio europeo, cuyo origen se situaba en terceros países con un inadecuado nivel de protección de estos derechos.

Además de esta normativa, en la redacción de la *Data Protection Act 1998* también tuvo cierta incidencia tangencial la promulgación de la Directiva 96/9/CE del Parlamento Europeo y del Consejo de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos. Ésta, otorga protección a las bases de datos con independencia de si son calificadas o no para su protección como derechos de autor, reconociendo un derecho de autor sobre la bases de datos -que por la selección o disposición de sus contenidos constituya creación intelectual- así como un derecho *sui generis* para el fabricante de una base de datos -con el objetivo de proteger la inversión llevada a cabo en la creación, verificación o presentación de su contenido-. Instituye así un derecho a la protección de las bases de datos cuya consecuencia potencial es otorgarle garantías de privacidad a las colecciones de datos así como a la información en sí misma.

Sin embargo el contenido de esta última normativa disminuyó enormemente a raíz de una decisión del Tribunal Europeo de Justicia que estableció[215], en relación con dicha norma, que sólo se infringirá el derecho a la protección de las bases de datos cuando la apropiación de una base de datos suponga privar a su creador de los resultados de su inversión limitando, en

[214] Cfr. CAREY. *Data Protection Act 1998*, Blackstone Press Limited, London, 1998, p. 31.

[215] STJUE, de 9 de noviembre de 2004, *British Horseracing Board Ltd and others v. William Hill Organisation Ltd*, Asunto C-203/02, [2004] ECR I-10415.

consecuencia, el potencial de las bases de datos para la protección de material académico, histórico y científico.

Por último, en el marco legal introducido por la *Data Protection Act 1998* también se tomó en consideración lo dispuesto por la Directiva 97/66/CE del Parlamento Europeo y del Consejo de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones[216]. Esta norma se adoptó principalmente para hacer frente al correo electrónico no deseado, estableciendo el derecho de los particulares a protegerse de cualquier intrusión provocada por el marketing directo. Trataba así de garantizar el respeto al consentimiento del destinatario en todo caso ya fuese, bien mediante casillas específicas que obligatoriamente debían rellenarse por el usuario (por ejemplo, realizando una compra online), bien mediante las cláusulas de autoexclusión en los mensajes.

La regla general que disponía era que los correos electrónicos no deseados no debían de enviarse hacia aquellos suscriptores que no hubiesen prestado su consentimiento a tal efecto. Asimismo, el remitente no podía ocultar ni disfrazar su identidad a ningún destinatario y su mensaje debía incorporar una dirección válida a la que el destinatario del correo pudiese dirigirse para comunicar que no deseaba seguir recibiendo dichos correos (*opt-out clause*).

Esta regulación englobaba también los SMS, las fotos, los videos y las llamadas telefónicas. Así, por ejemplo, se disponía que tanto las llamadas automáticas como los mensajes publicitarios, sólo podían ser enviados previo consentimiento del usuario[217].

A continuación va a pasarse a examinar, no sólo el contenido de la *Data Protection Act 1998,* sino la configuración general del modelo británico de protección de datos, como primer paso en la garantía de una esfera de privacidad de los ciudadanos de Reino Unido. Para ello se

[216] Actualmente derogada por la Directiva sobre la privacidad y las comunicaciones electrónicas, esto es, 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.

[217] Sin embargo, este consentimiento se obtenía implícitamente por el proveedor de servicios en el acto de contratación de los servicios, como parte de las cláusulas de adhesión, y ello se hacía bajo el amparo de dicha normativa, lo que no parecía ser una adecuada protección del consentimiento informado ni de los derechos de los usuarios.

sigue el modelo adoptado por el grueso de la normativa, esto es la *Data Protection Act 1998*, incorporando asimismo todos aquellos instrumentos y garantías que, sin formar parte de esta norma, integran el marco jurídico de protección.

b) Modificaciones sustanciales en la protección de datos personales

La *Data Protection Act 1998* (DPA en adelante), pese a compartir mucha de la terminología con la ley anterior, otorga un contenido distinto a ésta, debido principalmente a la evolución de la tecnología en este lapso de tiempo, así como a algunas exigencias introducidas por la Directiva 95/46/CE de protección de datos.

Así, por ejemplo, la definición de "datos" no sólo comprende registros manuales, se establece una categoría de información personal – *sensitive personal data*- que, por su contenido altamente sensible, no puede ser objeto de procesamiento como regla general salvo que se den ciertas circunstancias excepcionales

También se amplía el término "procesamiento" que incluye prácticamente todo lo que puede hacerse con los datos personales, incorporando su mera lectura en la pantalla de un ordenador. Y es que, en relación con el procesamiento de datos, la Ley hace referencias indistintas tanto a los registros en papel como a los electrónicos y automáticos, contemplando en ambos casos unos requisitos mínimos que deben cumplirse para que el procesamiento de datos sea legal y legítimo.

Se incorporan asimismo nuevos derechos subjetivos en torno a la protección de los individuos, se integran nuevos derechos de acceso y a ser informado respecto de las decisiones automatizadas, así como la previsión del derecho a cesar determinadas formas de procesamiento. Para todo ello, se diferencia entre el "data subject", la persona que es objeto de tratamiento de datos, y el "data controller", entidad responsable de hacer cumplir la legislación de datos en dicho tratamiento, como los principales sujetos interesados en esta materia.

Se incorpora el concepto de seguridad en el manejo de los datos personales, motivo por el cual se establecen medidas de protección y control. En términos generales, se amplían las

garantías de los derechos ya consolidados, incluso se hace especial hincapié en el derecho a la indemnización por daños y perjuicios en supuestos de procesamiento ilegal de datos.

Se incorpora el veto, sujeto a excepciones, a transferir datos personales hacia países que se encuentren fuera de la Comunidad Económica Europea. Así, como regla general, se prohíbe la exportación de datos a terceros países.

c) Ámbito territorial

Tal y como dispone la *Section* 5 de la DPA, la normativa británica resulta de aplicación a todo encargado del tratamiento de datos establecido en el Reino Unido y, además, a todo aquél encargado que, pese a no estar establecido en suelo británico ni tampoco del Espacio Económico Europeo, utilice equipos del Reino Unido para procesar los datos con una finalidad diferente al tránsito a través de Reino Unido[218]. Es decir, la normativa británica extiende su ámbito de aplicación más allá de las empresas establecidas en Reino Unido, abarcando también aquellas que utilizan equipos británicos para procesar datos personales[219].

En cuanto al concepto de "*establishment*" y pese a que se trata de un término variable en función del tipo de organización en concreto de la que se trate, a grandes rasgos se entiende que una empresa está establecida en el Reino Unido si lleva a cabo actividades en el país.

d) Definiciones básicas

i. Data

Curiosamente, la Directiva de 1995 no da una definición de datos, por lo que la *Data Protection Act 1998* lo ha interpretado como toda aquella información que es objeto de procesamiento por equipos que operan automáticamente, así como aquella que se almacena con la intención de procesarse con medios similares, aquella integrada en cualquier sistema de archivo, la información almacenada por las autoridades públicas u otro tipo de información

[218] Así, por ejemplo, una empresa brasileña que utilice una empresa en el Reino Unido para el almacenamiento de datos personales estará sujeta a las disposiciones de la DPA.

[219] Este principio de extensión territorial de la aplicación de la DPA está dispuesto en unos términos muy similares a lo que recoge el actual Reglamento de Protección de Datos en su artículo 3 y que ha sido objeto de tantos comentarios.

que, pese a no poder ser catalogada por ninguna de las categorías anteriores, forme parte de cualquier registro accesible[220].

Las referencias hechas a los "equipos operados automáticamente" incluyen, obviamente, a los sistemas de procesamiento electrónicas o realizados por ordenadores. Sin embargo, y de ahí la generalidad del precepto, puede llevarse a cabo procesamiento de datos personales por otros medios, bien manualmente, o bien bajo otros métodos como la grabación telefónica activada por voz o por dispositivos de video vigilancia que usen circuitos cerrados de televisión (CCTV).

En cuanto a las alusiones a la información almacenada con intención de procesarse en el futuro, se refiere a todos los documentos físicos que se acumulen con la intención de ser introducidos a mano en un sistema informático o bien escanearlos para incorporarlos. Es decir, para la DPA, la garantía jurídica se activa por la "intención" de un procesamiento automático futuro pese a que éste aún no haya tenido lugar.

Por último, respecto de las referencias del artículo 1 a la información "accesible" en otros registros o a la información recopilada por las autoridades públicas, éstas se hacen pensando en las bases de datos del sistema nacional de salud, en los institutos de educación o en la información en manos de la policía. El grueso de esta regulación se ha llevado a cabo por leyes especiales[221] como la *Personal Files Act 1987*, la *Access to Health Records Act 1990*, la *Education (School Records) Regulations* de 1989 o la *Freedom of Information Act 2000*, que extendió el contenido de la legislación de protección de datos, a aquella información personal que estaba en manos de entidades de gobierno local, las entidades cuasi-autónomas británicas

[220] Article 1 (1): "*In this Act, unless the context otherwise requires, "data" means information which (a) is being processed by means of equipment operating automatically in response to instructions given for that purpose, (b) is recorded with the intention that it should be processed by means of such equipment, (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, or (d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible record as defined by section 68*".

[221] Gracias a estas normas especiales –*statutory instruments*- se ha podido discernir el contenido y la extensión de la *Data Protection Act 1998* en un contexto más práctico. Encontramos, por ejemplo, la sentencia *Smith v. Lloyds TSB Bank Plc* [2005] EWHC 246 en la que se concluyó que una entidad privada, por el mero hecho de almacenar cantidad de información personal en unos paquetes no estructurados metidos, a su vez en cajas, no estaba llevando a cabo tratamiento de datos personales pues no formaba parte de un fichero automatizado ni siquiera se trataba de un sistema relevante de almacenamiento de información.

denominadas "*quangos*", las fuerzas armadas, los cuerpos de bomberos o el sistema de salud, entre otros.

ii. Personal Data

Su definición es clave para poder entender la aplicación de la *Data Protection Act 1998* cuyo objeto gira en torno al procesamiento, precisamente, de los datos personales, esto es "datos referidos a una individuo vivo que puede ser identificado (a) a partir de esos datos o (b) a partir de esos datos y otra información que se encuentre en su poder, o es probable que vaya a estar en poder del *data controller*, incluida cualquier expresión de la opinión del individuo y cualquier indicación de las intenciones del *data controller* o cualquier otra persona con respecto al individuo".

Esta definición de la DPA difiere de la ofrecida por la Directiva de 1995[222] a la que trataba de implementar y ha sido objeto de varia jurisprudencia por los problemas interpretativos que ofrece. El precepto de la ley inglesa hace referencia a una persona "identificada" mientras que la Directiva utiliza el término "identificable" y esto es un aspecto relevante a tener en cuenta porque una persona puede no estar plenamente identificada pero sí ser susceptible de serlo según el tipo de información que de ella se tenga y de si, por ejemplo, se cruzan datos[223].

Así, en el caso *Edem v. IC & Financial Services Authority*, se planteó la cuestión de si almacenar el nombre de una persona comporta automáticamente su consideración como datos personales o si se necesita obtener información adicional respecto de un sujeto para poder considerarlo identificado y, hasta dicho momento, sólo es susceptible de identificación. La Corte sentenció que un nombre puede constituir por sí mismo un dato personal, argumentando

[222] "'*Personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*", Artículo 2. a) de la Directiva 95/46/CE.

[223] Pongamos por ejemplo a un grupo empresarial dedicado a la correduría de seguros que ofrece seguros de salud mediante una marca y, mediante otra filial, presta servicios de seguros de vehículos. Una misma persona puede ser cliente de ambas compañías sin conocer que éstas pertenecen al mismo grupo empresarial, sin embargo, éstas compañías pueden cruzar información de sus bases de datos para, por ejemplo, cuantificar el seguro de salud teniendo en cuenta la cantidad de partes de accidentes de tráfico que su cliente presenta.

que no siempre se necesita de una connotación biográfica para determinar que un dato es un dato personal, sino que un dato puede constituir por si mismo un dato personal cuando su contenido es demasiado obvio acerca de una persona[224].

Otros aspectos debatibles de la redacción de este precepto es el uso de "*living individual*" por la DPA en lugar del "*natural person*" utilizada en la Directiva. Esto plantea dos cuestiones, en primer lugar, queda claro que una vez fallecida una persona, desaparecen sus derechos ejercibles conforme a la legislación de protección de datos personales pero no implica que automáticamente deban cesar las obligaciones que se derivan para el *data controller* pues, por ejemplo, estos pueden transformarse en información personal de otra persona (pensemos por ejemplo el caso de la pensión de viudedad o la indemnización que podrían recibir los familiares).

En segundo lugar, esta definición implica que el Derecho sólo se aplique respecto de personas individuales pero, ¿qué ocurre con los datos que se almacenan sobre una determinada compañía y que pueden identificar a su propietario? La información relativa a las sociedades no está sometida a esta legislación como se concluyó en el caso *Smith v. Lloyds*[225], sin embargo, cuando tales bases de datos incluyen nombres de funcionarios o empleados dentro de una empresa, sí que se sitúan bajo el paraguas de la protección de datos porque un individuo puede ser identificado por su nombre y puesto de trabajo. Sin embargo, la DPA no distingue entre la información procesada sobre personas a título profesional y a título personal.

En definitiva, la definición empleada en la DPA para los datos personales es tan genérica que los Tribunales se han visto obligados a concretarla en base a la casuística del momento. Por otra parte, también es cierto que, con la intención de ofrecer protección jurídica al mayor número de casos posibles, se ha ido alcanzando una definición de dato personal que

[224] "*Data may be personal data because it is clearly linked to an individual because it is about its activities and is processed for the purpose of determining of influencing the way in which that person is treated. You need to consider biographical significance only where information is not obviously about an individual or clearly linked to him*", *Edem v. IC & Financial Services Authority* [2014] EWCA Civ 92.

[225] *Smith v. lloyds TSB Plc* [2005] EWHC 246, la sentenció concluyó que la información relativa a un préstamo concedido a la empresa de Mr. Smith no eran datos personales sobre Mr. Smith.

hace que casi cualquier cosa que pueda relacionarse con un individuo pueda tener esta consideración[226] por lo que debe discernirse si en el caso concreto se está o no bajo el amparo de la norma.

iii. Sensitive Personal Data

Como era de esperar, viendo la *Data Protection Act 1984* que ya asentaba las bases para ello, la DPA establece una categorización de determinada información personal que, por su contenido altamente vulnerable, debe ser excluido del tratamiento como norma general y a la que llama "*sensitive personal data*".

Estos datos sensibles consisten[227] en información relativa a:

a. Origen racial o étnico del sujeto objeto de tratamiento
b. Opiniones políticas
c. Creencias religiosas u de carácter similar
d. Si es un miembro de un sindicato
e. Su condición física y mental
f. Su vida sexual
g. La comisión o presunta comisión de cualquier delito
h. Cualquier procedimiento por cualquier infracción cometida por él o que así haya sido alegado, la eliminación de tales procedimientos o la sentencia de cualquier tribunal en tales procedimientos

La Directiva ya recogía esta posibilidad y permitía a los Estados miembros cierta flexibilidad para establecer sus propias condiciones para poder procesar datos incluidos en dicha enumeración.

[226] Por ejemplo, los datos personales de un individuo pueden referirse a una pluralidad de personas, pensemos por ejemplo, en un individuo que tenga una enfermedad debida a la ingesta de agua corriente o por respirar ciertas sustancias inherentes a la partículas del entorno, cuando dicha persona viva en comunidad en un edificio dónde, es de suponer, estas mismas condiciones se dan respecto del resto de personas que conviven bajo las mismas circunstancias.

[227] Disposición Preliminar Primera, párrafo 2.

Haciendo uso de este derecho, la DPA dispuso más de veinte excepciones[228] por las cuales estos datos podían ser procesados, que pueden sintetizarse de la siguiente manera:

a) Cuando el sujeto haya dado su consentimiento explícito en los casos permitidos por la ley
b) Cuando sea necesario para poder ejercitar obligaciones o derechos específicos o venga impuesto por la legislación laboral
c) Para proteger los intereses vitales del sujeto u otra persona cuando ésta no pueda otorgar su consentimiento por sí mismo por su condición psíquica
d) En el curso de una actividad legitima llevada a cabo por un organismo o asociación sin ánimo de lucro con carácter político, religioso, sindical… cuando se lleve a cabo con las salvaguardas necesarias.
e) Cuando se haya hecho público deliberadamente por el interesado de los datos
f) Cuando sea necesario en el curso de un procedimiento legal o por motivos de interés público (prevención del fraude, fines médicos, registros sobre igualdad ciudadana, procesamiento policial, sistema de pensiones…)

Respecto de estas excepciones merecen ser aclaradas algunas cuestiones. En primer lugar, la diferencia entre el consentimiento explícito que se exige para poder procesar datos personales de contenido sensible y el mero consentimiento que es condición *sine qua non* para el procesamiento de todo tipo de datos, cabe decir que en ambos casos el sujeto debe ser informado apropiadamente sobre el futuro procesamiento para poder tomar una decisión consciente acerca de permitir o no su tratamiento pero, en el caso de los datos sensibles se exige además, que la voluntad del sujeto sea clara e inequívoca.

[228] Section 4 (3), Schedule 3.

En el Reino Unido, siguiendo las recomendaciones de la ICO, se ha convenido en que el consentimiento expreso en materia de datos sensibles sea, en primer lugar, obtenida en un formato que posibilite su archivo -preferiblemente por escrito- y, en segundo lugar, que se utilicen formularios con casilleros.

En segundo lugar, aclarar que la DPA emplea el término "*imposed by law*" para levantar el veto al procesamiento de datos sensibles cuando se trate de ejercer un derecho o una obligación, lo que puede llevar al equívoco de pensar que las obligaciones creadas por contrato pueden estar bajo este régimen cuando sólo por Ley se pueden legitimar estas excepciones.

Del mismo modo debe señalarse que, en la Directiva de 1995, entre los fines médicos no se encontraba la investigación, cosa que sí prevé la DPA y que ha sido una cuestión altamente controvertida pero, como bien señalaba la normativa europea marco, se concedía a los Estados miembros la posibilidad de modular el contenido de estas disposiciones.

En cuanto al procesamiento de datos sobre las opiniones políticas, esto está permitido por la legislación cuando se lleve a cabo por un partido político registrado conforme a Derecho[229], siempre que no cause "daño substancial" al sujeto. Esto, en la práctica, permite a los partidos políticos llevar a cabo procesamiento de datos respecto de sus afiliados sin su consentimiento aunque, una vez un afiliado tenga conocimiento de esta situación, puede solicitar que cese dicha actividad, y el *data controller* deberá cumplirlo en un periodo de tiempo "razonable según las circunstancias", concepto jurídico indeterminado dónde los haya.

El procesamiento de datos personales sensibles comporta algunos problemas prácticos, especialmente cuando su existencia se deriva del procesamiento de otra información personal adyacente. Por ejemplo, los pasaportes europeos son desde el año 2005 de formato electrónico en el que se utilizan datos biométricos[230] para cerciorarse de la identidad del individuo,

[229] *Registration of Political Parties Act 1998*, Section 1.

[230] Dentro de los datos biométricos que se pueden compilar, gracias a un chip de identificación por radio frecuencia (RFID) que permite almacenar digitalmente su contenido, encontramos: huellas dactilares, reconocimiento facial 3D, reconocimiento de iris, geometría de la mano, reconocimiento de voz, reconocimiento de firma o reconocimiento de la geografía de las venas de la mano o dedo.

¿pueden revelar información sensible al comprender información sobre la salud? o, el hecho de contemplar el lugar de nacimiento, ¿puede revelar el origen étnico?

Es decir, se plantea el problema práctico de si debe hacerse mención expresa a esos datos sensibles para activar el protocolo previsto en la Ley o si es suficiente con que dicha información sensible se pueda inferir de otros datos personales. En el caso *Campbell*[231] también se presentó esta cuestión cuando se publicaron unas determinadas fotografías de la modelo Naomi Campbell que sacaba a la luz información sobre su origen racial, pero el tribunal entendió que esto fue accesorio y anecdótico en relación al propósito de las fotografías, por lo que no activó las previsiones legislativas en materia de protección de datos sensibles.

Esta cuestión queda resuelta actualmente por el Reglamento Europeo de Protección de Datos que, en su artículo 9, cuando hace referencia a las categorías especiales de datos personales, ha incluido los datos biométricos, siempre y cuando estén dirigidos a identificar de manera unívoca a una persona física.

iv. Processing

Al contrario de lo que ocurre con los datos personales, la *Data Protection Act 1998* ofrece una definición del procesamiento de datos mucho más amplia que la Directiva de 1995[232]. Así, dispone que se considerará procesamiento de datos personales: la obtención, almacenamiento o llevar a cabo cualquier tipo de operación relacionada con información o datos que suponga (a) organizar, adaptar o alterar dicha información, (b) recuperar, consultar o usarla, (c) divulgar, transmitir o difundirla haciéndola disponible por cualquier medio, o (d) armonizar, combinar, bloquear, borrar o destruirla[233].

---

[231] *Campbell v. Mirror Group Newspapers Ldt*, de 27 de marzo de 2002 [2002] EWHC 499, Court Queen's Bench Division.

[232] "*'Processing' shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"*, Artículo 2.b) de la Directiva 95/46/CE.

[233] Disposición Preliminar Primera, párrafo 3.

Esta definición es bastante acertada porque permite adaptar la legislación, sin necesidad de modificaciones posteriores, a la tecnología existente y a las prácticas vigentes en materia de protección de datos. Así, el almacenamiento de información incluye tanto soportes físicos (como Disquetes, CDs, memorias USB o CPUs) como intangibles ("nube", páginas web u otros servidores de almacenamiento online), del mismo modo que se adapta a la evolución del procesamiento de datos, permitiendo su aplicabilidad a prácticas de almacenamientos de datos (*data warehousing*), minería de datos (*data mining*) o de verificación de datos (*data matching*), entre otras muchas existentes y aún por determinar.

La versatilidad de este concepto ha sido puesta de relevancia por la jurisprudencia, como por ejemplo, en el caso *Campbell v. Mirror Group Newspapers*[234] cuando se sostuvo que todo lo que el periódico Mirror había llevado a cabo con la información personal de la modelo, incluyendo su publicación en prensa impresa, era procesamiento de datos "*the definition of processing is so wide that it embraces the relatively ephemeral operations that will normally be carried out by way of the day-to-day tasks, involving the use of electronic equipment such as the laptop and the modern printing press, in translating information into the printed newspaper*".

v. Rellevant Filling System

Aunque hoy en día lo más habitual cuando hablamos de procesamiento de datos es pensar en el procesamiento mediante medios electrónicos, lo cierto es que también pueden procesarse datos mediante medios manuales. Por eso, la *Data Protection Act 1998* recoge explícitamente esta posibilidad cuando define un fichero como: cualquier conjunto de información relacionada con individuos el cual, aunque dicha información no resulte procesada mediante equipos que funcionan automáticamente en respuesta a las instrucciones dadas para ese fin, esté estructurado en su conjunto, ya sea por referencia a individuos o por referencia a criterios relativos a las personas, de tal manera que la información relacionada con un individuo en particular sea accesible.

[234] *Campbell v. Mirror Group Newspapers Ldt*, de 27 de marzo de 2002 [2002] EWHC 499, Court Queen's Bench Division.

Esta definición también ha ocasionado numerosos problemas prácticos que, una vez más, difieren de la disparidad de criterios al adaptar las definiciones de la Directiva. La DPA parece condicionar la aplicabilidad de la Ley a la existencia de unos datos "estructurados" en referencia a determinados individuos y/o cuando permitan "acceder" a información específica. Sin embargo, el considerando 27 de la Directiva establece que "considerando que la protección de las personas debe aplicarse tanto al tratamiento automático de los datos como al procesamiento manual, el alcance de esta protección no debe depender de las técnicas utilizadas, de lo contrario, se correría un grave riesgo de exclusión; que, no obstante, por lo que se refiere al tratamiento manual, la presente Directiva sólo abarca sistemas de archivo, no los archivos no estructurados".

Por ello, han surgido cuestiones jurídicas en torno al alcance de dicha disposición que han tenido que ser aclaradas por la jurisprudencia, la más relevante, el caso *Durant*[235] en el que se dispuso que, para que un fichero manual en el que se incluyan datos personales fuese relevante a afectos de la ley británica, éste debía ser equivalente en eficacia a un fichero informático pues se argumentó, la intención del Parlamento británico cuando reguló los ficheros manuales en la DPA era incluir sólo aquellos que fueran lo suficientemente sofisticados como para facilitar su accesibilidad en condiciones equivalentes con los ficheros comprendidos en un ordenador. Así las cosas, los ficheros manuales se limitaron a aquellos que estaban organizados mediante información específica claramente estructurada, permitiendo obtener información específica de un individuo en base a sus datos personales[236].

vi. Data controller

Es la entidad responsable de hacer cumplir la ley en materia de protección de datos, definida como "una persona (en solitario o en común con otras personas) que determina el

[235] *Durant v. Financial Services Authority* [2003] EWCA Civ 1746.

[236] "*1) In which the files forming part of it are structured or referenced in such a way as clearly to indicate at the outset of the search whether specific information capable of amounting to personal data of an individual requesting it under section 7 is held within the system and, if so, in which file or files it is held; and (2) which has, as part of its own structure or referencing mechanisms, a sufficiently sophisticated and detailed means of readily indicating whether and where in an individual file or files specific criteria or information about the applicant can be readily located*".

propósito para qué o de qué manera los datos personales han de ser o no procesados". Es lo que en nuestra legislación denominamos encargado del tratamiento de datos.

La palabra "persona" se entiende aquí (la legislación británica suele emplear la denominación "*individual*") como una persona legal, es decir el *data controller* puede ser una única entidad o varios organismos asociados encargados de velar por la protección de datos de lo que deberán responsabilizarse en última instancia. Y pueden serlo desde empresarios individuales, asociaciones o compañías que, a su vez, pueden ser entidades físicas o negocios online, tanto públicas como privadas. Estamos hablando pues de personas autónomas -como abogados, dentistas u ópticos-, asociaciones -como una consulta médica o una empresa de supermercados-, así como empresas físicas -como compañías de seguros o bancos-, y corporaciones cuya operación es exclusivamente online; o también pueden ser *data controller* páginas web o proveedores de Internet. Asimismo, también se incluyen entidades públicas como las administraciones públicas, las fuerzas del orden, los colegios, etc.

El precepto además, hace referencia a la posibilidad de que exista más de una entidad de control por cada operación de datos personales, según los distintos estadios o el recorrido que haga dicha información personal.

Del mismo modo, dice la DPA que sus disposiciones sólo serán de aplicación cuando el *data controller* esté establecido en el Reino Unido o cuando, sin estarlo, esté utilizando sistemas de procesamiento de datos en el Reino Unido.[237]

No debe confundirse la figura del *data controller* con la del *data processor* pues, como a continuación se observa, esta última es una entidad que procesa datos personales en nombre de la primera que es quien resulta responsable en última instancia de las operaciones de procesamiento que se lleven a cabo por la empresa que haya subcontratado (la *data processor*).

Tampoco debe confundirse la figura del *data controller* con la del *Data Protection Officer* pues este último es una persona individual encargada, en relación a una determinada empresa u organización, de hacer que ésta cumpla lo dispuesto en la legislación de protección

[237] Disposición preliminar quinta.

de datos, cosa de la que se hace responsable. Es decir, es la figura que el Reglamento Europeo de Protección de Datos ha puesto de nuevo de relieve para garantizar que en las empresas que tratan con datos personales haya algún encargado responsable de su correcto tratamiento, pero que en el momento de publicarse la DPA no era una figura de aplicación obligatoria en ninguno de los Estados miembros, de acuerdo con la Directiva del 95.

vii. Data processor

Figura definida por la DPA como "cualquier persona, que no sea un empleado del *data controller*, que procese los datos en su nombre", es decir, cuando se subcontrate sus servicios.

Es muy habitual que los encargados del tratamiento de datos utilicen a terceras compañías para que procesen sus datos debido al tiempo y dedicación que esto les supone. Ahora bien, el *data processor* actúa bajo la dirección del *data controller*, no determina los fines del tratamiento o, en caso contrario, se trataría de un *data controller*.

Por esta misma razón, los *data processor* no tienen responsabilidad bajo los incumplimientos que pueda comportar su tratamiento conforme a las disposiciones del DPA, a diferencia de la legislación doméstica de algunos Estados miembros que sí que prevén consecuencias en caso de no cumplir con las disposiciones de protección de datos, con el objetivo de dotar de mayores garantías al tratamiento[238].

Son infinitas las subcontrataciones de servicios a terceras empresas que puede llevar a cabo una compañía y en la que se pueden ver envueltos datos personales de empleados, clientes o terceras personas: *calls centers* para prestar atención al cliente, administradores de nóminas, reciclaje y destrucción de documentos, recaudación de deudas, *website hosting*, etc.

La DPA dispensa a los *data processor* de tener que notificar sus actividades de procesamiento de datos aunque habitualmente, es costumbre que en sus contratos de servicios con el *data controller* se disponga la obligatoriedad de cumplir con determinadas previsiones y

[238] En esta misma línea se ha optado en el Reglamento europeo de Protección de Datos, en el cual se establece que tanto encargado como responsable del tratamiento deben cumplir con las obligaciones dispuestas en el articulado y, de no hacerlo, ambos serán responsables, con el fin de garantizar la coherencia del articulado.

medidas de seguridad para así dar cumplimiento a lo dispuesto por la legislación de protección de datos personales.

e) Data Protection Principles: criterios orientadores para la protección de la privacidad

La legislación en materia de protección de datos exige el cumplimiento de ciertas reglas para que el tratamiento de éstos sea conforme a la Ley. Mientras que estas reglas se encontraban distribuidas por el conjunto del articulado en la Directiva de 1995, la DPA, siguiendo el proceder de la *Data Protection Act 1984*, aglutina todas estas directrices en un mismo apartado en lo que ha denominado "principios" y que no son otra cosa que el código de conducta que deben seguir todos aquellos encargados del tratamiento de datos para lograr que éste sea adecuado.

Los *data protection principles* son los siguientes[239]:

> *1. Los datos personales se procesarán de forma justa y legal y, en particular, no serán procesados al menos que:*
> *a) Se cumpla, como mínimo, una de las condiciones del Anexo 2*
> *b) En el caso de los datos personales sensibles, que se cumpla como mínimo una de las condiciones del Anexo 3*

Las exigencias legales para que se dé un tratamiento legal y justo vienen explicadas más adelante aunque podemos avanzar que su cumplimiento, no siempre conlleva el respeto pleno a este principio. Esto se observó en el caso *British Gas Trading Limited v. Data Protection Registrar*[240] que se origino a raíz de una sanción de la ICO contra la compañía británica de gas al entender que ésta estaba procesando ilegalmente los datos personales de sus clientes principalmente porque la empresa manejaba dos bases de datos, una sobre las tarifas y facturas de sus clientes y otra con fines de marketing. La compañía envió una carta a sus clientes en la

[239] Schedule I, Part I.

[240] *British Gas Trading Limited v. Data Protection Registrar* [1998] UKIT DA98 3/49/2.

que les comunicaba que les gustaría informarles sobre sus productos y servicios, así como sobre los de otras compañías de su mismo grupo empresarial y que si no estaban interesados en ello, devolviesen dicha carta a sus oficinas.

El Tribunal entendió que, pese a cumplir formalmente con los requisitos exigidos en la ley de protección de datos, se trataba de una práctica contraria a derecho pues, en primer lugar, porque no puede exigírsele al interesado un comportamiento activo para preservar sus derechos y en segundo lugar, porque omisión no es una forma adecuada de prestación del consentimiento. Por otra parte, la compañía tenía el monopolio del servicio de gas por lo que el Tribunal consideró además, que había competencia desleal en este caso.

2. *Los datos personales se obtendrán sólo para uno o más propósitos conforme a derecho, y nunca serán procesados de forma incompatible con estos fines*.

Este principio tiene dos facetas, la primera es asegurarse que se obtengan sólo aquellos datos que permite la Ley, y la segunda es evitar la reutilización de esos datos con otros fines. Esto es clave para evitar que, una vez obtenidos los datos por cualquier causa legítima éstos se cedan o vendan a terceras personas para que realicen un tratamiento posterior que nada tiene que ver con el primero.

Un ejemplo claro de contravención de este segundo principio es la práctica, aún no erradicada, por la que una empresa de telefonía móvil, por ejemplo, vende los datos personales de sus clientes a una empresa, por ejemplo también, de supermercados. Teniendo en cuenta la información comprendida en el primer fichero, la compañía envía publicidad sobre su cadena de supermercados a aquellos a quienes cree sus potenciales clientes, teniendo en cuenta un cálculo aproximado del nivel socio-económico de los clientes, que ha llevado a cabo tomando como referencia las tarifas contratadas con la compañía telefónica.

Muchas veces, sobre todo cuando se trata de un grupo empresarial conformado por diversas empresas de distinta índole, surgen problemas prácticos, por lo que para cerciorarse de

que se está cumpliendo el segundo principio, deben examinarse los siguientes extremos[241]: la relación entre el fin para el que se almacenó la información y el propósito para la que es procesada, ambos contextos, la naturaleza de los datos y el impacto del futuro procesamiento en los interesados y las garantías adoptadas por el responsable del tratamiento para evitar el impacto negativo en los interesados.

3. *Los datos personales deberán ser adecuados, pertinentes y no excesivos en relación con el o los fines para los que son procesados*.

El cumplimiento de este precepto debe hacerse teniendo en cuenta dos pasos, en primer lugar, cual o cuales son los fines para el tratamiento de los datos (por ejemplo, la finalidad de almacenar datos sobre las habilidades profesionales de determinados aspirantes a un puesto de trabajo es determinar quién es más idóneo para dicho empleo) y, en segundo lugar, determinar qué tipo de procesamiento de datos es el más idóneo para llevar a cabo ese fin (siguiendo con el ejemplo, cómo se va a llevar a cabo la revisión de las habilidades profesionales de los aspirantes: entrevista personal, examen de sus currículums vitae, test psicológicos, etc.).

El problema es que las empresas que almacenan datos personales tienden a acumular la mayor cantidad posible cuando muchos de ellos ni siquiera tendrán una relevancia importante en el propósito final (por ejemplo, ¿qué mas da cual sea el código postal de un candidato a publicista?) pero, sin embargo, el interesado no tiene forma alguna de prestar su consentimiento a un mayor o menor tratamiento de sus datos personales, por lo que debe ser el responsable del tratamiento quién determine los límites. Así, por ejemplo, a la hora de examinar a los candidatos a un puesto de trabajo, la información personal de los aspirantes debe estar disponible sólo para aquéllas personas que tengan un rol importante en la toma de decisiones y no en una base de datos a la que puedan acceder todos los trabajadores de la empresa.

[241] TREACY/BAPAT. "Purpose limitation – clarity at last?", en *Privacy & Data Protection Journals*, Vol. 3, Issue 6, 2013, pp. 11-14.

Es decir, este tercer principio requiere minimizar los datos en la medida de lo posible, de hecho, los Tribunales británicos han determinado en numerosas ocasiones[242] que recopilar "información adicional" puede ser aceptable en algunas circunstancias pero no cuando se almacena una enorme cantidad de información obtenida de respuestas voluntarias con efectos estadísticos que nada tenían que ver con el propósito del tratamiento de datos para el que no resulta necesaria[243].

4. Los datos personales deberán ser precisos y, de ser necesario, mantenerse actualizados

Este principio no merece demasiadas aclaraciones pues se explica por sí mismo, además se limita a transponer el contenido literal de la Directiva del 95. Cabe decir, no obstante, que, mientras que este principio matiza la necesidad de mantener la información actualizada sólo cuando sea "necesario", no especifica nada acerca del requisito de precisión, por lo que se deduce que el requisito de garantizar que los datos personales son precisos es absoluto.

La obligación de velar por que los datos personales almacenados sean precisos y estén actualizados recae en los *data controller*, sin embargo, esto no implica que tengan que llevar a cabo labores de investigación, sino que serán los propios sujetos objeto del tratamiento los que deberán comunicarle si se ha producido cualquier cambio[244].

De la interpretación de este cuarto principio, efectuado a raíz de las diferentes sanciones que ha impuesto la ICO, se deriva que no se infringirá éste cuando la información imprecisa en los datos personales registre con precisión la información obtenida del interesado o de un

[242] Por ejemplo, el caso *Community Charge Registration Officers of Runnymede Borough Council v. South Northamptonshire* [DA/ 90 24/49/3]

[243] "*The information the appellant wishes to hold on database concerning individuals exceeds substantially the minimum amount of information which is required in order for him to fulfil the purposes for which he has sought registration namely to fulfil his duty to compile and maintain the Community Charges register […] we are satisfied the evidence before us that the wide and general extent of the information about dates of birth is irrelevant and excessive*", *Community Charge Registration Officer of Rhondda Borough Council v. Data Protection Registrar* [DA/90 25/49/2].

[244] Así, debe proporcionarse algún método para que los sujetos verifiquen y corrijan los datos que posee el *data controller*, que cumplirá con este principio por ejemplo, haciendo un informe anual de sus clientes, revisando la información almacenada o solicitando actualizaciones, entre otros.

tercero si el *data controller* ha tomado las medidas necesarias para garantizar la corrección de una información o si, a raíz de la comunicación de una falta de actualización por parte del sujeto objeto de tratamiento, se han hecho constar estos hechos por parte del *data controller*.

En definitiva, los *data controller* tienen la responsabilidad de verificar que los datos que poseen son ciertos y están actualizados, por lo que deben de tomar medidas encaminadas a cumplir con este principio. Sin embargo, la exigencia de este deber de diligencia variará en función del tipo de datos personales que se almacenen, así como del tipo de procesamiento y su finalidad[245]. Hay que tener presente que este principio está relacionado con el derecho de rectificación, borrado o destrucción de los datos personales.

5. *Los datos personales procesados para cualquier fin o propósito no se conservarán por más tiempo del necesario para ese fin o esos propósitos*.

En la práctica, esto impone la obligación de que los datos personales se borren, se destruyan o se anonimizen cuando ya no sean necesarios para el propósito con el que fueron almacenados. Sin embargo, no hay disposiciones interpretativas acerca de este precepto ni límites temporales establecidos, por lo que se dejará a los *data controller* que hagan sus propias estimaciones en función del tipo de datos personales de los que dispongan y del tipo de acciones de tratamiento que lleven a cabo.

Así pues, en orden a garantizar el cumplimiento de este principio, en primer lugar los *data controller* deberán hacer un análisis del tipo de procesamiento que desean llevar a cabo en relación con los datos personales de los que disponen, y así hacer una estimación del tiempo que necesitarán para llevar a cabo estas acciones de tratamiento.

El factor clave a tener en cuenta es el tipo de información personal acumulada, pues no es lo mismo que un hotel almacene ciertos datos personales de sus clientes para verificar su

[245] Por razones obvias, no es lo mismo el contenido de un acta de una reunión de la Junta de Dirección (que puede comprender datos personales, empezando por los asistentes), que simplemente deja constancia y cuyo contenido no debe ser actualizado, que la información respecto de sus clientes de una entidad bancaria, que debe ser objeto de una permanente revisión.

identidad, que los datos que almacenen de aquellos clientes que deseen estar suscritos a su boletín de ofertas mensual. Así pues, también es posible que unos mismos datos personales sean retenidos para finalidades distintas, en cuyo caso, resulta apropiado almacenarlos hasta que el último de los propósitos haya sido ejecutado.

En cualquier caso, este quinto principio no permite almacenar información personal indefinidamente ni de forma especulativa, la ICO ha reiterado que los datos no pueden almacenarse "por si acaso", pese a existir una pequeña posibilidad de que los datos, después de haber finalizado el tratamiento, puedan necesitarse de nuevo, éstos deben borrarse. Quizás una buena alternativa a la destrucción en este caso sea la anonimización de los datos personales, muy útil en ciertas circunstancias.

Hay que tener en cuenta que, respecto de lo anteriormente dicho, el borrado y la destrucción de los datos personales son aspectos inherentes al procesamiento y que, por tanto, estas actividades deben cumplir con los preceptos legales a tal efecto.

> *6. Los datos personales se procesarán de conformidad con los derechos de los sujetos contenidos en esta Ley*

Las aclaraciones y notas relativas a este principio se remiten al apartado correspondiente de este Capítulo en el que se tratan detalladamente los derechos de los sujetos objeto del tratamiento: derecho a evitar el marketing directo, derecho de compensación, derecho de rectificación, derechos relacionados con las decisiones automatizadas y derechos de prevención de procesamiento que pueda causar daños o perjuicios.

> *7. Se tomarán medidas técnicas y organizativas apropiadas contra el procesamiento no autorizado o ilegal de datos personales y contra su pérdida accidental o destrucción o daño.*

La finalidad de este principio es asegurar que se toman las medidas necesarias para evitar un procesamiento o tratamiento inadecuado de los datos. Sin embargo, este principio, que se deriva del artículo 17 de la Directiva del 95, no está transpuesto en los mismos términos

pues, mientras que la norma europea dispone que los encargados del tratamiento deben asegurarse de que se toman medidas de seguridad necesarias en relación con los riesgos que se presentan para el procesamiento teniendo en cuenta la naturaleza de los datos, la interpretación que de ello hace la DPA se refiere al daño que podría provocarse en caso de incumplirse las medidas de seguridad.

Sin embargo, en otras disposiciones de la propia DPA[246] se dispone que el nivel de seguridad a adoptar se deriva del desarrollo de las nuevas tecnologías y del coste de implementar dichas medidas que, en última instancia, deben asegurar un estándar adecuado teniendo en cuenta la naturaleza de los datos que deben protegerse y de los daños y perjuicios que puedan derivarse de un procesamiento ilegal o no autorizado o de una pérdida o destrucción accidental.

> *8. Los datos personales no se transferirán a un país o territorio fuera del Espacio Económico Europeo a menos que éste garantice un nivel de protección de los derechos y libertades de los interesados por el procesamiento*

Este último principio, cuyo desarrollo se lleva a cabo en un ulterior apartado de este Capítulo, está motivado por la decisión europea que se consolidó en la Directiva del 95 de prohibir, como regla general, cualquier exportación de datos personales hacia países de fuera del Espacio Económico Europeo[247].

Esta decisión se tomó al considerar una prioridad el hecho de evitar cualquier transferencia internacional de datos personales hacia países que no tienen normas restrictivas de la privacidad de los datos o que no gozan de los mismos estándares de protección en la materia que los países del EEE. Sin embargo, existen excepciones y otros mecanismos previstos, que se examinarán a continuación, a efectos de facilitar el comercio global.

---

[246] Schedule 1, 9-12.

[247] A meros efectos recordatorios: éste incluye a los Estados miembros de la Unión Europea, a Noruega, Islandia y Liechtenstein.

Así, cada *data controller* deberá cumplir con estos ocho principios cuya importancia viene además subrayada, por el alcance de los poderes de la ICO en relación con la emisión de notificaciones en caso de contravención así como por su potestad para imponer sanciones pecuniarias en ciertas circunstancias. Sin embargo, como más tarde se examinará, existe un número considerable de excepciones en la aplicación de uno o varios de estos principios, aunque sólo hay dos previsiones por las cuales un *data controller* no tiene que cumplir con todos los principios: seguridad nacional y propósitos domésticos.

f) Estándar de garantía para un procesamiento de datos acorde a la legalidad

Se trata de una exigencia general aplicable a todo tratamiento de datos, que deriva del primer principio e implica varias facetas. En primer lugar exige que los datos personales se hayan obtenido y almacenado de forma justa. Esto implica que, cuando el *data controller* obtiene la información, debe hacerle partícipe al interesado de ciertos aspectos en relación al tratamiento de datos[248]: la identidad del *data controller*, el propósito o los propósitos para los que se tiene la intención de procesar la información, y cualquier otra información relevante en torno al procesamiento.

Sin embargo, esto fracasa a efectos prácticos pues este paso informativo no requiere la conformidad del interesado por lo que es posible que, por desinterés o por pereza, éste no lea dichos términos aunque estén "fácilmente disponibles" como exige la Ley. También conviene añadir que, entre la información que debe ponerse al alcance del interesado, no se incluye la identidad del *data controller*, cuando a nuestro parecer resulta un aspecto relevante[249].

En el entorno online, la mayoría de las veces la información que debe ponerse al alcance del interesado es tanta que, bien por agilidad como por estrategia comercial, se advierte del

[248] Esto es lo que nosotros conocemos por como política de privacidad y que los británicos llaman "*fair processing notice*", "*privacy notice*" o "*privacy policiy*".

[249] Esta opinión se comparte por ERDOS, quien profundiza en los requisitos exigidos por aplicación del primer principio de la DPA 1998 más allá de lo que permite la presente disertación. Cfr. "Stuck in the Thicket? Social Reserach Under the First Data Protection Principle" en *International Journal of Law and Information Technology*, Vol. 19, 2011.

procesamiento y se remite a otra página web para acceder a todos los términos de éste[250], en lo que ha sido denominado como enfoque multicapa (*multi-layered*) y que fue aprobado por el ICO en el año 2009[251].

En muchas ocasiones, el *data controller* obtiene los datos personales no directamente del propio interesado sino gracias a una tercera persona como, por ejemplo cuando la información se proporciona por un pariente o bien cuando se transmite de un *data controller* a otro, lo que se conoce como "*list rental*"[252]. La DPA dispone para estos casos, que no es necesario que se informe al interesado de las condiciones de procesamiento por el nuevo *data controller* siempre y cuando los fines de éste no sean "desproporcionados". Sin embargo, no se ofrece ni en la DPA ni en la Directiva ninguna definición de este término jurídico indeterminado por lo que, en la práctica, se aplica esta excepción como regla general, siempre y cuando no se trate de datos sensibles o de un procesamiento con un propósito claramente distinto.

En cualquier caso, cabe decir que bajo la DPA existe la presunción de que los datos se han adquirido conforme a derecho cuando quien los haya obtenido esté autorizado para suministrar dichos datos y cuando haya puesto a disposición del interesado toda la información preceptiva[253].

En segundo lugar, una vez se han obtenido estos datos personales de forma adecuada, su procesamiento debe llevarse a cabo de forma "justa, legal y legítima" conforme a la DPA[254]. Esto exige, por una parte, que el interesado haya prestado su consentimiento, libre y

---

[250] Es muy frecuente encontrar en las páginas web un anuncio en el que se advierte, por ejemplo, "su información será usada para procesar su pedido y mantenerle informado de nuestras ofertas y novedades. Para obtener información detallada del uso de su información, por favor, haga *click* aquí".

[251] *Code of Practice on Privacy Notices* (ICO). Exige que inicialmente, al menos, se contenga la información básica así como la identidad de la organización y el objeto principal del procesamiento de los datos; pudiéndose remitir el resto a otro emplazamiento.

[252] *List rental* es una práctica común entre las empresas mediante la cual se intercambian datos y direcciones de sus clientes y consumidores.

[253] Schedule 1.1 (2), Part II.

[254] Schedule 2.

específico[255], que puede ser obtenido por infinidad de métodos -no siendo uno de ellos, la omisión o silencio del sujeto ante cualquier comunicación del *data controller*-. Sin embargo, no hay que confundir, como se explica en este mismo Capítulo, el consentimiento exigido para el tratamiento general con el "consentimiento explícito" exigido para el tratamiento de los datos personales sensibles.

Por otra parte, exige que el procesamiento sea necesario por cuestiones relevantes: por necesidades contractuales (en las que el interesado sea parte o aspire a serlo), conforme a una obligación legal, por intereses vitales del sujeto, por funciones de naturaleza pública (por ejemplo, para el procesamiento judicial de una persona o para el ejercicio de la función pública) o por los legítimos intereses del *data controller*[256].

La última de las cuestiones es la que suscita ciertos recelos puesto que no hay definición alguna de "intereses legítimos" en la normativa, debe de entenderse que en ningún caso pueden resultar perjudiciales para los derechos, las libertades o los intereses legítimos de los sujetos objeto del tratamiento. Sin embargo, hay que decir que la normativa británica es mucho más amplia y permisiva que la de otros Estados miembros que, por ejemplo, condicionan este tipo de tratamiento a la obtención del visto bueno o de una autorización por parte de la entidad reguladora pertinente.

En cuanto al resto de condiciones, parecen claras las premisas para un tratamiento de datos adecuados. Sin embargo, la DPA se excede en el uso de términos ambiguos y conceptos jurídicos indeterminados por lo que los tribunales han debido de actuar para interpretar los detalles de la Ley. Esto ocurrió en el insólito caso *Johnson*[257], un cirujano ortopédico que vio como la mutua a la que pertenecía rechazaba su renovación, después de demostrarse que utilizaban un sistema de puntos basado en las reclamaciones que se hacía contra sus

[255] La DPA no proporciona una definición de consentimiento aunque la Directiva del 95 decía en su artículo 2 que éste debe ser "*freely given, specific and informed indication on his wishes by which the data subject signifies his agreement to personal data relating to him being processed*".

[256] Así, por ejemplo, cuando un cliente realiza una compra por Internet es necesario que introduzca sus datos personales y de su tarjeta de crédito para poder cobrarse el importe y hacerle llegar el envío. O, cuando una persona, para pertenecer a un partido político presta sus datos personales a la hora de afiliarse.

[257] *Johnson v. Medical Defence Union* [2007] EWCA Civ 262.

mutualistas. Los tribunales señalaron que, pese a que se trataba de un procesamiento injusto de sus datos, incluidas en las bases de datos de la empresa y sus ordenadores, la DPA no resultaba aplicable puesto que no fueron datos procesados automáticamente sino que fue una persona quien, examinando los datos, tomó la decisión legítima de no renovar la póliza, basada en la libertad de empresa.

Por último, conviene destacar otras restricciones importantes al tratamiento de datos: el deber de confidencialidad, la legislación acerca del *copyright*, la *Human Rights Act 1998* y las previsiones legales comprendidas en la *Computer Misuse Act 1990*, la *Police and Justice Act 2006* y la *Serious Crime Act 2007*.

g) Exportación de datos a terceros países

Aunque ya se ha hecho referencia previamente, en relación con el octavo principio, a la exportación de datos a terceros países, procede incidir aquí en su contenido pues una premisa fundamental para llevar a cabo un tratamiento de datos legal y justo es que éste se produzca dentro de los territorios considerados seguros por la Unión Europea.

Siguiendo la determinación de la Directiva del 95, la DPA prohíbe cualquier exportación de datos personales desde el Espacio Económico Europeo hacia terceros Estados o territorios salvo que éstos aseguren un nivel adecuado de protección de los derechos y las libertades de las personas en relación con el procesamiento de datos.

Así pues, la primera cuestión a tener en cuenta es si estamos ante una transferencia de datos. Pese a que la DPA no incorpora ninguna definición de "transferencia", la ICO ha dispuesto a través de sus resoluciones que, para que la exportación de datos sea contraria al octavo principio, no es suficiente con un simple tránsito de datos sino que se requiere, además, una operación sustancial de esos datos en el tercer país lo que, en la práctica, deja fuera dos actividades importantes: por una parte, la transferencia técnica de datos entre servidores localizados en distintos puntos del mundo (como páginas web o servidores de correo electrónico) y, por otra, el acceso electrónico a datos personales de viajeros de corta duración en países en los que se da un nivel adecuado de protección.

En segundo lugar, hay que determinar si la transferencia que pretende llevarse a cabo tiene como destino un territorio "seguro". La Comisión Europea es quien tiene la facultad de determinar cual es el nivel de seguridad de un territorio (que puede no ser uniforme en relación con los distintos tipos de procesamiento existentes).

No obstante la DPA contempla excepciones por distintas razones[258]: consentimiento informado, cuando se trate de una ejecución de una obligación contractual, por razones de interés público, para ejercitar un derecho legal, para preservar intereses vitales (razones médicas, de salud), en relación con los registros públicos y si la transferencia se autoriza o se da en los términos previstos por la Comisión, asegurando un nivel adecuado de protección.

Este último concepto jurídico indeterminado –nivel adecuado de protección-, se concreta generalmente en las llamadas *Binding Corporate Rules* (BCR) y las *contractual clauses*. Las primeras permiten transferencias internacionales de datos entre sociedades de un mismo grupo multinacional de empresas, cuando hubieran sido adoptadas normas o reglas internas vinculantes que garanticen los derechos y libertades de los interesados.

Es un mecanismo de autorregulación, implementado desde el 2003, que varía en función de cada empresa (no hay normas tipo), que garantiza el cumplimiento de los estándares de protección en materia de datos y establece procedimientos para garantizar su cumplimiento, tanto dentro como fuera del grupo empresarial.

Para su implementación se requiere la autorización previa todas las agencias nacionales de protección de datos[259], para lo cual se ha diseñado un mecanismo de cooperación entre éstas. La agencias deben prestar su conformidad con la propuesta de *Binding Corporate Rules* que redacte la propia empresa interesada y sobre la que se añadirán, en su caso, los cambios pertinentes.

---

[258] Schedule 4, Section 4 (3), DPA.

[259] Por éste y otros motivos, se trata de un mecanismo muy costoso en términos económicos y de tiempo, por lo que muy pocas empresas decidían emplearlo. Ahora, sin embargo, se ha agilizado la obtención de este estatus y cada vez son más las empresas que intentan llevarlo a cabo.

Éstas deben tener fuerza vinculante y ser susceptibles de someterse a mecanismos de ejecución, es decir, las personas protegidas bajo las BCR deben convertirse en terceros beneficiarios, ya sea en virtud de la legislación nacional pertinente como mediante acuerdos contractuales entre los miembros del grupo empresarial. Los interesados deben tener pues, derecho a exigir el cumplimiento de las BCR bien mediante un procedimiento ante una autoridad nacional de protección de datos, bien directamente ante los tribunales.

Las *contractual clauses* por su parte, consisten básicamente en la adhesión a una cláusulas contractuales dispuestas por el encargado del tratamiento en territorio europeo y firmadas por el encargado del tratamiento destinatario de las mismas, cuyo contenido garantiza el respeto a la protección de la privacidad así como de los derechos y libertades de las personas en el ejercicio de sus derechos en materia de protección de datos.

De nuevo es la Comisión Europea la que tiene facultades para determinar si unas cláusulas contractuales proporcionan garantías suficientes aunque se delega en los Estados miembros ciertas potestades para tomar las medidas necesarias encaminadas a cumplir con los estándares de la Comisión.

Aunque, en la práctica, estas cláusulas forman parte del propio acuerdo comercial, el destinatario no tiene posibilidad ninguna de negociar su contenido, sino meramente adherirse a ellas. Si, por cualquier circunstancia, se modifica la redacción de las cláusulas, el reconocimiento de adecuación en materia de protección de datos cesa automáticamente, aunque el propio encargado del tratamiento podría evaluar la adecuación a los estándares de protección por si mismo, sobre la base del acuerdo comercial.

Las transferencias internacionales de datos pueden llevarse a cabo hacia un *data processor* o un *data controller*, en cualquier caso, mediante la adhesión a este contrato el destinatario debe de garantizar el respeto al estándar europeo en materia de protección de

datos[260], disponiendo los mecanismos encaminados a su cumplimiento así como a la eventual compensación por los daños y perjuicios que puedan derivarse de su contravención[261].

Sin embargo, debemos señalar que la exportación de datos hacia un *data processor* comporta una rebaja significante de los estándares anteriores de protección, incluso, se prevé la posibilidad de subcontratar el cumplimiento de las obligaciones de los encargados del procesamiento. Ahora bien, las obligaciones del exportador de datos continúan comprendiendo la inclusión de una garantía sobre el cumplimiento permanente de la ley, una evaluación de los requisitos de seguridad aplicables y la obligación de notificar a los interesados cuando la transferencia incluya datos personales de contenido sensible.

Existen distintos tipos de modelos de cláusulas contractuales, los primeros empezaron a ser efectivos a partir de año 2001 y contenían una serie de requisitos para garantizar el cumplimiento, que se consideraron demasiado restrictivos para determinadas operaciones comerciales, por lo que, la Cámara de Comercio Internacional, en el año 2004[262], redactó un segundo conjunto alternativo de tipologías de modelos de cláusulas contractuales en las que, básicamente, el importador de los datos tiene una mayor discrecionalidad[263] a la hora de decidir cómo cumplir con las leyes de protección de datos[264]. Tanto es así, que las autoridades nacionales de protección de datos tienen, en última instancia, la facultad de oponerse a una exportación de datos cuando el importador rechace adoptar las medidas mínimas necesarias para hacer cumplir la Ley.

---

[260] La legislación aplicable a este tipo de contratos es la que se derive del Estado miembro del exportador de datos.

[261] La inclusión de una cláusula que garantice una indemnización en caso de incumplimiento puede también añadirse si se estima conveniente.

[262] Aún se aprobó un tercer estadio de modelos de contratos en el año 2010, con respecto a la importación de datos por parte de empresas de procesamiento.

[263] Esto comporta consecuencias directas para los sujetos objetos de tratamiento y su derecho de acceso pues, el exportador de datos sólo está obligado a responder las peticiones de los interesados cuando el importador no haya aceptado hacerlo, es más, puede denegar el derecho de acceso si considere el requerimiento "abusivo". Además, los interesados sólo pueden hacer valer sus derechos contra la parte responsable de un quebrantamiento relevante de la legislación.

[264] Sin embargo, el importador de datos debe continuar demostrando una serie de requisitos, entre ellos, que su legislación doméstica permite el cumplimiento íntegro de las cláusulas contractuales.

La legislación británica, además de los dos mecanismos anteriores compartidos por la mayoría de los Estados miembros, dispone de un tercer procedimiento para llevar a cabo transferencias internacionales de datos hacia países no europeos, bajo las denominadas *international outsourcing arrangements*[265].

Se trata de contratos mediante los cuales se suple una deficiencia en la protección de datos que, de no existir, permitiría una transferencia internacional de datos con todas las garantías. Se suple así dicha falta de garantía para una transferencia en concreto o un conjunto de transferencia mediante un acuerdo contractual.

Esta posibilidad se parece mucho a las *contractual clauses* con la diferencia de que, están pensadas para casos dónde el nivel de protección esté cuasi garantizado y además, su contenido no está encorsetado por ningún modelo estándar (lo que no es una ventaja necesariamente, ya que no cuentan con un guión a modo de paraguas, por lo que se puede denegar su eficacia en última instancia).

En definitiva, las *international outsourcing arrangements* son otra medida de autorregulación mediante la cual se le impone a la empresa que quiera ejercitar dicha posibilidad, la carga de examinar la legislación y el sistema de protección del país de destino a fin de determinar cual es su nivel de protección. Como en el caso anterior, no es necesario formalizar un contrato por separado para la protección de datos sino que pueden establecerse cláusulas dentro del articulado que regule la actividad con una determinada compañía extranjera. Ahora bien, estos contratos deben de ser muy exhaustivos a fin de garantizar el respeto al estándar de protección de los datos personales.

[265] Así lo dispone la ICO en su página web cuando dice "*even if the European Commission has not decided that the law in a country is adequate, you can still transfer personal information if you are satisfied that the particular circumstances of the transfer ensure an adequate level of protection*".

h) Derechos de los "data subject"

Los derechos de los sujetos objeto de tratamiento se contienen, principalmente, en la segunda parte de la DPA[266], y en su mayoría son derechos ejercibles contra los *data controllers*.

Aunque a continuación se procederá a un examen pormenorizado de éstos, resulta conveniente mencionar de antemano que el ejercicio de muchos de estos derechos queda vinculado a la notificación o solicitud por escrito. Y, para estos propósitos, el término "*writing*" de la DPA incluye el correo electrónico y, desde 2013, también otros medios de petición como puede ser *Facebook*, *Twitter* o cualquier cuenta de una red social[267].

Los niños pueden ejercitar sus propios derechos en materia de protección de datos cuando se haya probado que tienen juicio suficiente para comprender la naturaleza de lo que están solicitando, cuyo umbral, en principio, se sitúa en los doce años. Para edades comprendidas bajo este límite, serán los propios padres o representantes los que podrán ejercitar los derechos en su nombre.

Asimismo, resulta oportuno señalar que, para una comprensión completa de esta materia, es conveniente examinarla conjuntamente con el apartado correspondiente en este Capítulo relativo a las exenciones (Part IV, Sections 27-39, DPA.)[268], pues muchos de estos derechos están sujetos a ciertas excepciones en beneficio de los *data controllers*. Sin embargo, la legislación británica no hace mención alguna a la posibilidad de excluir mediante cláusula contractual alguno de estos derechos o incluso todos, cosa que no parece posible, ni creemos que se permitiese ni por la ICO ni por los tribunales. Además, la ley de protección al consumidor fácilmente podría anular el intento de un *data controller* de excluir los derechos de la DPA mediante contrato, pues esto es claramente contrario al Derecho.

---

[266] Part II, Sections 7-15.

[267] *Code of Practice on Subject Aceess Requests* 2013, de la ICO.

[268] Vid., *infra* Cap. III. 2. 5. h).

i. Right to subject access

Bajo este derecho, recogido en la Sección 7 de la DPA, los sujetos están facultados para hacer un requerimiento escrito mediante el cual solicitan que una organización determinada les proporcione toda la información personal que disponga sobre ellos. Y es que toda persona tiene derecho a saber cuántos datos personales se tienen sobre ella, quién los almacena y con qué propósito, pues para que el procesamiento de datos sea justo y legal, los sujetos objeto del tratamiento deben ser debidamente informados por el responsable del tratamiento, sobre la existencia y los términos para ejercer el derecho de acceso a sus datos personales.

Habitualmente, los interesados quedan informados de la existencia de este derecho a través de las políticas de privacidad de la empresa, dónde se hacen constar todos los extremos, la cual cosa suele estipularse en un documento a parte (lo que puede ser discutible a efectos de un correcto deber de información).

El derecho a obtener una copia acerca de los datos personales que se poseen por parte de una empresa, organización o administración pública[269], además, comporta toda una serie de informaciones accesorias: los propósitos para los que se utilizan esos datos, de dónde se han obtenido, los destinatarios finales de los datos y si ha habido lugar a decisiones automáticas y en qué términos. Y además exige que la información o copia de los datos que reciban sea comunicada en una forma adecuada para su comprensión.

Así pues, todo interesado puede interponer -por escrito- un requerimiento para conocer todos estos extremos, personalmente o a través de un representante, previo pago de una pequeña fianza -10 libras actualmente- y, acto seguido, el *data controller* tendrá la obligación de responder en el plazo máximo de 40 días.

Sin embargo, antes de contestar el *data controller* deberá de confirmar la identidad del solicitante y, una vez hecho, sólo tendrá obligación de proporcionarle tal información después

[269] Las autoridades públicas tienen las mismas obligaciones que las organizaciones privadas de proporcionar acceso a aquellos que lo soliciten, de hecho, están obligadas a ir un paso más allá en la búsqueda de información relevante, en virtud de otras normas sectoriales como la *Freedom of Information Act 2000*. Este deber se aplica respecto de toda categoría de datos aunque, las administraciones no estarán obligadas a cumplir con esta obligación cuando el requerimiento no contenga una mínima descripción de los datos a los que se pretende acceder.

de comprobar que la información que se posee de él constituye datos personales[270], y siempre y cuando proporcionarle tal información no infrinja los derechos de privacidad de terceras partes[271] ni le suponga un esfuerzo desproporcionado[272], ni tampoco se trate de un requerimiento muy similar a otro hecho hace poco tiempo.

En cuanto a la identidad, a diferencia de otros Estados miembros, Reino Unido no exige verificar la identidad con ningún documento de identidad oficial, sino que basta con una firma del solicitante mediante la cual declare ser la persona que indica y, si los datos no concuerdan con sus bases de datos o se duda, puede exigirle al solicitante una acreditación adicional de su identidad dentro del plazo: compeliéndole a responder algunas preguntas, solicitando un documento oficial que lo acredite, o mediante la verificación por parte de una tercera persona que atestigüe su identidad[273]. Esto, sin embargo, es problemático pues puede ocasionar una vulneración de los principios de la DPA si, con tal de acreditar la identidad del solicitante, el *data controller* solicita y adquiere nuevos datos personales que exceden de lo razonablemente necesario para acreditar la identidad personal.

En cuanto a los ficheros manuales de datos personales, es bastante frecuente que se deniegue el acceso a los solicitantes bajo el argumento de que, al no constituir éstos un sistema de organización suficientemente organizado, no se puede considerar un sistema de archivo "relevante" a los efectos de la DPA. Esto se produce como consecuencia de la sentencia del caso *Durant*[274] que ha limitado drásticamente el derecho de acceso en este tipo de ficheros, al

---

[270] Fue a partir del caso *Durant v. Financial Services Authority* [2003] EWCA Civ 1746, cuando se determinó que la información que una empresa tenía sobre ciertas personas no siempre tenía porqué constituir datos personales y, de no ser así, no tenía obligación ninguna de proporcionarle acceso a ésta.

[271] Salvo que se cuente con su consentimiento o éste no sea necesario teniendo en cuenta las circunstancias concretas. Esta excepción no se aplica cuando la tercera parte es una organización o una compañía (persona jurídica).

[272] Este concepto fue introducido por la sentencia *Ezsias v. Welsh Ministers* [2007] All ER (D) 65 (Dec), que dispuso que la proporcionalidad debe determinarse en función de la onerosidad que le supone al *data controller* extender copia de los datos personales que se tienen de una persona, en relación al tamaño de la organización y al tiempo que debe dedicarle a tal fin. De hecho, éste es el argumento clásico de los responsables del tratamiento que se quejan de la gran carga administrativa y económica que supone cumplir muchas veces con estas obligaciones en un breve plazo de tiempo.

[273] El problema, sin embargo, se plantea respecto de los métodos electrónicos de requerimiento, en los que, casi siempre será necesario acreditar la identidad mediante información adicional.

[274] *Durant v. Financial Services Authority* [2003] EWCA Civ 1746.

exigir para su ejercicio un doble test de idoneidad: en primer lugar, si existen referencias claras a la existencia o indexación de datos personales sobre una persona determinada y, en segundo lugar, si consta de suficientes y sofisticados mecanismos de búsqueda que puedan indicar exactamente dónde puede encontrarse un dato personal (sin necesidad de hacer una búsqueda manual).

Este derecho también extiende su aplicación a los correos electrónicos cuando contengan información personal pese a que esto supone muchos problemas prácticos dada la naturaleza de los correos electrónicos y los datos personales que incorporan, ya que en muchos casos éstos se almacenan en recodos oscuros de los sistemas tecnológicos así como en los mismos terminales, cuya propiedad está fuera del alcance de los responsables del tratamiento[275].

Otra de las cuestiones que ocasiona problemas prácticos es la determinación de qué se consideran datos personales. Si bien la ICO ha dispuesto en más de una ocasión que, toda la información personal que permita identificar a una persona puede considerarse dato personal, los tribunales con el caso *Durant* de nuevo, han limitado el contenido de los datos personales a aquella información biográfica significante y siempre y cuando el individuo sea el foco principal de dicha información.

Esto, sin duda, ha tenido un impacto muy negativo ya que, en la práctica muchas empresas, bajo el argumento de que los datos personales de los que disponen son relativos especialmente a una persona, declinan sistemáticamente solicitudes legitimas de acceso, criterios que han tenido que flexibilizarse por la ICO[276].

Por último, en cuanto a las consecuencias de no cumplir con este derecho, así como cuando, bajo falsos argumentos, los *data controllers* se nieguen a proporcionar información detallada de sus datos personales a los interesados, se prevén mecanismos específicos en la

[275] Sin embargo, los encargados del tratamiento deben buscar en todos los sistemas de archivo los correos electrónicos relevantes que contengan datos personales de aquél que lo solicite pese a que tales emails se hayan podido eliminar del ordenador o dispositivo electrónico del interesado, pues una copia debe quedar almacenada en el servidor de tal organización.

[276] El caso *Durant* ha sido tan relevante en relación con el derecho de acceso de los particulares que, en 2007, la ICO redactó una guía especificando todos los extremos de este derecho y su nueva configuración a través de las modificaciones introducidas por dicha sentencia, y ampliando nuevamente los márgenes de esta garantía.

DPA, que se examinarán posteriormente, y que básicamente consisten en la aplicación de sanciones por parte de la ICO.

ii. Right to prevent direct marketing

Recogido en la *Section* 11, constituye el derecho de cualquier particular a solicitar que cesen las actividades de marketing directo contra él o que ni siquiera tenga comienzo un procesamiento en cuanto a la publicidad se refiere. Este es uno de los derechos más controvertidos, pues son muchas las voces que sostienen que entra en conflicto con la libertad de empresa. Sin embargo, hay que tener presente que la ausencia de cualquier objeción a recibir marketing directo no implica que recibirlo sea lícito, pues por una parte, se prevé el derecho a no recibir publicidad directa cuando no se haya solicitado expresamente y, de haberse prestado el consentimiento necesario, la publicidad debe respetar todos y cada uno de los estándares legales previstos.

No es que la legislación británica prohíba como regla general las actividades de marketing directo sino que, puesto que el *data controller* tiene obligación de informar al interesado sobre toda actividad de procesamiento que se vaya a producir con sus datos (y el marketing directo constituye también procesamiento), el interesado tiene derecho a oponerse a cualquiera de estos procesamientos, por lo que puede también manifestar por escrito que no desea ser objeto de ninguna táctica publicitaria de este tipo, ni que sus datos se empleen para ello.

En cuanto al periodo para aplicar este derecho, la DPA omitió en su versión final el plazo máximo de 21 días que se manejaba en el anteproyecto y lo sustituyó por un periodo de tiempo "razonable" lo que, en la práctica, dilata enormemente la efectividad de este derecho llegándose incluso a omitir todo *feedback* una vez el sujeto solicita formalmente la finalización de toda actividad publicitaria para con él.

Este derecho de autoexclusión también debe ejercitarse por escrito, aunque no hay forma estándar a cumplimentar ni obligación por parte del *data controller* de contestar. En cuanto al marketing ejercido mediante correos electrónicos, es preceptivo como parte de las exigencias

de la DPA[277], que éstos consten con cláusulas de autoexclusión o direcciones a las que dirigir una petición para exceptuar el marketing directo del tratamiento y dejar de recibir comunicaciones publicitarias vía email. Lo mismo ocurre respecto del marketing vía SMS, donde deben necesariamente comprender el órgano al que dirigirse para darse de baja de las notificaciones.

En cuanto al marketing telefónico, para que una empresa pueda realizar dicha actividad, debe de estar registrada en el *Telephone Preference Service* (TPS), cuya subscripción debe renovarse anualmente. Esto ha permitido tener un mayor control respecto de las organizaciones dedicadas a ello, del mismo modo que ha posibilitado tomar acciones en contra de las llamadas publicitarias no solicitadas, lo que claramente supone una contravención de la ley británica y que, en consecuencia, comporta una sanción económica y, además, la publicación de ésta en la página web de la ICO.

También se tienen en cuenta las llamadas automáticas operadas por máquinas, cuyos receptores deben de haber prestado consentimiento previo y específico para este tipo de marketing, pues se trata de una forma de tratamiento de datos distinta a, por ejemplo, autorizar que un agente comercial le ponga al día de las ofertas de una empresa.

Sin embargo, se produce en la práctica de los correos electrónicos una excepción muy controvertida y es que, pese a no estar contemplada en la DPA, vendría autorizada por otra norma especial (la *PEC regulations* concretamente) consistente en la posibilidad de enviar publicidad no solicitada a una persona cuando ésta haya prestado su consentimiento para el marketing directo respecto de otros bienes o servicios similares del mismo *data controller*[278].

---

[277] En el famoso caso *Microsoft v. Paul McDonald, trading Bizads UK*, de 12 de diciembre de 2006 [2006] EWHC 3410 (Ch) All ER (D) 153, la compañía Microsoft, con la finalidad de proteger a sus usuarios de Hotmail frente al *spam* que recibían y que habían denunciado a los proveedores del servicio, creó cuentas con las que pudo demostrar ante los tribunales que sus clientes acababan incluidos en listas de *data controllers* a los que no habían prestado el consentimiento y de los que recibían acciones de marketing directo sin haberlo solicitado.

[278] El caso *Nigel Roberts v. Media Logistics* [2005] fue el primero en conceder una compensación económica a un sujeto de tratamiento no solicitado precisamente porque el demandante recibía emails publicitarios no solicitados de una empresa con la que no tenía relación contractual alguna previa aunque, sin embargo, la empresa demandada sí que tenía una relación comercial con otra empresa que sí que contaba con el consentimiento del demandado y entre ambas compañías, estaban intercambiándose datos personales de sus clientes.

Lo que, sin embargo, no quita que tengan la obligación de identificarse y de conceder cláusulas de autoexclusión de estos nuevos emails publicitarios.

La ICO ha interpretado extensivamente el concepto de marketing, incluyendo en él todas las actividades en las que no sólo se comuniquen ofertas de bienes y servicios sino también en los que se promueva la finalidad de una determinada organización o sus ideales. Esto incluye, por ejemplo, a asociaciones caritativas y a partidos políticos.

Esta normativa, dada su amplia temática, incluye una infinidad de normas británicas regulando distintos sectores colindantes como, por ejemplo, el *British Code of Advertising*, la *Sales Promotion and Direct Marketing* producida y ejecutada por el Committee of Advertising Practice o la *Consumer Protection form Unfair Trading Regulations 2008*, entre otras.

iii. Right to rectify inaccurate personal data, blocking, erasure and destruction

Es un derecho que surge como reacción a la vulneración del cuarto principio de la DPA que otorga a las personas facultades para solicitar la rectificación de sus datos personales cuando éstos son incorrectos o engañosos.

Para el ejercicio de este derecho se exige instar el procedimiento directamente en los tribunales donde además, puede ejercitarse conjuntamente o separadamente, la acción solicitando el borrado, bloqueo o la destrucción de los datos o de una información basada en datos erróneos. En el caso de ser estimado, los tribunales emitirán una orden de rectificación, bloqueo, borrado o destrucción.

A la hora de emitir su dictamen, los tribunales tendrán en cuenta los requerimientos derivados del cuarto principio, esto es, si los *data controller* han actuado con diligencia tomando todas las medidas necesarias en orden a cumplir la Ley. Si así lo estima, emitirá la orden correspondiente y, si por el contrario, concluye que se ha incumplido todo deber de diligencia, podrá imponérsele asimismo una obligación de compensar al interesado.

También puede instarse ante los tribunales una acción de compensación de daños y perjuicios provocados como consecuencia de una información inadecuada. Así ocurrió en el

caso *Wozencroft* [279] en el que un padre ejercitó esta acción en contra de dos informes en relación a su persona (datos personales) efectuados por el *data controller* (un psiquiatra) que eran incorrectos y que le perjudicaron en el régimen de custodia de sus hijos.

iv. Right to compensation

Cualquier persona que sufra un daño o un perjuicio como consecuencia de una vulneración de cualquier disposición de la DPA por parte de un *data controller*, tiene el derecho a exigir una compensación por ello.

"Daño" significa aquí, una pérdida económica (lucro cesante) y también un daño moral. Para su defensa el *data controller* debe de probar que ha actuado con la mayor diligencia posible, cumpliendo todos y cada uno de los mandatos de la DPA.

Este derecho debe ejercitarse frente a los tribunales ya que la ICO no tiene poder alguno para otorgar compensaciones a los afectados.

En cuanto a los perjuicios, en principio éstos sólo pueden reclamarse cuando se han producido como consecuencia del procesamiento de datos personales con "propósitos especiales" esto es, con fines periodísticos, artísticos o literarios. Aquí, el *data controller* también tiene que probar que cumplió con todas las exigencias legales. Sin embargo, existen algunos casos especiales en los que no haría falta que el procesamiento causante de los perjuicios se produzca específicamente por estos fines, siempre que el interesado pueda probar que los perjuicios se han sufrido efectivamente.

Los tribunales han aclarado que no procede derecho a una compensación cuando el daño producido es "general" como por ejemplo, la pérdida de la reputación de una persona[280]. En este caso, dichos efectos negativos deberían de reclamarse mediante la vía de la *defamation* prevista en el *common law*.

[279] *P. v. Wozencroft* [2002] 2 FLR 1118.

[280] *Johnson v. Medical Defence Union* [2007] EWCA Civ 262.

Es decir, se exige en todo caso una relación directa de causalidad entre el daño y los perjuicios producidos y la vulneración de la legislación en materia de protección de datos pues, en caso contrario, puede ser muy difícil para una persona probar, por ejemplo, las pérdidas económicas sufridas.

El caso paradigmático que ejemplifica el alcance de este derecho es el del matrimonio *Douglas*[281] que vio como una revista publicaba fotografías de su boda sin su consentimiento, motivo por el cual cursaron una reclamación y obtuvieron una compensación económica. El tribunal, sin embargo, entendió que los daños y perjuicios sufridos por los demandantes no se derivaban del incumplimiento de las disposiciones de la DPA, sino de los daños económicos producidos al romper el demandado la exclusiva que los demandantes habían concertado con otra revista, en relación con el derecho de explotación comercial de la propia imagen.

v. Right relating to automated decisions

Como parte de las obligaciones de los *data controller* se encuentra la determinación concreta de las situaciones en las que se produce un tratamiento automatizado y la comunicación a los interesados de esta circunstancia. Y es que toda persona tiene derecho, previa petición por escrito, a exigirle a un *data controller* que le asegure que ninguna decisión que le pueda afectar significativamente está basada excesivamente en un procesamiento automatizado de sus datos personales.

Este derecho está íntimamente ligado al derecho de acceso pues, la respuesta al requerimiento del interesado debe de contener no sólo qué datos personales son almacenados por una organización y con qué propósito, sino también si existe algún procedimiento de decisión automatizado en relación a éstos.

Para cumplir con esta obligación legal, la empresa, organización u administración pública requerida deberá comunicar al interesado si ha sido objeto de una decisión automatizada, así como el proceso que se ha llevado a cabo para su decisión final y el método

[281] *Michael Douglas & Catherine Zeta-Jones v. Hello! Ldt*, de 7 de noviembre de 2003 [2003] EWHC 2629 (Ch), Court Chancery Division.

(la lógica) en que se basa la misma. La DPA incluye algunos ejemplos: evaluando la candidatura a un puesto de trabajo, para la concesión de un crédito bancario, para determinar su fiabilidad, o incluso su conducta.

Ante la petición escrita del interesado, el *data controller* tiene la obligación de contestar y si lo hace negando la existencia exclusiva de tales procesos automatizados, durante los siguientes 21 días el interesado puede nuevamente dirigirse al *data controller* para pedirle que reconsidere la decisión tomada o realice una nueva evaluación, frente a lo cual éste tendrá un plazo de 21 días para contestar al sujeto de tratamiento -por escrito- detallando todos los pasos tomados para la valoración solicitada. Eso sí, la DPA prevé también excepciones[282] y, a diferencia del derecho de acceso, no se exige que la información que se proporcione al interesado sea comunicada de una manera inteligible.

Asimismo, si los *data controller* no cumplen con las obligaciones anteriores, los Tribunales podrán emitir una orden requiriendo al *data controller* que reconsidere la decisión o realice una nueva evaluación que no esté basada exclusivamente en un procesamiento automático.

vi. Right to prevent causing damage or distress

Los *data controller* no deben procesar datos personales cuando, al hacerlo, puedan provocar un daño o un perjuicio sustancial al sujeto objeto de tratamiento.

"Substancial" es un concepto jurídico indeterminado que no goza de definición alguna en la DPA, aunque la ICO ha dispuesto que basta con la mera causación de una pérdida, molestia, daño o sufrimiento real -sea cual sea el nivel de intensidad-, sin justificación alguna.

Si una persona cree que un *data controller* está llevando a cabo un procesamiento de este tipo o que, de otro modo, pueda causar daños y perjuicios, puede emitir por escrito una

[282] En la Sección 12.6 de la DPA existen ciertas excepciones legales por las cuales no se aplican las previsiones anteriores y, por tanto, se consideran "decisiones automatizadas exentas", como por ejemplo, cuando se haga para preservar los intereses legítimos del sujeto o para llevar a cabo el cumplimiento de un contrato.

"*notice*" al *data controller* para requerirle la paralización de dicho tratamiento en el plazo más breve posible.

Una vez recibida esta advertencia, el *data controller* tiene un plazo de 21 días para contestarle por escrito, bien negando que esté llevando a cabo un procesamiento en estos términos, o bien reconociendo los hechos y paralizando dichas actividades.

No obstante, un *data controller* puede continuar llevando a cabo este tipo de procesamientos cuando se den ciertas circunstancias como que el sujeto haya prestado, a sabiendas, su consentimiento expreso, cuándo éste sea necesario para cumplir con los términos de un contrato, o cuando sea necesario para proteger las necesidades vitales de un sujeto.

Encontramos ciertas similitudes con lo anteriormente explicado en el caso *Google Spain*[283] donde dicho buscador, al mostrar los resultados web en un orden determinado, estaba ocasionando un perjuicio sustancial al demandante, del que se mostraba cierta información personal y verdadera pero no relevante por el transcurso de tiempo, que afectaba a su credibilidad profesional, ocasionándole perjuicios económicos y daños morales.

Sin embargo, y debido al procedimiento previsto para la articulación de este derecho, entre todas las facultades concedidas por la legislación británica en protección de daños, ésta es la que menos se ejercita en la práctica pues, en primer lugar, tiene una aplicación limitada y, en segundo lugar, la mayoría de los interesados desconocen que tienen derecho a emitir una "*notice*" de estas características[284].

i) Garantías de cumplimiento de la Ley

i. Information Comissioner Officer (ICO)

La *Information Commissioner Officer* (ICO), creada a tenor de la *Data Protection Act 1984* bajo la denominación de *Data Protection Registrar*, se ratifica y se amplía en sus funciones con la *Data Protection Act 1998*.

[283] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

[284] CAREY. *Data Protection Handbook*, The Law Society, London, 2008, p. 259.

La ICO tiene como objetivo vigilar por el cumplimiento de los principios dispuestos en la DPA y, en su caso, será la encargada de imponer sanciones económicas. Así, se le atribuyen facultades para investigar si se han producido infracciones a la legislación en materia de protección de datos, bien de oficio bien a instancia de un interesado.

Además, cuenta con facultades para exigir que se haga pública determinada información (mediante una *information order*) así como para exigir que se hagan los cambios necesarios para que cese un procesamiento contrario a la Ley (a través de una *enforcement order*).

Sin embargo, cabe decir que, en la práctica, la ICO no suele emplear los instrumentos anteriores para exigir el cumplimiento de las normas sino que, en su lugar, se lleva a cabo un proceso más informal y sencillo consistente en obtener información de los *data controller* y lograr de éstos un consentimiento firmado de que van a adoptarse las medidas oportunas para cumplir con las disposiciones de la Ley. Estos compromisos se hacen públicos por la ICO y, hasta el momento, se han revelado como los mecanismos más efectivos a la hora de hacer cumplir la Ley

Cualquier persona puede dirigirse a la ICO y cumplimentar una solicitud de evaluación (*request for assessment*) si se cree afectado directamente por el procesamiento que un *data controller* está efectuando sobre sus datos personales[285]. En el caso de que esta solicitud prospere y se aprecien indicios de infracción, se comunicará al *data controller* el inicio de la investigación para esclarecer la situación. Si, a resultas de ésta se aprecian indicios criminales, la ICO iniciará acciones legales ante los tribunales, a los que remitirá los indicios resultantes de dicha investigación.

En cualquier caso, una vez haya tenido lugar la evaluación de la situación, la ICO tiene discrecionalidad para tomar o no acciones adicionales como puede ser, firmar un compromiso escrito con el *data controller* o bien emitir un aviso de ejecución (*Enforcement Notice*). En principio, los avisos que puede emitir la ICO no implican la obligatoriedad por parte del *data*

[285] No debe confundirse esta figura con la posibilidad de que la ICO evalúe el procesamiento de datos de un *data controller* con su consentimiento, previsto en el artículo s.51(7) de la DPA.

controller de tomar medidas pues no incluyen medidas coercitivas, se trata simplemente de dar cuenta pública acerca de la falta de adecuación a la Ley de las prácticas empresariales de cierto *data controller*. Sin embargo, si éste no cumple con la Ley en el periodo de tiempo que estipule la *notice*, ello podría constituir sanción penal.

En cualquier caso, la ICO puede llevar a cabo tres tipos de avisos, en primer lugar, las *Enforcement Notices*[286], mediante la cual la ICO informa al *data controller* que está vulnerando la Ley y le solicita que cese de procesar datos -en general- o ciertos datos, que cese en un tipo de procesamiento concreto, o bien que tome ciertas medidas para remediar la situación en el periodo de tiempo que se le estipule.

En segundo lugar encontramos las *Information Notices*[287], mediante la cuales se solicita al *data controller* que proporcione cierta información a la ICO sobre su actuación en tiempo y forma específica. Normalmente éstos avisos se suelen emitir cuando se ignoran los anteriores.

En tercer lugar, se prevén las *Special Information Notices*[288], mediante las cuales se busca información sobre el procesamiento realizado para fines especiales (periodísticos, artísticos o literarios), generalmente cuando se tiene la sospecha de que el procesamiento no se está llevando a cabo por estos motivos.

Cabe señalar además, que la ICO tiene facultades para entrar en el local de un *data controller* e inspeccionar[289]sus archivos siempre que tenga autorización judicial previa (salvo casos urgentes), cuando tras la solicitud de acceso al responsable, éste haya decidido no colaborar con la justicia y siempre que se tengan sospechas fundamentadas de contravención de la Ley. No obstante, antes de llegar a este extremo, la ICO puede llevar a cabo una evaluación del procesamiento de datos a un *data controller* con el consentimiento de éste, como una especie de auditoría consensuada.

---

[286] Schedule 40 (2), DPA.

[287] Schedule 43, DPA.

[288] Schedule 44, DPA.

[289] *Powers of entry and inspection*, Schedule 9, DPA.

ii. Notification

De acuerdo con la Directiva de 1995, toda actividad de procesamiento de datos debía de estar registrada previamente por la autoridad nacional correspondiente. En Reino Unido, esta actividad de control le corresponde a la ICO que es quien lleva a cabo el registro de los *data controllers*[290].

De esta forma, toda persona que tenga la intención de procesar datos personales debe informar de ello a la ICO. La DPA llama *notification* al proceso obligatorio mediante el cual un *data controller* le proporciona a la ICO todos los detalles de su futura actividad[291]. Una vez este registro se lleva a cabo, previo pago de una tasa, la ICO hace pública su inscripción en el *register of data controllers* con el propósito de que dicha información sea accesible a cualquier persona que pueda resultar interesada.

A pesar de que los encargados del tratamiento, salvo excepciones, estén obligados a notificar sus actividades a la ICO pueda verse como un proceso formal, esto no supone en modo alguno la obtención de una licencia para realizar sus actividades ni tampoco que éstas estén dotadas de garantías suficientes.

No obstante, este proceso sólo debe llevarse a cabo cuando los datos personales objeto del tratamiento encajen dentro de los parámetros de la Ley, es decir, ser o estar destinados a ser procesados automáticamente. Del mismo modo, el procesamiento manual de datos, a pesar de que éstos encajen con la definición de la DPA, no está sujeto a notificación.

En cuanto al resto de supuestos, deben notificarse previamente a la ICO siempre y cuando no incurran en las siguientes excepciones por:

a) Motivos domésticos (personas individuales que procesen datos personales en el ámbito personal o familiar y con éstos mismos propósitos).
b) Motivos de seguridad nacional.

[290] Este proceso de notificación sustituye el sistema de registro dispuesto en la *Data Protection Act 1984*.

[291] La omisión de este proceso conlleva la imposición de sanciones por parte de la ICO.

c) Registros públicos.

d) Administración de personal (como información relativa a nóminas, nombramientos, despidos, sanciones disciplinarias, citas, etc.).

e) Publicidad, marketing y relaciones públicas del *data controller* en relación a sus actividades y siempre y cuando éste no se dedique a actividades de marketing con una tercera empresa.

f) Libros de cuentas y registros de una empresa (por ejemplo, el registro de los proveedores o de los clientes).

g) Organizaciones sin ánimo de lucro, cuando el propósito del tratamiento sea mantener a los socios o al apoyo a la organización.

h) De acuerdo con otras finalidades públicas (por ejemplo, por orden de un Juez o en cumplimiento de la Ley).

Salvo estas excepciones, el procesamiento de datos personales sin haber llevado a cabo el proceso de notificación ante la ICO supone la comisión de un delito[292], asimismo ocurrirá en el caso de que se haya producido un cambio en la actividad de procesamiento sin haberlo comunicado a dicho organismo.

iii. Privacy Impact Assessments (PIA)

Las *Privacy Impact Assessments* (PIA en adelante) son un instrumento válido para evaluar los riesgos que un determinado sistema, producto o servicio puede repercutir para la protección de datos, con el objetivo de minimizar su impacto[293].

A pesar de que la *Data Protection Act 1998* no obliga a las organizaciones a llevar a cabo medidas PIA, la ICO, así como otros autoridades europeas de protección de datos, han promovido las PIA como herramientas útiles para ayudar a las organizaciones a asegurarse de

[292] Section 21 (1), DPA.

[293] Este instrumento ha sido incorporado al Reglamento europeo de Protección de Datos, en su artículo 35, bajo la denominación "evaluación de impacto relativa a la protección de datos".

que están cumpliendo los estándares en materia de protección de datos y evitar así ciertas prácticas empresariales que puedan poner en riesgo los datos personales.

Las PIA son un instrumento adecuado para llevar a cabo en todo tipo de procesamientos de datos personales, no sólo aquéllos que se llevan a cabo por las nuevas tecnologías. Del mismo modo, tampoco están reservadas a actividades nuevas sino que pueden llevarse a cabo en empresas con años de actividad a sus espaldas para examinar cual es el nivel de garantía y cumplimiento actual.

Sin embargo, debe tenerse claro que las PIA sólo son un instrumento adicional que de ningún modo puede sustituir los mecanismos jurídicos más efectivos para garantizar, en última instancia, el cumplimiento legal de las disposiciones. Asimismo, las PIA deben entenderse como un arma que ayuda a fomentar la privacidad desde el diseño, permitiendo a las organizaciones calibrar los potenciales riesgos para la privacidad que pueden conllevar sus prácticas empresariales y ayudarles a garantizar su cumplimiento[294].

Es decir, en el fondo, se trata de una especie de códigos de conducta llevados a cabo por las empresas que manejan datos personales, elaborados en estrecha colaboración con la ICO[295]. No existe un borrador estándar de PIA sino que éste se elabora en función de las necesidades de la empresa que lo lleva a cabo, aunque se pueden diferenciar algunas fases comunes a todos los procesos: 1) Determinar si es necesario un PIA y porqué, 2) Examinar las actividades de procesamiento de datos personales, 3) Identificar los riesgos existentes para la privacidad, 4) Proponer estrategias para mitigar el impacto negativo en la privacidad, 5) Informar e implementar las recomendaciones adoptadas y 6) Hacer una revisión o una auditoria de la implementación llevada a cabo.

iv. Information Tribunal

Igual que establece la continuidad de la *Information Commissioner Officer* (ICO), la *Data Protection Act 1998* instituye que el *Data Protection Tribunal* (ahora *Information*

[294] CAREY. *Data Protection: a practical Guide to UK and EU Law*, Oxford University Press, Oxford, 2015, p. 298.

[295] Con éste objetivo la ICO publicó en febrero de 2014, el *Code of Practice on Conducting Privacy Impact Assessments*.

Tribunal) continúe desempeñando las funciones que ya venía ejerciendo al amparo de la anterior normativa en materia de protección de datos, eso sí, con ciertos cambios respecto a sus jurisdicción[296]. De hecho, con la ampliación de sus competencias a raíz de la aprobación de las *Freedom of Information Act 2000*, la *Privacy and Electronic Communications Regulations 2003* y la *Environmental Information Regulations 2004*, pasó a llamarse *Information Tribunal*, denominación más acorde con su nueva jurisdicción[297][298].

En cualquier caso, sigue siendo el Tribunal ante el que, cualquier afectado, puede recurrir una decisión del ICO o presentar una reclamación si se le deniega el acceso a la información solicitada.

En cuanto a los datos personales, y salvo los casos relacionados con la seguridad nacional[299], los recursos pueden presentarse en contra de:

a) Un aviso de cumplimiento o una nota informativa de la ICO.

b) Una denegación por parte de la ICO de cancelar una notificación de cumplimiento de la ley.

c) Una decisión de la ICO consistente en un aviso de ejecución o de incumplimiento de la ley.

d) Una decisión de la ICO que disponga que los datos no se están procesando con fines especiales o con fines periodísticos, literarios o artísticos cuando no haya sido publicado previamente por el *data controller*.

[296] BAINBRIDGE. *Data Protection Law*, XPL publishing, Great Britain, 2005, p. 240.

[297] En la actualidad, además de la protección de datos, el *Information Tribunal* tiene competencias en libertad de información, privacidad y las comunicaciones electrónicas e información ambiental.

[298] Conviene señalar que, tras una reordenación general del sistema jurisdiccional del Reino Unido en 2010, el Tribunal ha pasado de ser un órgano independiente no adscrito a formar parte del *General Regulatory Chamber of the First-tier Tribunal*.

[299] Estos supuestos siguen un procedimiento diferente basado en la inexistencia de publicidad de su contenido y en la intervención forzosa de un *Minister of the Crown*. El grueso de su contenido no se explica aquí por razones de extensión,

Los tres primeros casos pueden presentarse por la persona a la que se le ha notificado la *notice* pese a que el derecho a recurrir pertenece al *data controller* en cuya determinación se ha dispuesto la resolución[300].

Los plazos para recurrir finalizan transcurridos 28 días después de la notificación de la decisión de la ICO y el procedimiento a seguir viene determinado por leyes especiales[301] que, en la actualidad, han agilizado este procedimiento hasta el punto de poder iniciarse mediante un formulario estándar vía online.

En cuanto a la sustentación del procedimiento, nos limitamos a comentar un par de aspectos. En primer lugar, que el Tribunal puede tomar una decisión sin convocar a las partes a una audiencia cuando no lo considere necesario. En segundo lugar, esclarecer que el Tribunal puede admitir el recurso, sustituir una *notice* si considera que ésta no es conforme a Derecho o es objeto de una decisión arbitraria por parte de la ICO, cancelar o variar su contenido, o declarar ineficaces algunas de sus actuaciones. Esta resolución judicial del *Information Tribunal* podrá ser, asimismo, objeto de recurso de apelación.

v. Sanciones penales

Conforme a lo dispuesto en la *Data Protection Act 1998*, el tratamiento de datos sin previa notificación a la ICO así como el cambio sustancial de las circunstancias[302] sin comunicación de antemano, comportan una infracción penal.

Cuando se sospecha sobre la comisión de una infracción penal, la ICO[303] abre una investigación para esclarecer las circunstancias, produciéndose una visita a las instalaciones del *data controller* para analizar cómo se está llevando a cabo el procesamiento de datos. Acto

[300] Un recurso puede interponerse por cualquier persona directamente afectada cuando verse sobre la emisión de un certificado en aras a la excepción de seguridad nacional.

[301] *The Data Protection Tribunal (Enforcement Appeals) Rules 2000*.

[302] Los cambios deben comunicarse con un máximo de 28 días para no constituir infracción penal.

[303] Conviene recordar aquí que la ICO es una "*prosecuting authority*" por ella misma, lo que implica que puede instar un procedimiento penal en caso de que se haya producido alguna de las causas previstas en la Ley además, por supuesto, del Ministerio Fiscal.

seguido, en función del tipo de indicios, el procedimiento puede sustanciarse sumariamente por la propia ICO o bien, directamente ante los Tribunales.

Las infracciones que se puedan cometer frente a la DPA son sancionables generalmente con una multa pecuniaria aunque hay delitos por los que además, si así lo consideran los Tribunales, pueden conllevar confiscación, destrucción o borrado de material que contenga datos personales o que haya sido usado para su procesamiento fraudulento[304].

Estos hechos delictivos son de diversa índole y no están sistematizados en la DPA sino que se deducen de preceptos aislados, sin embargo, pueden estructurarse en la siguiente enumeración: llevar a cabo un procesamiento sin previa notificación a la ICO, omitir a la ICO cambios en el procesamiento autorizado de datos (cambios en los datos registrables, en las técnicas empleadas, en las medidas de seguridad, etc.), obstruir la ejecución de una garantía por la ICO (de entrada e inspección, por ejemplo), cuando se haga caso omiso a un aviso (*notice*) de la ICO o bien se conteste a éste con una declaración falsa -ya sea a sabiendas o imprudentemente-, cuando los datos personales se obtengan, se hagan públicos o se vendan mediante métodos contrarios a Derecho; cuando se procesen datos prohibidos de acuerdo con la legislación laboral, cuando el procesamiento de datos pueda causar daños o perjuicios en los interesados y no se cuente con la preceptiva evaluación de la Secretaria de Estado, cuando no se conteste en el periodo preceptivo -21 días desde su recepción- a una solicitud de un particular sobre los detalles del tratamiento de sus datos, o, cuando se haga pública -a sabiendas o imprudentemente- información proporcionada por la ICO acerca de una persona individual o una empresa, cuando ésta no sea accesible de otro modo[305].

En cuanto a los sujetos susceptibles de ser sancionados encontramos -como no podía ser de otro modo- al *data controller*, que puede ser tanto una persona física como una persona jurídica y, además, a cualquier empleado de un *data controller* con responsabilidad en la empresa (director, gerente, secretario general…) cuando el tratamiento de datos fraudulento se

[304] Esto puede acarrear el borrado íntegro de los discos duros de una empresa así como de sus archivos físicos y, en muchas ocasiones, puede suponer el borrado íntegro de todas sus bases de datos.

[305] CAREY. *Data Protection Handbook*, The Law Society, London, 2008, pp. 49-55.

haya llevado a cabo con su consentimiento, connivencia o debido a su negligencia, así como cualquier persona que haya ayudado, instigado, aconsejado o procurado la comisión de dicho delito.

vi. Sanciones civiles

La ICO también tiene competencias en el ámbito de la responsabilidad civil cuando se produce una infracción de la legislación de protección de datos. La *Data Protection Act 1998* dispone expresamente la posibilidad de que, cualquier persona que sufra daños o perjuicios por cualquier actuación contraria a la Ley, tendrá derecho a una compensación por parte del *data controller*[306].

Como ya se ha dicho antes, la ICO dispone de amplias facultades de investigación, que puede iniciar bien a instancias de una reclamación, bien por iniciativa propia[307]. Cualquier persona puede poner en conocimiento de la ICO, mediante una queja o una reclamación, la existencia de un procesamiento ilegal de datos, sin que sea necesario tener un interés legítimo en el mismo o estar directamente afectado por éste.

Para obtener compensación por daños y perjuicios, el interesado deberá dirigirse contra el responsable del tratamiento de datos o contra la ICO y, en ciertas ocasiones, se será preceptivo interponer demanda ante los Tribunales[308]. Sin embargo, cabe decir que los casos en

[306] Schedule 13, DPA: "*(1) An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of this Act with certain is entitled to compensation from the data controller for that damage. (2) An individual who suffers distress by reason of any contravention by a data controller of any of the requirements of this Act is entitled to compensation from the data controller for that distress if— (a) the individual also suffers damage by reason of the contravention, or (b) the contravention relates to the processing of personal data for the special purposes. (3) In proceedings brought against a person by virtue of this section it is a defence to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned*".

[307] Sin embargo, en la práctica, parece que la actuación de la ICO es más bien reactiva que proactiva, pues como demuestra su trayectoria, ésta suele actuar a raíz de las quejas presentadas por particulares.

[308] Destacan entre otras, aquéllas ocasiones en las que exista cierta urgencia en el procedimiento, o cuando el daño económico producido sea muy elevado o bien cuando el caso ya haya sido investigado por la ICO pero el particular no esté conforme con el resultado.

los que se ha otorgado una indemnización por daños y perjuicios a resultas de un procedimiento de este tipo son más bien escasos, así como las cuantías satisfechas por este motivo[309].

Por otro lado, y mediante un aviso de multa llamado *Monetary Penalty Notices*[310], la ICO puede, desde mayo de 2008, imponer sanciones pecuniarias cuando se produzca una infracción grave de la legislación en materia de protección de datos que, sin embargo, no sea constitutiva de delito. Este procedimiento, instado más frecuentemente, requiere para su imposición que se haya contravenido la DPA y que con ello se hayan causado daños sustanciales, ya sea de forma deliberada o cuando el *data controller* tenia obligación legal de haber sabido que no estaba actuando conforme a la Ley.

vii. Otros mecanismos de control

Cuando la ICO no considere adecuado adoptar medidas de ejecución, puede optar por acordar compromisos escritos con aquellas organizaciones que, sin contravenir la Ley, lleven a cabo un procesamiento de datos peligroso para los interesados. Es una especie de código de buenas prácticas, que se hace público por la ICO, en el que se incluyen las medidas a tomar para mejorar la situación de un determinado organismo, con la esperanza de que así sea, al menos, debido a la presión mediática de dicha empresa por mantener su buena reputación.

En términos generales, la ICO también ha publicado numerosos códigos de buenas prácticas que, pese a no tener ningún efecto legal, tratan de promover el respeto a la legislación en materia de protección de datos por parte de los responsables de su tratamiento. Además de la ICO, otras agencias británicas han publicado códigos y guías para el procesamiento de datos en su ámbito regulador específico, como por ejemplo, en materia de publicidad[311].

---

[309] En el popular caso *Campbell v. Mirror Group Newspapers Ldt* [2002] EWHC 499 (QB), la modelo obtuvo una compensación por daños de 2.500£ por haberse publicado unas fotos suyas recibiendo tratamiento contra sus adicciones; peor parado salió el matrimonio Douglas cuando se publicaron las fotos de su boda sin su consentimiento y, en primera instancia, que sólo vieron reconocidos sus daños y perjuicios con 100£ en *Michael Douglas & Catherine Zeta-Jones v. Hello! Ldt*, de 7 de noviembre de 2003 [2003] EWHC 2629 (Ch), Court Chancery Division.

[310] Schedule 55, DPA.

[311] Entre otros, el *British Code of Advertising, Sales Promotion and Direct Marketing* (CAP) publicado por el *Committee of Advertising Practice*.

Por último, aquellos *data controllers* que están exentos de la obligación de notificar su actividad a la ICO[312] pueden, voluntariamente, comunicarle su labor y sus circunstancias. Ahora bien, una vez lleven a cabo esto, se adscriben al régimen general de las notificaciones, incluyendo la obligatoriedad de pagar las tasas y de avisar sobre cualquier cambio en el procesamiento de datos. Si bien a simple vista, no parece un buen negocio para los *data controllers* vincularse voluntariamente a este régimen, en caso de hacerlo así, no les será de aplicación el deber de divulgación previsto en el DPA para el resto de *data controllers*[313], motivo por el cual se explica el gran éxito de dicha práctica.

j) Exenciones al procesamiento de datos atendiendo a la protección de derechos subjetivos

Frente a todas las exigencias y obligaciones que la normativa británica exige respecto del tratamiento de los datos personales, hay algunas salvedades incluidas en la legislación debidas, principalmente, a los derechos de los sujetos objeto del tratamiento sobre tipos específicos de procesamiento, y no tanto a causa de la tipología de los datos en cuestión.

La Directiva del 95 contempló algunas excepciones y otorgó amplios poderes a los Estados miembros para que creasen sus propias prerrogativas. En el caso británico el grueso de éstas viene regulado en la Parte IV de la DPA[314], autorizando, según el caso concreto, el incumplimiento de una o varias disposiciones de la DPA.

Para una lectura más liviana se ha convenido sistematizar dichas exenciones en la siguiente enumeración:

1. Seguridad Nacional
2. Delito y fiscalidad

[312] Por ejemplo, por procesar datos manualmente o por poseer datos personales con la finalidad de mantener actualizado un registro público.

[313] Los *data controllers* tienen, como regla general, la obligación de contestar en el plazo de 21 días a los requerimientos formulados por particulares respecto de los pormenores del procesamiento de sus datos conforme a la Section 24 de la DPA.

[314] Aunque también se contemplan en el Schedule 7 (como las referencias confidenciales) e incluso se han dispuesto en la legislación especial como por ejemplo, la *Data Protection (Subject Access Modification) (Social Work) Order 2000*.

3. Salud
4. Educación
5. Trabajo social
6. Actividad reguladora
7. Periodismo, literatura y arte
8. Investigación, historia y estadística
9. Autoridades públicas, designaciones de funcionarios, ministeriales y de la casa real
10. Privilegios parlamentarios
11. Registros públicos
12. Inspección pública
13. Finanzas
14. Divulgación exigidas por la Ley
15. Referencias confidenciales
16. Fuerzas armadas
17. Asesoramiento legal[315] y procedimientos jurídicos
18. Patria potestad, adopciones, procedimientos de fertilización y embriología
19. ONGs
20. Propósitos domésticos

En cuanto a los procedimientos de los que están exentos, como ya se ha dicho, éstos varían en función del caso concreto, sin embargo, pueden diferenciarse dos tipologías distintas de exenciones. En primer lugar, aquellos casos en los que no resulta obligatorio registrarse con la ICO a efectos de notificarle el tipo de actividad de tratamiento que se realiza, sus garantías o sus cambios, lo que exime también de pagar las tasas correspondientes.

[315] Muchos de estos extremos han necesitado de una interpretación por parte de la jurisprudencia como es el caso de los datos facilitados para sustentar un procedimiento judicial en defensa de intereses legítimos o para obtener asesoramiento legal. Los tribunales han dispuesto que, pese a que el *data controller* tome la determinación de hacer públicos ciertos datos personales argumentando la existencia de "legítimos intereses" eso no se aplica como regla general, pues es perfectamente posible rechazar ese argumento cuando una información es privada y confidencial. Veáse por todos, *Totalize Plc v. The Motley Fool Ltd* [2002] 1 WLR 1233.

En segundo lugar, aquellos casos por los cuales los *data controller* no tienen obligación de facilitar el acceso a los pormenores del tratamiento a los interesados. Es una excepción a la regla general por la cual toda persona tiene derecho a dirigirse al responsable del tratamiento y exigirle detalles acerca de sus datos, ante lo cual, el *data controller* debe responder en un plazo máximo de 21 días.

En definitiva, la DPA prevé que, concurriendo determinadas circunstancias, existan ciertas dispensas al deber de cumplimiento íntegro de la Ley. Estas dispensas se dan en dos direcciones, bien restringiendo ciertos derechos de las personas en relación con el procesamiento de sus datos personales, bien limitando los deberes de las organización al procesar dichos datos[316]. Ambas circunstancias pueden darse conjuntamente o aisladamente, por lo que hay que examinar cada caso en concreto.

k) Outsourcing. Subcontratación en el procesamiento de datos

Es una práctica muy frecuente que las empresas subcontraten muchas de las actividades que deben desempeñar en su día a día, desde el mantenimiento de su página web hasta la gestión de residuos, por ejemplo. Los datos personales también son objeto de subcontratación en distintas ocasiones, como puede ser su mero almacenamiento o bien su propio procesamiento, en cuyo caso surgen ciertas obligaciones legales.

Una vez dicha externalización de servicios se produce, la legislación británica denomina *outsourcing organization* al *Data controller* -cuando éste actúa como cliente- y *Data processor*[317] o tercera parte, al proveedor de dicha actividad de procesamiento al cual ha subcontratado.

Conviene recordar aquí que sólo los *data controller* están obligados bajo la DPA a cumplir con la legislación en materia de protección de datos, mientras que los *data processor*

[316] Estas dos tipologías son denominadas por la doctrina como "*subject information provisions*" y "*non-disclosure provisions*". CAREY. *Data Protection Act 1998*, Blackstone Press Limited, London, 1998, p. 52.

[317] Section 1(1) DPA: "*Any person (other tan an employee of the data controller) who processes personal data on behalf of the data controller*". La Directiva del 95, sin embargo, disponía expresamente que éste podría ser una persona física o jurídica, una autoridad pública, una agencia o cualquier otro tipo de organización (artículo 2. e). En cualquier caso, también cabe la posibilidad de que el *data processor* forme parte del mismo grupo empresarial que el *data controller*.

no, pese a que tienen la obligación legal-contractual de cumplir con la normativa respecto del procesamiento que lleven a cabo en nombre de los responsables del tratamiento y, además, están sujetos a la Ley en relación al tratamiento de datos efectuado para sus propios fines (respecto de sus empleados o sus clientes, por ejemplo).

Esto implica que, los *data controller* serán responsables en última instancia de cualquier vulneración de la Ley causada por las acciones u omisiones que lleven a cabo las empresas a quienes han externalizado el procesamiento (los *data processor*). Sin embargo, la Directiva del 95 obliga a toda empresa externa que preste dichos servicios a formalizar un contrato con el responsable del tratamiento a fin de comprometerse a cumplir las disposiciones en materia de protección de datos así como a tomar las medidas oportunas para lograrlo.

En cuanto a la actividad de tratamiento subcontratada, ésta puede consistir en una gran variedad de formas aunque, sin embargo, todas ellas tienen en común el procesamiento de información personal por el *data processor* en nombre del *data controller*. En algunos casos, la subcontratación puede conllevar también la transferencia de datos desde el *data controller* hacia el *data processor*, pese a que dicha circunstancia no es indispensable en la relación entre ambos.

También puede ocurrir que, con motivo de una finalidad concreta (una operación de marketing, por ejemplo), un *data processor* procese información proporcionada por distintos *data controller* sin que esto altere las relaciones contractuales de todos los implicados, pues cada *data controller* será responsable del tratamiento de los datos obtenidos por él mismo, así como del tratamiento que se haga de éstos por la empresa subcontratada.

A veces, resulta difícil distinguir entre un *data processor* y un *data controller*, cosa que resulta de gran importancia dado el diferente régimen jurídico al que están sometidos unos y otros, motivo por el cual algunas organizaciones prefieren ser clasificadas como empresas de procesamiento y no como responsables del mismo[318]. Sin embargo, el grado de autonomía es

[318] Esto ocurre, por ejemplo, con el *cloud computing* -"la nube"-, dónde los prestadores de servicios en este espacio son, habitualmente, *data processors,* pues en sus servidores se almacenan grandes cantidades de datos personales. En otros casos, sin embargo, se convierten en *data controllers* al hacer uso de esa información que almacenan.

sustancialmente distinto en uno y otro caso por lo que, a la hora de clarificar esta distinción, ayuda recordar que la entidad de procesamiento no puede utilizar los datos de los que dispone para sus propios propósitos, sino que actúa conforme a lo estipulado por contrato con el responsable del tratamiento.

Por último, destacar que cuando la compañía a la que se le subcontrata el procesamiento está localizada fuera del Área Económica Europea[319] y la subcontratación comporte una trasferencia de datos desde un *data controller* situado en Reino Unido, la DPA exige[320], de acuerdo con la legislación europea y tal y como se ha expuesto anteriormente, una serie de requerimientos adicionales para legalizar esta actividad de exportación de datos[321].

2.5. Normativa accesoria y modificaciones en la legislación británica como consecuencia de la entrada en vigor del Reglamento Europeo de Protección de Datos

En los apartados anteriores se ha intentado exponer una panorámica general del sistema británico de protección de los datos personales, como un primer paso a la salvaguarda del derecho a la privacidad, sistematizando dicho análisis conforme a lo dispuesto por las sucesivas normas reguladoras, la pionera *Data Protection Act 1984* y la *Data Protection Act 1998*, que revocó la anterior y que estaba en vigor en el momento de redactar este Capítulo.

Sin embargo, la DPA no es el único *statutory instrument* con influencia en la materia, junto a ella, ha habido infinidad de normas que, aunque parcialmente y de forma incidental, han incidido en este núcleo de protección, ya sea por iniciativa británica como por exigencia europea[322].

---

[319] Es una práctica empresarial muy recurrente subcontratar las oficinas de atención telefónica al cliente, denominadas *call centers*, a empresas ubicadas en otros países como la India –en el caso de Reino Unido- o América Latina – en el caso de España-.

[320] Chapter 8.

[321] En el caso de que se use el método de las cláusulas contractuales estandarizadas, la DPA permite que éstas puedan asimismo legitimar las disposiciones comprendidas en los principios 1 (poniendo en conocimiento del interesado los detalles de los acuerdos de exportación), 7 (ofreciendo seguridad para los datos más el requerimiento de contar con acuerdos contractuales apropiados con los procesadores de datos) y 8 (restricciones en la exportación de datos) de su articulado.

[322] Destacan, entre ellas, La *Computer Misuse Act 1990* (en la actualidad, derogada parcialmente, dispone garantías para la protección de material y equipos informáticos contra el acceso no autorizado), la *Freedom of Information Act 2000* (estipula la obligación de ciertas autoridades públicas de hacer pública una determinada información, modifica parcialmente la DPA),

Del mismo modo, no pueden obviarse otras herramientas legales que, aunque a veces de forma tangencial, ofrecen protección a esta cuestión y cuyo examen se remite a apartados posteriores, principalmente algunas figuras clásicas del *common law* británico -como la *breach of confidence* o la *nuisance*- que se han venido empleando ininterrumpidamente por la jurisprudencia[323] y, en mayor medida, la *Human Rights Act 1998*, que supuso un giro radical en la materia.

En el plano más inmediato, es obligado hacer mención al Reglamento Europeo de Protección de Datos Personales 2016/679 (GDPR por sus siglas en inglés), directamente aplicable a los Estados miembros, cuyos principios y articulados han cambiado las reglas del juego en materia de protección de datos.

La unificación de criterios ha sido uno de los motivos principales de creación de dicho instrumento regulador, de hecho, sólo en el Reino Unido, hasta el momento de promulgarse el

---

la *Anti-Terrorism Crime and Security Act 2001* (muy controvertida por cambiar los parámetros generales de la legislación británica a tenor de los recientes acontecimientos terroristas, por ejemplo, al considerar delito no divulgar información a un agente policial cualquier información que podría prevenir un acto de terrorismo o asegurar la aprehensión, enjuiciamiento o condena de otra persona en el Reino Unido por cualquier acción relacionada con el terrorismo), la *Electronic Commerce (EC Directive) Regulations 2002* (en relación con la anterior, implementa la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior), la *Privacy and Electronic Communications (EC Directive) Regulations 2003* (conocida como PEC, incorpora un sistema de control de datos idéntico al concebido por la DPA, otorgando a la ICO la potestad principal para hacer cumplir la Ley, y estableciendo un derecho a la compensación incluso para las personas jurídicas – a raíz de la sentencia *Microsoft Corporation v. Paul McDonald (trading as Bizads UK)* [2006] EWHC 3410-. Esta norma implementó la Directiva 2002/58/EC cuya finalidad es mitigar el impacto negativo en el estándar de privacidad causado por las nuevas tecnologías como el email o las cookies), la *Defamation Act 2013* (estatuto complementario a la figura clásica de la *defamation* del *common law*, instrumento principal para combatir los ataques a la reputación y al honor), la *Criminal Justice and Data Protection (Protocol nº 36) Regulations 2014* (mediante esta Ley se transpuso la Decisión del Consejo -Decisión Marco 2008/977/JAI del Consejo de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal- sobre el marco de cooperación europeo policial y judicial en el procesamiento de los datos personales en asuntos criminales), la *Investigatory Powers Act 2016* (sustituye a la controvertida *Data Retention Regulation and Investigatory Powers Act 2014* –DRIPA- que se derogó a raíz de una sentencia del TJUE – Gran Sala, 8 de abril de 2014, *Digital Rights Ireland Ltd v. Minister for Communications and Others; Kärntner Landesregierung v. Michael Seitlinger and Others,* asuntos acumulados C-293/12 y C-594/12- que consideraba que constituía "una injerencia de gran magnitud y especial gravedad" en los derechos fundamentales a la privacidad y a la protección de datos), o la *Money laundering regulations 2017* (transpone la Directiva 2015/849 de 20 de mayo de 2015 relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales, mediante ésta los despachos de abogados quedan obligados a poner en conocimiento de las autoridades aquellas actividades relacionadas con el blanqueo de dinero y les impide asesorar a un cliente cuando se tiene la convicción de que está preparándose para cometer un acto delictivo, incluidos aquellos previstos bajo las disposiciones de la DPA).

[323] Cfr. FENWICK/PHILLIPSON. "Breach of Confidence as a Privacy Remedy in the Human Rights Act Era", en *Modern Law Review*, nº 63, 2000.

Reglamento, estaban en vigor 40 normas distintas entre Reglamentos, Directivas y otras normas con fuerza jurídica vinculante, en materia de protección de datos[324].

En cierto modo, el Reglamento pretende acabar con la disparidad legislativa, intentando unificar el mayor numero posible de normativa sectorial al respecto. Y al hacerlo, ha

---

324

1. The Data Protection Act 1998 (Commencement) Order 2000 (SI 2000/183)
2. The Data Protection (Corporate Finance Exemption) Order 2000 (SI 2000/184)
3. The Data Protection (Conditions under Paragraph 3 of Part II of Schedule 1) Order 2000 (SI 2000/185)
4. The Data Protection (Functions of Designated Authority) Order 2000 (SI 2000/186)
5. The Data Protection (Fees under section 19(7)) Regulations 2000 (SI 2000/187)
6. The Data Protection (Notification and Notification Fees) Regulations 2000 (SI 2000/188)
7. The Data Protection Tribunal (Enforcement Appeals) Rules 2000 (SI 2000/189)
8. The Data Protection (International Co-operation) Order 2000 (SI 2000/190)
9. The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000 (SI 2000/191)
10. The Data Protection Tribunal (National Security Appeals) Rules 2000 (SI 2000/206)
11. The Consumer Credit (Credit Reference Agency) Regulations 2000 (SI 2000/290).
12. The Data Protection (Subject Access Modifications) (Health) Order 2000 (SI 2000/413)
13. The Data Protection (Subject Access Modifications) (Education) Order 2000 (SI 2000 414)
14. The Data Protection (Subject Access Modifications) (Social Work) Order 2000 (SI 2000/415)
15. The Data Protection (Crown Appointments) Order 2000 (SI 2000/416)
16. The Data Protection (Processing of Sensitive Personal Data) Order 2000 SI 2000/417)
17. The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 (SI 2000/419)
18. The Data Protection Tribunal (National Security Appeals) (Telecommunications) Rules 2000 (SI 2000/731)
19. The Data Protection (Designated Codes of Practice) (Nº 2) Order 2000 (Si 2000/1864)
20. The Data Protection (Miscellaneous Subject Access Exemptions) (Amendment) Order 2000 (SI 2000/1865)
21. The Data Protection (Notification and Notification Fees) (Amendment) Regulations 2000 (SI 2001/3214)
22. The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) (Amendment) Regulations 2001 (Si 2001/3223)
23. The Information Tribunal (Enforcement Appeals) (Amendment) Rules 2002 (SI 2002/2722)
24. The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) Order 2002 (SI 2002/2905)
25. The Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations 2004 (SI 2002/2905)
26. The Information Tribunal (National Security Appeals) Rules 2005 (SI 2005/13)
27. The Information Tribunal (Enforcement Appeals) Rules 2005 (SI 2005/14)
28. The Information Tribunal (Enforcement Appeals) (Amendment) Rules 2005 (SI 2005/450)
29. The Data Protection (Subject Access Modification) (Social Work) (Amendment) Order 2005 (SI 2005/467)
30. The Data Protection (Processing of Sensitive Personal Data) Order 2006 (SI 2006/2068)
31. The Data Protection Act 1998 (Commencement Nº 2) Order 2008 (SI 2008/1592)
32. The Data Protection (Notification and Notification Fees) (Amendment) Regulation 2009 (SI 2009/1677)
33. The Data Protection (Processing of Sensitive Personal Data) Order 2009 (SI 2009/1811)
34. The Data Protection (Monetary Penalties) (Maximum Penalty and Notices) Regulations 2010 (SI 2010/31)
35. The Tribunal Procedure (Amendment) Rules 2010 (SI 2010/43)
36. The Data Protection (Monetary Penalties) Order 2010 (SI 2010/910)
37. The Data Protection (Processing of Sensitive Personal Data) (Elected Representatives) (Amendment) Order 2010 (SI 2010/2961)
38. The Data Protection Act 1998 (Commencement Nº 3) Order 2011 (SI 2011/601)
39. The Data Protection (Subject Access Modification) (Social Work) (Amendment) Order 2011 (SI 1034/2011)
40. The Data Protection (Processing of Sensitive Personal Data) Order 2012 (SI 2012/1978)

introducido cuantiosas novedades en la materia, influenciando el régimen hasta la fecha en vigor, incluso para el sistema de protección británico, pionero en estas cuestiones.

A continuación, va a pasarse a examinar brevemente cuales son las materias y cuestiones principales que, a tenor del nuevo marco normativo, reciben un mayor impacto en el sistema anglosajón y deben abordarse por la legislación británica para la unificación de criterios. Para ello, y con el objetivo de lograr una mayor comprensión, se sigue el orden y la sistematización empleada en el punto anterior.

a) Ámbito territorial de aplicación

El alcance territorial de la normativa europea de protección de datos ha cambiado radicalmente a raíz de las introducciones hechas por el Reglamento pues ahora éste se aplicará, no sólo a los encargados y responsables del tratamiento que tengan su sede en territorio europeo, sino también a aquéllos que, estando fuera, presten servicios o lleven a cabo un tratamiento de datos en la Unión Europea.

Sin embargo, esto no difiere notablemente de la legislación británica hasta la fecha pues la DPA[325], pese a que se aplica generalmente al procesamiento de datos llevado a cabo por una entidad establecida en el Reino Unido (como una empresa registrada, sociedad, sucursal o agencia), prevé además que, si el procesamiento de la información almacenada electrónicamente se lleva a cabo en el Reino Unido en nombre de una entidad que, no obstante, no tiene presencia física en suelo británico o en el Espacio Económico Europeo, éste quedará sujeto a las disposiciones de la DPA[326].

No obstante el GDPR va un paso más allá, al extender la aplicación de sus disposiciones a todo responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas bien con la oferta de bienes o servicios a dichos interesados en la

[325] Sección 5ª.

[326] Por ejemplo, para el caso de que una entidad de los EE. UU. utilice un proveedor o una agencia de servicios del Reino Unido para procesar información almacenada electrónicamente con el propósito de litigar en los EE. UU.

Unión -independientemente de si a éstos se les requiere su pago-, bien con el control de su comportamiento, en la medida en que éste tenga lugar en la Unión[327].

En cuanto a aquellas empresas que tengan más de un establecimiento en territorio europeo, el Reglamento introduce el concepto de "establecimiento principal" en su artículo 4, cuya importancia radica en que la localización de éste será clave para determinar qué autoridad de control se encargará de su inspección y responderá ante un posible incumplimiento. Así, el establecimiento principal de un encargado del tratamiento será el lugar donde radique su sede administrativa o en donde se tomen las decisiones principales, mientras que el establecimiento principal de un encargado del procesamiento será, en defecto de su sede de administración, el emplazamiento en el que tengan lugar la mayor parte de las actividades de tratamiento.

b) Definiciones básicas

En cuanto a la definición de datos personales, el GDPR introduce una versión ampliada bajo la cual se incluye toda información sobre una persona física identificada o identificable, acabando así con la disparidad producida entre la Directiva del 95 y la DPA. Ahora, a diferencia de lo dispuesto en la legislación británica, se consideran "interesados" aquéllos quienes, sin estar identificados al tiempo de la recopilación de los datos, pueden estarlo en el futuro gracias a esa información personal.

Es decir, "identificable" significa, a efectos del GDPR, que su identidad pueda determinarse, directa o indirectamente, y en particular, mediante un identificador "como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona"[328]. Esto tiene un gran impacto en la legislación británica que deberá ampliar su concepto de interesado para incluir a individuos cuya identidad

[327] Artículo 3.

[328] Artículo 4.1).

no se conoce en el momento en que se recopilan los datos pero que puede determinarse en el futuro[329].

En cuanto a los datos especialmente sensibles, conviene destacar que el artículo 9 del GDPR enumera estas categorías especiales de datos personales y añade, frente a lo dispuesto por la DPA, aquéllos que revelen las convicciones filosóficas así como la orientación sexual de una persona, el tratamiento de datos genéticos[330] y los datos biométricos dirigidos a identificar de manera unívoca a una persona.

Asimismo, el GDPR impone requisitos más estrictos a la hora de procesar datos, precisamente para tratar de salvaguardar los datos sensibles que de éstos puedan extraerse, y con tal objetivo, exige mayores controles a aquéllos que traten datos quienes deben revisar si concurre información sensible así como la categorización de datos preexistente, por si alguno de los datos almacenados ahora pueda considerarse "información sensible" según los nuevos parámetros del Reglamento[331].

c) Principios inspiradores

Respecto de los principios inspiradores que vertebran toda la legislación británica de protección de datos, si bien el Reglamento refleja en gran medida su grueso, éste contiene una regulación más detallada, haciéndolos más restrictivos y rigurosos.

Así, en cuanto al primer principio ("los datos personales se procesarán de forma justa y legal"), el GDPR exige, además, que el tratamiento se produzca de una forma transparente en relación con el sujeto objeto del tratamiento. Esto supone una novedad frente a la DPA que no contempla la transparencia en ninguno de sus preceptos.

---

[329] Cuando, por ejemplo, el *data controller* añade datos adicionales o realiza una investigación más exhaustiva cruzando datos, por ejemplo.

[330] La novedad de este concepto hace necesaria su definición, por lo que el artículo 4.13) dispone que éstos serán los "*datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona*".

[331] Para evitar los posibles perjuicios que puedan ocasionarse mediante el tratamiento de datos especialmente sensibles, podría emplearse por la legislación británica el nuevo mecanismo de "seudonimización" que incorpora el GDPR, para lograr un tratamiento de datos que no puedan atribuirse al interesado sin utilizar información adicional.

La exigencia de transparencia, por ser un concepto nuevo, viene regulada más detalladamente en la Sección I del Capítulo III aunque, a grandes rasgos, puede decirse que ésta exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro.

En cuanto al contenido de los datos, el GDPR ahonda más en el tercer principio de la DPA ("los datos personales deberán ser adecuados, pertinentes y no excesivos en relación con el o los fines para los que son procesados") al exigir una minimización de su contenido y de su tratamiento, atendiendo a criterios de proporcionalidad y necesidad[332]. Esto, en la práctica, comporta cambios para la mayoría de las organizaciones británicas que recopilan y procesan datos en demasía, cuyos defensores no han dudado en expresar su disconformidad, alegando que ello supondrá incrementar los costes económicos.

Siguiendo esta línea, y en relación al cuarto principio ("los datos personales deberán ser precisos y, de ser necesario, mantenerse actualizados"), el GDPR exige una conducta más proactiva por parte de los encargados del tratamiento para asegurarse que los extremos de adecuación y actualización se cumplen, y para ello se ponen a su disposición las técnicas de seudonimización[333] y anonimización cómo medidas efectivas para lograr que la identificación de un individuo sólo sea posible por un periodo no superior al necesario para el tratamiento.

Para asegurarse del cumplimiento de todos y cada uno de estos extremos, se dispone la obligatoriedad, tanto para el encargado como para el responsable, de designar un Delegado de Protección de Datos[334] a los efectos de asesorar y supervisar el cumplimiento de la legislación de datos, así como de cooperar con la autoridad de control, con la que estará en permanente contacto y a la que deberá comunicar cualquier atisbo de infracción.

---

[332] Este objetivo de minimizar los datos retenidos, forma parte de la estrategia global del Reglamento por imponer una política de protección de los datos desde el diseño.

[333] El Reglamento pretende incentivar esta práctica de protección de datos personales, que define en su artículo 4.5) como "*el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable*".

[334] Sección cuarta, artículos 37 y siguientes.

El Reglamento, en relación al cumplimiento de todos estos principios, impone más obligaciones a los encargados del tratamiento, bajo el principio de responsabilidad y de "*accountability*", por lo que a partir de ahora deben demostrar no sólo que han tomado las medidas necesarias para el cumplimiento de las disposiciones sino que, en caso de duda, tienen la carga de demostrar su buen hacer. Asimismo, se impone a los responsables del tratamiento la obligación de vigilar que los encargados a los que subcontratan el procesamiento, tengan implementadas medidas adecuadas de seguridad.

d) Procesamiento legal y justo

Entre los distintos tipos de tratamiento, el GDPR hace mención expresa a una práctica empresarial muy extendida como es la "elaboración de perfiles" que consiste en analizar datos personales para evaluar determinados aspectos personales de una persona física, posiblemente con el objetivo de predecir aspectos personales como pueden ser el rendimiento profesional, la situación económica, los intereses o su ubicación. Queda introducido en el Reglamento como una novedad que, sin embargo, no afecta a la legislación británica gracias a sus preceptos redactados en términos generales que han permitido aplicar la DPA a las diferentes técnicas de procesamiento de cada momento.

En cuanto al procesamiento de datos, el artículo 5 del GDPR dispone que éstos serán tratados "de manera lícita, leal y transparente en relación con el interesado" añadiendo a la definición prevista por el DPA el concepto de "transparencia", detallado en el artículo 11 cuando establece "*información en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo*".

Se disponen también, en el artículo 14, los pormenores que deben de informase al interesado en relación con el tratamiento de sus datos personales cuando éstos no se hayan obtenido del interesado. Se incluyen como novedades, la identidad y la información de contacto

del responsable del tratamiento así como la existencia de medidas de *profiling*[335] o la intención de usar este tipo de técnicas.

Conviene destacar también que, respecto de la elaboraciones de perfiles, esta técnica se ve afectada por la previsión del artículo 22 que prohíbe las decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, salvo que el individuo haya dado su consentimiento expreso, exista un deber legal de llevar a cabo el procesamiento o un contrato con el individuo y siempre y cuando se adopten medidas apropiadas para garantizar la equidad.

La ICO se mostró contraria a esta novedad pues advirtió que esta disposición afecta a los envíos con objeto de marketing por lo que, ahora, las empresas británicas deben de contar con el consentimiento de los sujetos objeto de tratamiento para llevar a cabo cualquier evaluación basada en el procesamiento automatizado, incluida la publicidad conductual en línea.

El artículo 6 del GDPR dispone las condiciones para una licitud del tratamiento que, básicamente, reproduce lo dispuesto en la Directiva de 1995 con dos excepciones: el consentimiento y los intereses legítimos. En cuanto al primero, se introducen restricciones incluyendo el hecho de que el consentimiento haya perdido su validez o haya expirado una vez la finalidad para la que fue recabado haya cesado, además, se exige que el consentimiento se obtenga explícitamente en todos los casos y no sólo respecto de la información altamente sensible. Esta exigencia supone, en la práctica, que los encargados del tratamiento de datos deben de prever mecanismos para asegurarse de que los interesados prestan su consentimiento explícito, para lo cual, en la legislación británica se inclina por el sistema de rellenar casillas (*box ticking*).

La segunda excepción, radica en el hecho de que se ha eliminado toda referencia a los legítimos intereses perseguidos por terceros a quienes se les revelan los datos y se ha sustituido

[335] La técnica de elaboración de perfiles viene descrita en el artículo 4.4) como "*toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*".

por la expresión "expectativas razonables del interesado" basadas en su relación con el encargado del tratamiento, que resulta más acorde con las interpretaciones realizadas por la ICO en este sentido.

En relación al consentimiento, respecto de los menores de edad, y pese a que se define "niño" como aquél que tenga menos de dieciocho años, el Reglamento dispone como regla general la edad mínima de dieciséis años para considerar lícito el tratamiento de los datos personales de un menor o cuando éste, se supla por el consentimiento de sus padres o tutores. Sin embargo, se faculta a los Estados miembros para que, si lo consideran necesario, establezcan por ley un límite inferior de edad, siempre y cuando éste no sea inferior a trece años[336]. Las previsiones legislativas británicas en estos términos, se inclinan por rebajar la edad para prestar el consentimiento a los trece años, el mínimo autorizado por la nueva norma europea.

e) Exportación de datos

Respecto del régimen de la exportación de datos a terceros países, el GDPR no incorpora grandes novedades al sistema anglosajón que ya preveía como regla general la prohibición de cualquier exportación de datos personales desde el Espacio Económico Europeo hacia terceros estados o territorios, aunque con cuantiosas excepciones. Con la voluntad de continuar exportando los estándares europeos en materia de privacidad fuera de nuestras fronteras, el Reglamento prohíbe todas las transferencias internacionales a aquellos territorios que no garanticen un nivel adecuado de protección conforme a la Comisión Europea siguiendo criterios más restrictivos[337].

Sin embargo, la doctrina británica[338] se ha manifestado contraria a la adopción de estas medidas, al parecerles demasiado restrictivas en materia comercial. En las elaboraciones

[336] Artículo 8.

[337] El nivel de protección que se adopta mediante el Reglamento es tal que, en su artículo 48, dispone que cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales, únicamente será reconocida o ejecutable si se basa en un acuerdo internacional vigente entre el país tercero y la Unión Europea o el Estado miembro en cuestión.

[338] CAREY. *Data Protection Handbook*, The Law Society, London, 2008, p. 194.

doctrinales de esta cuestión se observa como el arraigo del *common law* impera en las argumentaciones de los autores que tienen una concepción de la privacidad distinta y que entienden esta medida como una regresión en materia de liberalización del Mercado. También es verdad que, por motivos históricos y geográficos, Reino Unido mantiene gran cantidad de operaciones comerciales con Estados Unidos, uno de los principales afectados por la norma[339].

Además de la excepciones, que no aportan cambios significantes en la regulación, las transferencias internacionales están permitidas siempre que se lleven a cabo mediante los mecanismos de las *Binding Corporate Rules* y las cláusulas contractuales de adhesión, expresamente reconocidas por los artículos 46 y 47 del Reglamento.

En cambio, en cuanto a la legislación británica, el cambio más sustancial será la imposibilidad de que se continúen llevando a cabo procedimientos de exportación de datos mediante los *international outsourcing arrangements*, figura de aplicación exclusivamente en Reino Unido que no cuenta con ninguna previsión al respecto en el GDPR.

f) Derechos de los sujetos

Bajo el régimen del GDPR, los sujetos objeto de tratamiento mantienen los derechos recogidos en la DPA con pequeñas modificaciones y, además, se añaden otros nuevos como el derecho a la portabilidad de datos (artículo 20) o el derecho de supresión o al olvido (artículo 17). En cuanto a su ejercicio, si bien se mantiene el hecho de que los responsables últimos del cumplimiento de éstos sean los encargados del tratamiento, se prevé en el Reglamento que la autoridad supervisora pueda ordenar directamente al encargado del procesamiento que cumpla con la solicitud de un interesado para ejercitar sus derechos al respecto.

Respecto del derecho al olvido merece la pena detenerse pues realmente esto supone un cambio sustancial respecto de la posición del Reino Unido, hasta ahora escéptica ante el reconocimiento del derecho de supresión debido a sus disparidades con la lógica jurídica anglosajona, en la que se aboga por ejemplo, por la publicidad íntegra de las sentencias

[339] De hecho, desde la patronal se viene solicitando, entre otras cosas, la redacción de otro lote de modelos de *contractual clauses* que rebajen las exigencias actuales a los importadores de datos.

judiciales así como el libre acceso a los antecedentes penales. Esto unido al funcionamiento propio de la sociedad británica, dónde el *lobby* de los medios de comunicación, altamente sensacionalistas, tiene un vasto poder e influencia. De hecho, puede negarse la existencia de cualquier manifestación de un derecho general al olvido en la tradición jurídica del *common law*, cosa que deberá cambiar ahora, al menos, para el Reino Unido.

Los derechos se contemplan ahora en los artículos 15 a 22 y en cuanto a los cambios sustanciales frente a la DPA puede destacarse, entre otros, como el derecho británico a oponerse al tratamiento automatizado de datos se sustituye ahora por la prohibición total de usar perfiles automatizados sin el consentimiento de los afectados. Se impide así, la toma de decisiones en exclusiva de forma automatizada en base al "*profiling*", es decir, mediante el procesamiento de información automatizada como la localización, las preferencias o el comportamiento.

Para asegurarse el cumplimiento de todos estos derechos, el Reglamento impone un deber de transparencia y accesibilidad general para que los interesados reciban en todo momento información clara y entendible, con sumos detalles, lo que obliga a los encargados del procesamiento y tratamiento a elaborar políticas de privacidad extremadamente minuciosas. Por el contrario, ante una contravención sustancial de estas obligaciones, se prevén sustanciosas multas que a partir de ahora podrá imponer la entidad británica ICO.

g) Garantías de cumplimiento de la Ley

Por lo que respecta a la actividad supervisora, el Reglamento cambia la denominación empleada por la Directiva del 95 y también por la DPA, y pasa a llamar las antiguas "*national data protection regulators"* como "autoridades de control" ("*supervisory authority"* en su versión en inglés)[340].

[340] Se regulan en el Capítulo VI, artículos 51 y siguientes.

Cada Estado miembro tendrá al menos una autoridad de control, que supervisará a los encargados y responsables del tratamiento establecidos en su jurisdicción[341]. A grandes rasgos, esto significa que las autoridades de control supervisarán todas las organizaciones con sucursales u oficinas de negocios en su jurisdicción así como a todas las autoridades públicas. También supervisarán a los controladores de datos ubicados fuera de la UE que ofrecen servicios remotos en su país pero que no tienen presencia en su territorio[342].

Respecto de otros mecanismos de garantía, debe señalarse que el Reglamento, a diferencia de la ley británica, no establece la obligación a los encargados del tratamiento de notificar a la autoridad nacional de control pertinente la existencia de dicho tratamiento así como sus extremos. Esta obligación se sustituye por la de llevar un escrupuloso registro de las actividades de tratamiento efectuadas bajo su responsabilidad[343] que incluyan los extremos detallados en la normativa[344] y que, si son requeridos por la autoridad de control, se pongan a su disposición[345].

En este sentido, la DPA resulta más garantista que el Reglamento, que dispone un régimen de autorregulación salvo que haya indicios de actividad ilegal por parte de los encargados del tratamiento. Paralelamente, los extremos que hay que registrar son mucho

[341] Las autoridades de control tienen amplias facultades para investigar infracciones sobre protección de datos y para tomar medidas coercitivas (incluyendo poderes de entrada, confiscación, suspensión o prohibición de procesamiento, así como capacidad para ordenar el borrado de datos) y para imponer multas. Cuando una empresa opere en varios países de la UE, una novedad del Reglamento es que se permite que dicha organización tenga una autoridad de control base (en el Estado dónde la empresa tenga su establecimiento principal) que será responsable de supervisar todas sus actividades.

[342] Puesto que, cuando las empresas operan a través de empresas independientes de fuera de la UE pueden estar sujetas a la supervisión de varias autoridades distintas, se ha previsto el "mecanismo de coherencia" (artículo 63) para que las autoridades puedan trabajar conjuntamente y llegar a un acuerdo sobre asuntos que afectan a los sujetos del tratamiento en distintos Estados miembros.

[343] Artículo 30.

[344] El nombre y los datos del responsable (y, en su caso, el corresponsable, el representante y del delegado de protección de datos), los fines del tratamiento, una descripción de las categorías de interesados y de datos personales, las transferencias de datos que se efectúen, en su caso, a una organización internacional o a un tercer país; y, cuando sea posible, una descripción de los plazos previstos para la supresión de datos así como de los mecanismos de seguridad previstos.

[345] Esta obligación e registro se impone tanto al responsable del tratamiento como al encargado de su procesamiento lo que supone, frente al régimen dispuesto por la DPA, una considerable extensión de las obligaciones de los *data processors*, produciéndose una duplicidad de registros para las mismas actividades. La reacción de los británicos no se hizo esperar, por una parte las empresas encargadas del procesamiento de datos que mostraron su descontento por la implementación de dichas medidas, argumentado que éstas repercutirán en los costes económicos de su actividad que se verán incrementados. Por otro lado, el gobierno se adhirió a sus protestas al entender esta medida como excesivamente onerosa.

mayores que los de la normativa británica que, mediante el sistema de *notices*, simplificaba a la postre, este procedimiento.

No obstante, se impone a los responsables del tratamiento la obligación de colaborar con las autoridades de control cuando sean requeridas para ello[346] así como el deber general de implementar todas las políticas y medidas que sean necesarias para garantizar que sus actividades de procesamiento respetan las disposiciones del Reglamento.

En cuanto a las Evaluaciones de Impacto (las llamadas PIA), denominadas por el GDPR *Data Protection Impacts Assessments* (DPIA), pasan ahora a ser obligatorias en algunas circunstancias: "cuando exista la probabilidad de que, por su naturaleza, alcance o fines, las operaciones de tratamiento entrañen un alto riesgo para los derechos y las libertades de los interesados"[347], en particular cuando se empleen nuevas tecnologías. Dicha evaluación debe comprender las medidas y garantías para la protección de los datos personales así como los sistemas y procesos correspondientes a las operaciones de tratamiento, siendo capaz de demostrar su conformidad con el Reglamento.

Por otra parte, se establece también el deber de los encargados del tratamiento de notificar a la autoridad de control cualquier violación de la seguridad de los datos personales en un plazo máximo de setenta y dos horas desde que haya tenido constancia de ello, salvo que sea improbable que se deriven daños para los derechos y libertades de las personas físicas. Por el contrario, cuando sí que exista tal riesgo, debe comunicársele al interesado[348].

Esto alterará sustancialmente el régimen de las *notices* británicas que establecían dicha posibilidad como una potestad, relacionada con las buenas prácticas empresariales. Sin embargo, con el Reglamento esto pasa a ser una obligación más de los encargados del

[346] Artículo 31.

[347] Artículo 27. Por ejemplo, cuando se procesen datos personales de carácter sensible, genéticos o biométricos o cuando se lleve a cabo *profiling*.

[348] Artículos 32 y 33. Esto supone ciertos problemas prácticos pues el interesado debería ser informado siempre a la vez que la autoridad competente sobre una posible brecha de seguridad de sus datos para, según su criterio, tomar las acciones que considere necesarias (pensemos por ejemplo, en una brecha de seguridad respecto de los datos bancarios) con independencia de que se considere o no relevante por la autoridad o por el responsable del tratamiento.

tratamiento que deben informar a la autoridad de control sin dilación indebida y especificando una serie de extremos en relación a dicha violación de seguridad[349]. Asimismo, y con posterioridad, deberá de informarse de ello al interesado, en un lenguaje claro y sencillo[350].

Las evaluaciones de impacto están estrechamente ligadas con las funciones del Delegado de protección de datos (DPO en la redacción inglesa)[351] quien, además de orientar la actuación del responsable del tratamiento y de supervisar el cumplimiento de las disposiciones de la Ley, debe ofrecer asesoramiento preciso acerca de la evaluación de impacto[352].

Así pues, conforme a la nueva regulación introducida por el GDPR, la ICO deberá de llevar a cabo una lista en la que se comprendan aquellas actividades relacionadas con datos personales que necesariamente deban someterse a una evaluación de impacto y así, según el nivel de riesgo que entrañen, requerirán o no una autorización previa. Cualquier encargado del tratamiento podrá someterse voluntariamente a una evaluación para verificar con ello si está cumpliendo o no con todas las exigencias introducidas por el GDPD.

h) Exenciones

Por lo que respecta a las exenciones, la Sección quinta del Reglamento regula éstas, a las que llama "limitaciones" cuya finalidad es precisamente, limitar el alcance de las obligaciones y de los derechos y obligaciones contenidas en los apartados anteriores siempre y cuando "tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática[353]". Y, a continuación, esgrime los motivos por los cuales pueden aplicarse dichas limitaciones[354].

---

[349] Extremos comprendidos en el artículo 33.3.

[350] Artículo 34.

[351] Esto evidencia como el Reglamento ha depositado sus esperanzas en las DPIAs aunque, no hay que olvidar que se corre el riesgo de caer en formularios burocráticos en lugar de herramientas de evaluación útiles, ya que los controladores de datos tratarán de asegurar que ninguna información sensible o comercial llegue al dominio público.

[352] Artículo 39. 1. C).

[353] Artículo 23.

[354] a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la

Pese a que el Reglamento impone a los Estados miembros la obligación de legislar estos extremos, también recoge ciertas exenciones a lo largo de su articulado en relación a situaciones específicas de procesamiento de datos, incluyendo la libertad de expresión e información y los fines periodísticos (artículo 85), documentos oficiales (artículo 86 y 87), el ámbito laboral (artículo 88), fines de investigación científica o histórica o fines estadísticos (artículo 89), obligación de secreto profesional (artículo 90) y asociaciones religiosas (artículo 91).

Sin embargo, como ya se dispuso en la Directiva del 95, el Reglamento faculta a los Estados para que adopten en sus legislaciones exenciones y excepciones necesarias para equilibrar los derechos fundamentales que puedan verse afectados por un cumplimiento exhaustivo de la Ley. El gran margen discrecional que se le otorga a las legislaciones domésticas hace que, en este aspecto en particular, la nueva regulación europea no produzca demasiados cambios en el régimen británico cuyo tratamiento de la materia tiene cabida suficiente en los nuevos márgenes legales.

i) Subcontratación (outsourcing) en el procesamiento de datos

La externalización del tratamiento está prevista expresamente en el Capítulo IV del Reglamento e incorpora ciertas novedades respecto del régimen de la legislación británica como por ejemplo, la obligación para el responsable del tratamiento de velar para que éste se lleve a cabo conforme a los principios de la protección de datos por defecto y desde el diseño, extremos que deben incorporarse, asimismo, al contrato que vincule al responsable con el encargado del tratamiento[355].

---

seguridad pública y su prevención; e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; f) la protección de la independencia judicial y de los procedimientos judiciales; g) la prevención, la investigación, la detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g); i) la protección del interesado o de los derechos y libertades de otros; j) la ejecución de demandas civiles.

[355] Junto a esto, deben incluirse los siguientes extremos: objeto del tratamiento, duración, naturaleza, finalidad, tipos de datos personales, categorías de interesados y las obligaciones y derechos de ambos (Artículo 28).

Para que se pueda externalizar esta actividad, el GDPR exige a los encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas para cumplir con la normativa europea de protección de datos. Entre éstas, se exige que disponga de las medidas necesarias para proceder a la supresión o devolución de los datos personales así como sus copias una vez finalice la prestación de los servicios, por si así se le solicitase por el responsable del tratamiento.

En consecuencia, se incorpora la exigencia, por una parte, a los responsables del tratamiento de llevar un registro de todo el tratamiento que se lleve a cabo en su nombre y bajo su responsabilidad, y de otra, a los encargados del tratamiento, sobre todas las categorías de actividades de tratamiento efectuadas en nombre de un responsable. Ambos registros deberán constar por escrito, inclusive en formato electrónica, y deberán de facilitarse a la autoridad de control en caso que así lo requiera, pues se impone un deber de cooperación con éstas en todo caso[356][357].

También se contempla expresamente por el GDPR la posibilidad de que dos o más responsables del tratamiento determinen conjuntamente los objetivos y los medios de éste, lo que les confiere la consideración de corresponsables del tratamiento[358]. En este supuesto, deberán determinar de forma transparente y de mutuo acuerdo cuales serán sus respectivas responsabilidades y cómo podrán ejercitarse los derechos de los interesados, designando un punto de contacto único o común para facilitárselo.

Así las cosas, la legislación británica debe adoptar un cambio de modelo donde, además del autocontrol por parte del encargado del tratamiento, se incorporen exámenes previos por parte de las autoridades públicas y sistemas de autorización anticipada, además de registros

[356] Artículos 28 y 30.

[357] Las operaciones de tratamiento mediante sistemas automatizados están reguladas expresamente en el artículo 30 del Reglamento que impone a los Estados la obligación de velar por la conservación de los registros de este tipo de tratamiento, en los que se incluyan los extremos que especifica (a grandes rasgos: la recogida, alteración, consulta y comunicación -incluidas las transferencias, combinación o supresión e datos-) y que sean accesibles para su consulta por cualquier interesado. Se configura así una medida adicional de control de la legalidad del tratamiento y la seguridad de los datos que incluye también, el ámbito de los procesos penales.

[358] Artículo 26.

accesibles por parte de los interesados. En definitiva, reforzar las medidas que garanticen la integridad y la seguridad de los datos, pudiendo adoptar, como se instaura en el Reglamento, medidas de cifrado o similares, para preservar, también, la confidencialidad.

Por otra parte, las disposiciones del GDPR establecen deberes y obligaciones conjuntamente a los responsables y a los encargados del tratamiento lo que supone un cambio de modelo frente a la legislación británica que impone una mayor carga a los responsables del tratamiento, que son quienes responden en última instancia de las actuaciones de los *data processor*. Y es que, el nuevo marco europeo ha expandido notablemente las funciones de los encargados del tratamiento, que tienen consideración de responsables y a quienes se les impone la carga de la prueba[359].

Esto implica que derechos y obligaciones ahora son exigibles tanto para los responsables del tratamiento como para los encargados, que deben aunar esfuerzos con el fin de garantizar una supervisión coherente del procesamiento de datos personales pues, en caso contrario, ambos serán susceptibles de recibir sanciones por la autoridad competente. Esto conlleva necesariamente que tanto el responsable como el encargado del tratamiento deben mantener registros de las actividades de éste bajo su responsabilidad, y que, además, ambos están obligados a cooperar con la autoridad de control y a poner a su disposición dichos registros, si son requeridos para ello.

El gobierno británico ya expresó su disconformidad con el sentido de estos preceptos por parecerle desproporcionada la extensión de obligaciones hacia el encargado del tratamiento pues, en comparación con su legislación, esto supone un giro radical que, según denuncian, implica una duplicidad de funciones.

Todas estas modificaciones se han recogido e incorporado en la nueva *Data Protection Bill* -en tramitación parlamentaria en el momento de redacción de estas líneas- la cual pasará a

[359] La carga de la prueba recae en ambos casos en los encargados y responsables del tratamiento, en lo ha sido denominado por el Reglamento "principio de responsabilidad proactiva".

comentarse más adelante, y que parece que marcará un nuevo punto de inflexión en la protección de datos en el Reino Unido, al menos hasta que se consume finalmente el *Brexit*.

3. El impacto de la *Human Rights Act 1998* en este contexto

La *Human Rights Act 1998* (HRA en adelante) entró en vigor el 9 de noviembre de 1998, cuarenta y siete años después de que el Reino Unido ratificase el Convenio Europeo de Derechos Humanos (CEDH), sobre el que más tarde se incidirá[360].

Para tomar consciencia de la importancia de esta norma, debe recordarse que el Reino Unido carece de una Constitución escrita mediante la cual se concede derechos positivos a sus ciudadanos, lo que no implica que, en el ordenamiento jurídico británico no existan derechos fundamentales. El sistema anglosajón cuenta con lo que se ha llamado "*unwritten constitution*", que otorga fuerza vinculante al *common law*, a las disposiciones normativas de origen parlamentario así como a los tratados internacionales, y es a través de estos instrumentos, y siguiendo el criterio orientador de la *rule of law*, que se provee a la ciudadanía de derechos y libertades exigibles[361].

En este contexto reside la significación de la HRA, que convierte el CEDH en derecho vinculante para los poderes públicos británicos, proclamando los derechos recogidos en la nueva norma como una suerte de declaración de derechos fundamentales para su ciudadanía. Es por ello que el Gobierno británico argumentó en su día que, con dicha normativa, se "estaban trayendo los derechos humanos a casa"[362] pues el objetivo principal era, precisamente, incorporar el contenido del Convenio a la legislación doméstica del Reino Unido[363].

---

[360] Sobre la *Human Rights Act*, puede destacarse la reciente aportación en castellano, desde la perspectiva del sistema de justicia penal, de CORRECHER MIRA, J. *Principio de legalidad penal*: *ley formal vs. law in action*, Tirant lo Blanch, Valencia, 2018, pp. 179-207.

[361] A diferencia de los ordenamientos jurídicos de la cultura legal continental, en la que los Estados tienen una fuerte raigambre codificadora, el Reino Unido se caracteriza por la ausencia de una norma constitucional en los términos continentales protegiendo, sin embargo, de forma equivalente, derechos y libertades públicas a los ciudadanos.

[362] "*Bring Rights Home*" fue el eslogan utilizado por el partido laborista, entonces en el gobierno, para escenificar la importancia de la aprobación de la HRA.

[363] De hecho, en la presentación del proyecto de la HRA, se incidió en que dicho texto normativo no suponía la creación de nuevos derechos para los británicos sino que se dotaba de eficacia directa a los mismos con el objetivo de que los tribunales

Así las cosas, la publicación de la HRA supuso un punto de inflexión en el funcionamiento del sistema jurídico anglosajón pues a partir de entonces, la supremacía del CEDH se impuso en las relaciones jurídicas de los británicos, superando de una vez por todas un modelo en el que los derechos civiles eran concebidos como una libertad negativa[364], y la conducta permitida era toda aquella que no estuviera prohibida expresamente[365], rigiendo una presunción de legalidad[366].

Además de convertir en vinculante el contenido del CEDH, la HRA impone a todos los poderes públicos la obligatoriedad de actuar, en el ejercicio de sus funciones, de forma compatible con los derechos de la CEDH, lo que incluye también a la judicatura. A partir de entonces, los tribunales del Reino Unido deben de interpretar la legislación primaria -vigente o futura- de manera coherente con los derechos del Convenio[367], acatando en todo lo posible la jurisprudencia emanada del Tribunal Europeo de Derechos Humanos (TEDH, en adelante) por lo que, en caso de encontrarse con una disposición legislativa en sentido contrario a la HRA, los órganos jurisdiccionales deberán declarar la incompatibilidad de la misma[368].

---

dispusieran de mecanismos suficientes para su efectiva protección. Sin embargo, eran muchos los derechos del CEDH que no se recogían en el *common law* británico, entre ellos, el derecho a la vida privada y familiar.

[364] Así, un denunciante debía probar la comisión de un delito, el demandante probar la vulneración del derecho civil y el Estado probar la existencia de la prohibición. Cfr. EWING/GEARTY. *Freedom under Thatcher*, Oxford University Press, 1990, p.8.

[365] Explicado de una forma simplista podría decirse que, anteriormente, un ciudadano podía en principio llevar a cabo cualquier acción siempre que ésta no fuese ilegal -bien porque el Parlamento lo hubiese considerado delito o por estar prohibido por un acto administrativo-, de modo que quien se quejase de lo que un ciudadano quisiese hacer o hubiese hecho, debería probar su ilegalidad. Una vez promulgada la HRA, el punto de partida ya no es la libertad de cada ciudadano para hacer lo que desee, sino los derechos que todos los ciudadanos disfrutan en virtud del CEDH, por lo que el goce de estos derechos, prevalecerá en todo caso excepto que la interferencia en los mismos quede debidamente justificada. Cfr. HARVERS/GARNHAM. "The Convention and the Human Rights Act: A New Way of Thinking", en *An Introduction to Human Rights and the Common Law* (English/Havers eds.), Hart Publishing, Oxford and Portland (Oregon), 2000, pp. 5-29.

[366] DAVIS. *Human Rights and Civil Liberties*, Willan Publishing, Cullompton, 2003, p.15.

[367] Critica GEARTY que la eficacia de la HRA recae principalmente en la judicatura nacional, a "quien se le ha entregado un poder mayor, pero limitado". GEARTY. "Reconciling Parliamentary democracy and human rights", en *Law Quaterly Review*, nº 118, 2002, p. 269.

[368] No su inaplicación ni su invalidez. Sólo el Parlamento británico podrá enmendar la norma declarada incompatible por los tribunales y sortear así dicho conflicto. Además, establecen mecanismos de reparación en la legislación doméstica británica para el caso de que los derechos y libertades que recoja sean vulnerados, evitando así recurrir sistemáticamente y como segunda instancia al Tribunal Europeo de Derechos Humanos.

En cuanto al objeto de estudio de la presente disertación, la entrada en vigor de la HRA supuso un paso decisivo en la protección de la privacidad en la jurisdicción anglosajona, mediante el reconocimiento del derecho a la privacidad en su artículo 8, derecho que, hasta entonces, no gozaba de soporte legal específico en la legislación británica pero que, a partir de dicho momento se instituyó como un bien jurídico a proteger con independencia del derecho a la protección de datos o, mejor, como un mecanismo adicional.

Así, el artículo 8 de la HRA, en el que se profundizará más adelante, dota de soporte legal a un derecho subyacente en la doctrina británica, reconocido a través de figuras tradicionales del *common law* y el derecho a la protección de datos, mediante la incorporación directa del derecho a la vida privada y familiar reconocido en el CEDH, acercándose a la doctrina más continental y, en consecuencia, dotándolo de una completa autonomía. La transcendencia de la HRA en este contexto se puso de relevancia por Lord Hoffman en el famoso *caso Campbell*: "lo que ha hecho la *Human Rights Act* es identificar la vida privada con algo que merece la pena proteger, como un aspecto fundamental de la autonomía personal y la dignidad humana"[369].

Del mismo modo, como también se detallará a continuación, la jurisprudencia del TEDH y su forma de interpretar el artículo 8 ha sido esencial en la formación y aplicación jurídica del derecho a la privacidad por los tribunales británicos. El cambio de las reglas de juego propiciado por la HRA, ha logrado incluso reconocer un efecto horizontal a dicho precepto[370], disponiendo la obligación de los tribunales de alcanzar, en su labor de interpretación y aplicación del *common law*, una compatibilidad con los derechos reconocidos en la CEDH.

---

[369] Y, añade: "*The result of these developments has been a shift in the centre of gravity of the action for breaches of confidence when it is used as a remedy for the unjustified publication of personal information […] instead of the cause of action being based upon the duty of good faith applicable to confidential personal information and trade secrets alike, it focuses upon the protection of human autonomy and dignity-the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people*", *Campbell v. Mirror Group Newspapers Ldt* [2004] UKHL 22.

[370] *Michael Douglas & Catherine Zeta-Jones v. Hello! Ldt*, de 7 de noviembre de 2003 [2003] EWHC 2629 (Ch), Court Chancery Division.

Por todo ello, y como se analizará en mayor profundidad más adelante, la HRA supone un ejercicio complicado a la hora de encontrar un equilibrio entre la democracia y los derechos humanos, dicho de otro modo, entre la soberanía parlamentaria británica y el reconocimiento formal de las libertades fundamentales del CEDH. Esto se ejemplifica en el mencionado artículo 8 y su regulación de la vida privada y familiar, derecho que, si bien no tenía precedentes significativos en la jurisdicción británica, a partir de la entrada en vigor de la HRA pasa a formar parte del conjunto de derechos e intereses que el Reino Unido debe proteger como valor fundamental para garantizar la autonomía y la dignidad personal, que le son intrínsecas[371].

3.1. La firma del Convenio Europeo de Derechos Humanos por Reino Unido

El Convenio Europeo de Derechos Humanos (CEDH) es una iniciativa del Consejo de Europa tras la finalización de la Segunda Guerra Mundial. El texto aprobado por el Comité de Ministros fue firmado por el resto de Estados parte el 4 de noviembre de 1950[372]. La estructura resultante del Convenio obedecía al orden que será expuesto a continuación.

En su primera versión, el CEDH establece la Comisión Europea de Derechos Humanos, a la que atribuye la función de tramitación, gestión e investigación de cada uno de los supuestos de hecho presentados, para, posteriormente, trasladar al Tribunal Europeo de Derechos Humanos (TEDH) la función declarativa sobre los hechos presentados por el recurrente, dictando sentencia e imponiendo las sanciones necesarias en el caso concreto. En este esquema, el Comité de Ministros del Consejo de Europa quedaba encargado de supervisar la ejecución de la sentencia del TEDH por parte de los Estados.

Este primer sistema se presentó insuficiente ante el gran número de casos presentados ante la Comisión Europea de Derechos Humanos[373], siendo necesario modificar el sistema

[371] Cfr. ENDICOTT. " 'International Meaning': Comity in Fundamental Rights Adjudication", en *International Journal of Refugee Law*, Vol. 13, Issue 3, 2001, p. 83.

[372] Junto a Reino Unido, fueron firmantes la República Federal Alemana, Bélgica, Dinamarca, Francia, Irlanda, Islandia, Italia, Luxemburgo, Noruega, Países Bajos y Turquía.

[373] Cfr. ASHWORTH/EMMERSON/MACDONALD. *Human Rights and Criminal Justice*, Sweet and Maxwell, London 2012, p. 7.

vigente desde 1953. En este sentido, buscando simplificar su estructura y desformalizar el procedimiento, además de fortalecer la protección efectiva de los derechos y libertades de los nacionales de los Estados parte, los Estados firmantes llevan a cabo una reformulación del modelo creado en 1953 a través de la aprobación el 11 de mayo de 1994 del Protocolo 11. La principal innovación se concreta en la reducción de las funciones atribuidas a la Comisión Europea de Derechos Humanos, trasladando parte de sus funciones al Tribunal Europeo de Derechos Humanos, pasando éste a establecerse como órgano jurisdiccional permanente, asumiendo también determinadas funciones de investigación. Siguiendo con la línea reformista emprendida en 1994, se aprueba posteriormente el Protocolo 11, con la finalidad de aportar agilidad y dinamismo al desarrollo del sistema de protección de derechos y libertades propio del Consejo de Europa[374].

En lo relativo al contenido del Convenio, interesa a efectos de la investigación planteada en este trabajo la protección del derecho a la vida privada y familiar a través del artículo 8. Su reconocimiento supone delimitar la salvaguarda de la intimidad y privacidad como uno de los retos a los que se enfrenta el sistema de protección de derechos y libertades del CEDH:

> 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 sino en tanto en cuanto 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 los demás*.

Este artículo contiene la declaración de una esfera privada del individuo en el sistema de protección de derechos y libertades propio del Convenio. Como se verá a continuación, su

[374] Esto es, el Protocolo número 14 al Convenio para la protección de los Derechos Humanos y de las Libertades Fundamentales, por el que se modifica el mecanismo de control del Convenio, elaborado en Estrasburgo el 13 de mayo de 2004. Su contenido normativo se justifica por la necesidad de garantizar un funcionamiento efectivo del Tribunal Europeo de Derechos Humanos.

reconocimiento e incorporación en el ordenamiento jurídico británico a través de la aprobación de la *Human Rights Act 1998* (HRA) supone la creación de un marco de referencia donde, siguiendo la interpretación evolutiva de su contenido por el TEDH, permite apreciarse un desarrollo armonizado del *right to privacy* en el ordenamiento jurídico británico. En este sentido, la incorporación mediante la HRA de las disposiciones del CEDH al ordenamiento jurídico británico, supone una modificación en los fundamentos de éste, en la medida en que su estructura clásica propia del ámbito jurídico del *common law* experimenta una evolución significativa.

3.2. La codificación de los derechos y libertades en el ordenamiento jurídico británico por la *Human Rights Act 1998*

a) Presupuestos constitucionales para la integración de la Human Rights Act 1998

La elaboración de la *Human Rights Act 1998* (HRA) corresponde al gobierno laboralista británico comandado por el primer ministro Tony Blair. El texto definitivo entró en vigor el 2 de octubre de 2000, siendo su finalidad facultar a la ciudadanía británica para reclamar ante los tribunales nacionales los derechos y libertades reconocidos en el CEDH, pudiendo así recurrir ante los órganos jurisdiccionales internos la protección de los derechos y libertades propios del CEDH, siendo asimismo posible presentar recurso ante el TEDH. Así las cosas, la finalidad última de la HRA es otorgar una mayor efectividad al sistema de garantías establecido en el CEDH, buscando que su articulado pase a ser parte fundamental del conjunto del ordenamiento jurídico británico[375]. La *Human Rights Act 1998* es aplicable al conjunto del territorio del Reino Unido, integrando a Gales, Irlanda del Norte y Escocia.

La importancia de la HRA se mide si consideramos la ausencia, con carácter previo a su aprobación, de una declaración de derechos y libertades del ciudadano en el Reino Unido. Sobre esta cuestión, la *Bill of Rights de 1689*, pese a su marcado simbolismo, no tiene ni la vigencia ni validez necesaria para ser considerada un texto de estas características. La ausencia de una Constitución propiamente dicha, al menos en el sentido de presentar ésta como

[375] Cfr. CORRECHER MIRA. *Principio de legalidad penal: ley formal vs. law in action*, ob. cit., p. 183.

articulado sistemático propio del *civil law*, contribuyó a la falta de un catálogo de derechos y libertades donde quedara expresamente reconocido un sistema de garantías ante las actuaciones del poder público[376]. En este escenario, la introducción de una *Bill of Rights* como instrumento corrector de los posibles excesos o arbitrariedades realizados por el poder ejecutivo[377] parece del todo recomendable. No sólo desde la propia función inspiradora que puede desarrollar para el orden jurídico en su conjunto, sino también considerando su importancia como punto de anclaje normativo para el desarrollo por parte de los tribunales de una jurisprudencia estable en la protección de los derechos y libertades públicas[378].

En consecuencia, la integración en el ordenamiento jurídico británico de los derechos y libertades reconocidos en el Convenio mediante la *Human Rights Act 1998* responde a una doble necesidad: en primer lugar, cohonestar la interpretación-aplicación de las normas de acuerdo al régimen de derechos y libertades propio del CEDH, desarrollando de este modo una función correctora de las posibles vulneraciones cometidas en el orden interno[379]; en segundo lugar, la HRA supone una respuesta a las necesidades evolutivas del ordenamiento jurídico británico. En este sentido, la demanda por una modernización de un sistema excesivamente disperso dada su dependencia del *case law* ha sido puesta de manifiesto, en tanto que el casuismo propio de un sistema de fuentes donde el precedente jurisprudencial mantiene una importancia nuclear puede ser contradictorio con la protección de los derechos y libertades de los ciudadanos[380].

Así las cosas, la *Human Rights Act 1998,* supone una declaración de derechos y libertades públicas. En este sentido, puede afirmarse su posición como cuerpo legal donde se

---

[376] *Ibid*., p. 184.

[377] Cfr. SMITH. "The Human Rights Act 1998 (1) The Human Rights Act and the Criminal Lawyer: The Constitutional Context", en *Criminal Law Review*, Sweet and Maxwell, London, 1999, p. 251.

[378] Cfr. HICKMAN. *Public Law after the Human Rights Act,* Hart Publishing, Oxford, 2011, p. 22.

[379] BINGHAM critica la incapacidad de los tribunales para llevar a cabo una protección efectiva de los derechos y libertades de los ciudadanos principalmente, según expone, por la incapacidad de los sucesivos gobiernos respecto de la incorporación del Convenio Europeo de Derechos Humanos. Cfr. "The European Convention of Human Rights – Time to incorporate", ob. cit., p. 390.

[380] Cfr. CORRECHER MIRA. *Principio de legalidad penal: ley formal vs. law in action*, ob. cit., pp. 186-187.

recogen los derechos y la libertades públicas del ciudadano, pero también las obligaciones de dicho Estado respecto de la creación de las instituciones jurídicas necesarias para salvaguardar las garantías expuestas. Igualmente, puede considerarse la *Human Rights Act* 1998 como una declaración de derechos en relación con los presupuestos constitucionales inspiradores de una texto de estas características en el ámbito jurídico del *common law*[381]. En primer lugar, se le confiere una categoría superior que a las leyes ordinarias, en la medida en que toda disposición contraria a su contenido requiere de su corrección, estableciéndose en caso contrario su inaplicabilidad. Asimismo, la aprobación de la HRA supone la creación de una serie de herramientas jurídicas destinadas a garantizar la compatibilidad del conjunto del sistema legal con su contenido, De igual modo, se la otorga a sus disposiciones un carácter privilegiado, en tanto que las posibles modificaciones o enmiendas a su contenido son más difíciles de realizar que en el caso de la legislación ordinaria. Finalmente, su articulado contiene el reconocimiento de una serie de principios programáticos enfocados a actuar como criterios orientadores del conjunto del ordenamiento jurídico, tales como el respeto al sistema democrático o el reconocimiento de una serie de derechos y libertades que orienten la convivencia en el medio social. Por lo tanto, puede considerarse la importancia a efectos constitucionales de la HRA, dado que su contenido termina estableciendo una serie de pautas político-constitucionales de innegable incidencia en el conjunto del ordenamiento jurídico[382].

Por lo tanto, para entender la incidencia de la *Human Rights Act 1998* en el ordenamiento jurídico británico, expondremos a continuación las herramientas jurídicas implementadas por ésta, en tanto que modifican los fundamentos propios de un sistema legal propio del *common law*. En el apartado siguiente, se hará referencia a la posición asumida por el *case law* de los tribunales británicos en la interpretación-aplicación del acervo jurisprudencial del TEDH, puesto que la HRA determina que los órganos jurisdiccionales

[381] Cfr. KAVANAGH. *Constitutional Review under the UK Human Rights Act,* Cambridge University press, Cambridge, 2009, pp. 307-309; RAZ. "On the Authority and Interpretation of Constitutions: Some preliminaries", en *Constitutionalism. Philosophical Foundations,* (Alexander, L. Ed.)*,* Cambridge University Press, Cambridge, 1998, pp. 152-194.

[382] Cfr. CORRECHER MIRA. *Principio de legalidad penal: ley formal vs. law in action*, ob. cit., p. 189.

internos, en lo relativo a la exegesis del contenido de la *Human Rights Act 1998* debe tomar en consideración lo dispuesto por el TEDH.

b) La incorporación de la jurisprudencia del TEDH por los tribunales británicos respecto a la interpretación de los derechos y libertades del Convenio

La sección 2 (1) de la HRA[383], relativa a la interpretación de los derechos y libertades propios del Convenio Europeo de Derechos Humanos, considera que dicha interpretación debe encontrarse vinculada a la correspondiente línea jurisprudencial del Tribunal Europeo de Derechos Humanos en relación con supuestos donde sea invocada una disposición normativa del Convenio incorporada por la HRA. Así pues, la *s. 2 (1)* de la *Human Rights Act 1998* dispone:

> *s. 2 (1) Interpretation of Convention rights*
>
> *A Court or tribunal determining a question which has arisen in connection with a Convention right must take into account any:*
>
> *a) judgement, decisión, declaration or advisory opinión of the European Court of Human Rights*

De acuerdo con lo expuesto, la s. 2 (1) dispone la vinculación de los tribunales británicos a la interpretación realizada en el *case law* del Tribunal Europea de Derechos Humanos. Si bien ésta no será completamente prescriptiva, en tanto que la fórmula *take into account* no supone una obligatoriedad, sino más bien una recomendación, sí puede reconocerse un efecto persuasivo de los criterios interpretativos desarrollados por el TEDH en su implementación por los órganos jurisdiccionales internos. En consecuencia, la línea jurisprudencial seguida por el Tribunal de Estrasburgo representa un punto de partida para la interpretación-aplicación desarrollada por los tribunales internos, si bien ésta será modulada atendiendo al contexto de aplicación de la norma[384]. En consecuencia, los derechos y libertades

[383] En la legislación británica, las secciones de las disposiciones normativos incorporan una suerte de exposición de motivos y disposiciones adicionales y transitorias, siendo un marco explicativo sobre las necesidades, alcance y criterios de la norma a la que preceden.

[384] Cfr. FELDMAN. *English Public Law*, Oxford University Press, Oxford, 2009, p. 329.

de la Convención incorporados al ordenamiento jurídico británico mediante la *Human Rights Act 1998*, así como la interpretación de éstos desarrollada por el TEDH, pasa a ser un estándar mínimo de garantía que deberá ser asumido por los órganos jurisdiccionales británicos[385].

Este sistema contribuye al carácter dinámico y evolutivo de los derechos y libertades reconocidos en el CEDH, realizando además una armonización en la incorporación de la *Human Rights Act 1998* que respeta el margen de apreciación propio de los órganos jurisdiccionales británicos. Esta discrecionalidad puede permitir en supuestos concretos una interpretación divergente con la dispuesta por el Tribunal de Estrasburgo, en casos donde ésta sea necesaria para garantizar una protección efectiva de los derechos y libertades contenidos en el Convenio[386]. Si bien es cierto que, en cualquier caso, lo convenido en la HRA supone ampliar las funciones de los jueces británicos en tanto que se les obliga a estar al corriente de la más reciente jurisprudencia dictada en Estrasburgo, esta fórmula es la única idónea para, de una parte, homogeneizar el derecho y, de otra, asegurarse de que su interpretación evoluciona, haciéndolo coherente con las circunstancias sociales, culturales y económicas del momento. Estas obligaciones para los tribunales al interpretar la Ley se aplican en todo momento, cuando interpreten cualquier materia relacionada con los derechos del CEDH, tanto en la jurisdicción civil como en la penal, y por supuesto también a la hora de interpretar las disposiciones de la *Data Protection Act 1998*[387].

Todo ello en plena consonancia con el concepto anglosajón *rule of law,* que obliga a adoptar una postura balanceada que permita integrar todas estas perspectivas para dotar de coherencia el ordenamiento jurídico británico, de marcado carácter dual. Así, si bien es necesario el respeto a la naturaleza procedimental de las normas jurídicas para asegurar su

---

[385] Cfr. GROSZ/BEATSON/DUFFY. *Human Rights. The 1998 Act and the European Convention*, Sweet and Maxwell, London, 2000, p. 17.

[386] Cfr. CORRECHER MIRA. *Principio de legalidad penal: ley formal vs. law in action*, ob. cit., p. 191.

[387] Así lo advirtió la ICO en 2001 en la *Guidance* que pretendía informar de la situación que estaba a punto de cambiar: "*The full effect of the Human Rights Act on our legal system, and on society as a whole, has yet to felt. It is however, clear, that the role of information in our society makes it increasingly important to develop respect among data controllers for the private lives of individuals and to ensure good information handling practice. The Human Rights Act, and in particular Articles 8 and 10 of the European Convention on Human Rights, provide the legal framework within which interpretation of the Act, and the data protection principles which underpin it, can be developed*".

validez formal, no puede negarse, de acuerdo con la propia naturaleza evolutiva del *common law*, la importancia de la interpretación y aplicación de las normas jurídicas realizada por los tribunales.

En este sentido, centrando el discurso en el objeto de esta investigación, es indudable que la protección de la privacidad requiere de un marco legal aprobado de acuerdo con un procedimiento formal que lo dote de vigencia. No obstante, la propia realidad jurídica, cambiante en disciplinas en constante evolución como la protección de datos, más en el líquido contexto del *Big data*, requiere de los tribunales una función interpretativa coherente con el concepto *rule of law* entendido como marco de referencia para garantizar los derechos y libertades de los ciudadanos.

De este modo, la exposición seguida en estas páginas muestra de qué manera la interpretación y aplicación de las normas -por ejemplo, en materia de protección de datos- en un sistema propio del *common law* requieren de una actividad de los tribunales donde se integre dentro de la interpretación de la norma la necesidad de proteger la privacidad, entendiendo éste como el criterio que determina el concepto *rule of law* desde la perspectiva dual presentada en estas páginas.

c) La interpretación del ordenamiento jurídico británico de acuerdo con la Human Rights Act 1998: supuestos de incompatibilidad

A continuación, pasará a exponerse el contenido de las secciones 3 y 4 previas al articulado propiamente dicho de la Human Rights *Act 1998*. Éstas engloban una serie de criterios orientadores que prescriben a los tribunales británicos a interpretar el conjunto de la legislación de acuerdo con el articulado del Convenio, incorporado al ordenamiento jurídico británico por la *Human Rights Act 1998*. De este modo, la HRA lleva a cabo una reformulación del ordenamiento jurídico británico lo que, como después se verá, hace mella no sólo en la garantía efectiva de la privacidad y de los datos personales, sino también en el sistema de relaciones entre el poder legislativo y judicial, en tanto que las interpretaciones de estos últimos

conforme a lo dispuesto en la HRA pueden conllevar alteraciones sustanciales respecto de la normativa emanada del legislador.

Las citadas secciones establecen las siguientes disposiciones:

s.3 (1) Interpretation of legislation

"So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention Rights"

s. 4 (2) Declaration of incompatibility

"If the court is satisfied that the provision is incompatible with a Convention right, it may make a declaration of that incompatibility."

Antes de la aprobación de la *Human Rights Act 1998*, los tribunales británicos acudían al CEDH exclusivamente con carácter consultivo para resolver, en su caso, aquéllas dudas que pudiesen surgir de la interpretación de dicha normativa. Así las cosas, la s.3 (1) supone un cambio significativo en esta materia, en tanto que prescribe el requerimiento a los órganos jurisdiccionales para la interpretación de la legislación interna de acuerdo con el articulado de Convenio, en tanto que los derechos y libertades reconocidos en ésta han pasado a informar el Derecho británico gracias a la aprobación de la HRA. En consecuencia, la s. 3 (1) atribuye a los tribunales la legitimidad para reconstruir la legislación británica a partir de los principios programáticos establecidos en el marco de referencia del binomio CEDH-HRA.

A partir de entonces, el CEDH se configura como un instrumento orientador para los tribunales británicos que, mediante el *case law*, deben adaptar el ordenamiento jurídico británico a sus disposiciones[388]. Sin embargo, ésta no es una potestad absoluta, puesto que encuentra una restricción formal en los supuestos donde pueda observarse por el poder legislativo una aplicación errónea por parte de los tribunales que exceda el contenido

[388]Asumiendo así la posición que ARDEN denomina como "living instrument". Cfr. "Criminal Law at the Crossroads: The Impact of Human Rights from the Law Commission's Perspective ant The Need for a Code", *Criminal Law Review,* Sweet and Maxwell, London, 1999, p. 447.

fundamental de la norma objeto de interpretación. En estos supuestos problemáticos, se abre la posibilidad de establecer una nueva redacción por el Parlamento para garantizar el retorno al significado legislativo inicial.

Sobre esta cuestión, resulta pertinente analizar el *case law* más relevante respecto de la s.3 (1), a efectos de delimitar el alcance que los tribunales británicos asignan a la interpretación conforme al Convenio de la legislación británica. Como *leading case* puede citarse lo dispuesto en *Ghaidan v. Godin-Mendoza*[389], donde pasa a considerarse que el mandato de la s.3 (1) es prescriptivo, requiriendo a los órganos jurisdiccionales a realizar una aplicación extensiva de la protección de los derechos y libertades recogidos en el Convenio. En este sentido, puede llegarse si fuera necesario a modificar parcialmente el sentido del cuerpo legislativo objeto de interpretación. Sin embargo, esta posible modificación por la vía de la interpretación jurisprudencial no puede suponer una modificación sustancial de los fundamentos de la disposición objeto de interpretación[390]. Por lo tanto, el resultado de la interpretación debe ser compatible con el cuerpo normativo previo[391].

Asimismo, otro de los límites a la s.3 (1) establecidos en el caso *Ghaidan v. Godin-Mendoza*[392] hace referencia a los supuestos donde no sea posible realizar una interpretación de acuerdo con el contenido del Convenio[393]. Esta limitación remite a los supuestos de modificación de la voluntad fundamental de la legislación, cambio completo en el carácter sustantivo de la norma o violación de los principios inspiradores de la legislación objeto de interpretación. Sobre esta cuestión, destaca la reflexión introducida en *Attorney General's Reference (No. 4 of 2002)* sobre las limitaciones a la s.3 (1) recogidas en *Ghaidan v. Godin-Mendoza*, considerando la vaguedad y falta de determinación de las posibles limitaciones a la

[389] *Ghaidan v. Godin-Mendoza* [2004] UKHL para. 30.

[390] Cfr. ASHWORTH, *et al*, *Human Rights and Criminal Justice*, ob. cit., p.188.

[391] Cfr. CORRECHER MIRA. *Principio de legalidad penal: ley formal vs. law in action*, ob. cit., p. 194.

[392] *Ghaidan v. Godin-Mendoza*, para. 33, 49,110-113 y 116.

[393] En relación con dichos supuestos, los ponentes del caso *Ghaidan v. Godin-Mendoza* acudieron al *case law* de *R. v Secretary of State for the Home Department* [2002] UKHL 46 y *Bellinger v. Bellinger* [2003] UKHL 21 para construir su veredicto.

interpretación conforme a la s.3 (1). Así las cosas, considera que la excesiva amplitud de estos supuestos requiere de un atento análisis por parte de los tribunales, para así garantizar que la interpretación sea efectivamente realizada conforme a los derechos y libertades del CEDH, como así dispone la s.3 (1) HRA[394]. Sin embargo, el establecimiento de determinados deberes al Parlamento es parte consustancial a la s.3 (1) HRA, en tanto que la elaboración de las leyes debe ser realizada de forma que asegure la coherencia de la actividad interpretativa de los tribunales de acuerdo con el articulado del Convenio Europeo de Derechos Humanos.

Pasando a la s.4 (2) HRA, ésta atribuye la potestad a los tribunales superiores para la realización de declaraciones de incompatibilidad cuando una ley no pueda ser interpretada atendiendo a las disposiciones del Convenio[395]. Esta posibilidad es indispensable para analizar el equilibro constitucional entre la soberanía parlamentaria y la protección judicial de los derechos y libertades recogidos en el Convenio de acuerdo con el nuevo escenario delimitado por la *Human Rights Act 1998*.

d) La complementariedad entre el respeto a la soberanía parlamentaria y la actividad interpretativa del case law

La aprobación de la *Human Rights Act 1998* supone la necesidad de repensar la relación entre parlamento y tribunales en el proceso de aprobación de los cuerpos legales, así como en su sucesiva interpretación por el *case law*. En este nuevo estado de cosas, resulta necesario determinar un modelo de complementariedad que permita respetar la soberanía parlamentaria, pero también mantener el poder adjudicativo propio de los tribunales en su actividad interpretativa de las disposiciones normativas. Para armonizar esta doble perspectiva, la doctrina británica ha desarrollado un esquema de correlación entre poderes conocido como *democratic dialogue*[396].

---

[394] Cfr. CORRECHER MIRA. *Principio de legalidad penal: ley formal vs. law in action*, ob. cit., p. 195.

[395] Se reconocen como tribunales superiores, de acuerdo con la s. 4 (5), para la realización de la declaración de incompatibilidad los siguientes órganos: *House of Lords, Privy Council, Courts-Martial Appeal Court, Court of Appeal, High Court*. En Escocia, la *Hight Court of Justiciary*.

[396] Sobre este concepto, pueden destacarse las siguientes referencias, pertenecientes a la doctrina constitucionalista británica: YOUNG. *Parliamentary Sovereignty and the Human Rights Act*, Hart Publishing, Oxford, 2009; HICKMAN.

Esta dinámica parte de la consideración de la HRA como una declaración de derechos y libertades asumida por los poderes públicos y los tribunales británicos. La coincidencia de la *Human Rights Act 1998* con el catálogo de derechos propio del CEDH no representa en ningún caso considerar la HRA como un texto internacional, sino que su implementación en el ordenamiento jurídico británico supone que de pleno derecho se entienda como normativa interna. Esto, añadido a las reglas de interpretación que para los jueces se derivan conforme a la jurisprudencia del TEDH, propicia que efectivamente pueda hablarse de un modelo de dialogo democrático entre la soberanía parlamentaria y el *case law* para la interpretación de su contenido. Sin embargo, los autores críticos con este modelo reprochan que ello resultaría imposible si se eleva a estatus internacional a la HRA[397].

A nivel teórico, la fórmula del *democratic dialogue* supone la existencia de un marco de referencia donde soberanía parlamentaria en la elaboración de los cuerpos legales y la actividad interpretativa del *case law* destinada a construir el sistema de derechos y libertades propio de la HRA puedan actuar de forma complementaria y coordinada. El marco normativo resultante de la HRA, a partir de las secciones 3 (1) y 4 (2) anteriormente expuesta permite esta complementariedad.

Así pues, la s.3 (1) otorga la potestad a los tribunales en el ejercicio de su función interpretativa y dinamizadora en la protección de los derechos y libertades recogidas en el Convenio, imponiéndoles la obligación de aplicar el derecho anglosajón de acuerdo con las garantías incorporadas por la *Human Rights Act 1998*[398]. Asimismo, como contrapeso, la s.4 (2) actúa como contrapartida para el poder legislativo, en tanto que la previa declaración de

---

"Constitutional Dialogue, Constitutional Theories and the Human Rights Act 1998", en *Public Law,* Sweet and Maxwell, London, 2005, p. 306; CLAYTON. "Judicial Deference and Democratic Dialogue: the Legitimacy of Judicial Intervention under the Human Rights Act 1998", en *Public Law,* Sweet and Maxwell, London, 2004, p. 33. En su exposición sobre la *Human Rights Act 1998* desde el punto de vista del Derecho penal británico, CORRECHER MIRA traduce el concepto como "diálogo democrático". Cfr. *Principio de legalidad penal: ley formal vs. law in action*, ob. cit., pp. 196 ss.

[397] Crítico, EKINS niega que, a partir de la entrada en vigor de la HRA, exista un diálogo efectivo entre el poder legislativo y judicial en términos de interpretación y compatibilidad de la legislación británica. Y es que el autor, pese a la fórmula y justificación de la HRA, no acaba de creer que su contenido sea autónomo sino que considera que contenido viene impuesto por una instancia supranacional. Cfr. "Right-Consistent Interpretation and The Human Rights Act 1998", en *Law Quarterly Review*, Sweet and Maxwell, London, 2011, pp. 227-230.

[398] Cfr. YOUNG. *Parliamentary Sovereignty and the Human Rights Act*, ob. cit., p. 145.

incompatibilidad por los tribunales, supone un reconocimiento de la potestad de la soberanía parlamentaria para emprender las modificaciones legislativas necesarias para adecuar el cuerpo legal a las disposiciones del Convenio[399]. En consecuencia, la soberanía parlamentaria aparece como elemento corrector de las vulneraciones de derechos y libertades detectadas por los tribunales, en los casos más importantes donde sea posible desarrollar una interpretación conforme al CEDH de acuerdo con la s.3 (1)[400].

Así las cosas, este modelo de *democratic dialogue* puede variar en función del alcance de las potestades conferidas a las instituciones legislativas y judiciales, así como en relación con la interpretación ofrecida a las s. 3 (1) y s. 4 (2). Si fuera extensiva la competencia conferida en la s. 3 (1), ofreciendo una mayor potestad interpretativa a los tribunales, daría como resultante un marco donde la iniciativa de este diálogo correspondería al *case law*[401]. Contrariamente, si se restringe la regla contenida en la s. 3 (1), remitiendo de forma expresa a una expansión de la declaración de incompatibilidad recogida en la s. 4 (2), podría ofrecerse un mayor punto de contacto para el establecimiento del diálogo entre ambas instituciones, en tanto que recaería en la soberanía parlamentaria la posibilidad de decidir sobre la incompatibilidad previamente declarada por los tribunales. En todo caso, para contrarrestar la posible situación de desigualdad entre ambas instituciones, es necesario asegurar una relación complementaria en los dos ámbitos, para garantizar la protección de los derechos y libertades de la ciudadanía, pero también el respeto a la soberanía parlamentaria[402]. De acuerdo con lo expuesto, es indispensable un compromiso institucional de las partes implicadas, de forma que el *democratic dialogue* termine convirtiéndose en un espacio donde la soberanía parlamentaria y el *case law* antepongan sus prerrogativas para conseguir la solución más satisfactoria para

[399] *Ibidem.*

[400] Cfr. CORRECHER MIRA. *Principio de legalidad penal: ley formal vs. law in action*, ob. cit., p. 198.

[401] Cfr. PHILIPSON. "(Mis) representing section 3 of the Human Rights Act 1998", en *Law Quarterly Review,* Sweet and Maxwell, London, 2003, p. 187.

[402] HICKMAN incide en la necesidad de afianzar el diálogo democrático entre las instituciones legislativas y judiciales, como único marco posible en que podría producirse un equilibrio apropiado. Cfr. "Constitutional Dialogue, Constitutional Theories…" ob. cit., p. 306.

garantizar los derechos y libertades recogidos en el CEDH, de acuerdo con el respeto a los procedimientos y la asunción de las funciones legitimas de ambas instituciones[403].

e) El derecho a la vida privada

El derecho a la vida privada queda reconocido explícitamente en el Artículo 8 de la *Human Rights Act 1998* el cual, asimismo, reproduce literalmente el contenido del Artículo 8 del Convenio Europeo de Derechos Humanos. Ambos textos tienen la siguiente redacción:

> *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 sino en tanto en cuanto 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 los demás.*

El objetivo general de este precepto es múltiple y variado pero cuyo denominador común redunda en la protección de la esfera personal de un individuo, es decir, su identidad, su autonomía, su integridad física y moral, su privacidad así como el mantenimiento de las relaciones con el resto de la sociedad en un lugar seguro y libre de injerencias[404] salvo en algunas circunstancias y por motivos tasados.

Desde un punto de vista formal el artículo 8 comprende cuatro elementos: vida privada, vida familiar, hogar y correspondencia pero, sin embargo, son muchas las facetas que incorpora en su protección, desde la identidad sexual hasta la protección frente al almacenamiento, procesamiento y publicación de los datos personales. En cuanto este último aspecto, cuando

[403] Cfr. YOUNG. *Parliamentary Sovereignty and the Human Rights Act*, ob. cit., p. 130.

[404] *Connors v. United Kingdom* [2005] 40 EHRR 9.

dichas acciones se llevan a cabo sin el consentimiento del interesado, se produce directamente una vulneración del artículo 8[405] pues la jurisprudencia del TEDH considera los datos personales como un aspecto fundamental del disfrute de cualquier persona de su privacidad.

i. Contenido

Examinando el contenido literal del precepto puede claramente atisbarse el empleo de términos muy genéricos como "vida privada" o "injerencia" sin añadir nada más a dichas definiciones. La brevedad de la referencia ha hecho necesario que la jurisprudencia desarrolle y perfile el contenido de dicho precepto en numerosas ocasiones.

Una definición expresa de estos términos no se ofrece tampoco por el Tribunal Europeo de Derechos Humanos, aunque su jurisprudencia ha proporcionado toda una doctrina interpretativa de los conceptos y límites de su contenido, por lo que a lo largo de este Capítulo se hará referencia a distintas sentencias del TEDH que han concedido virtualidad al Artículo 8 de la HRA así como dotado de contenido su articulado. Así por ejemplo, respecto del concepto "vida privada", encontramos varias sentencias que, sin ofrecer una definición concreta del término[406], ayudan a discernir en el caso concreto, su contenido. A grandes rasgos, la jurisprudencia del Tribunal ha impregnado la noción de vida privada con la identidad y el desarrollo personal, autonomía, la integridad física y psicológica, la dignidad, el género, el nombre, la orientación y vida sexual, la salud y las relaciones personales[407].

Valga decir que esta redacción del Artículo 8 en términos puramente descriptivos no es un caso aislado ni tampoco es casualidad sino que obedece a una estrategia global garantista

[405] *Z v. Finland* [1997] 25 EHRR 371.

[406] El propio Tribunal de Estrasburgo ha reiterado en numerosas ocasiones que "vida privada" es un término no susceptible de una definición exhaustiva, incluso ha incidido en la importancia de no ofrecer una definición precisa que acabe por restringir su contenido.

[407] Estas distintas facetas del artículo 8 pueden observarse a través de la distinta jurisprudencia al respecto, entre otras, el caso *Niemietz v. Germany* [1992] 16 EHRR 97, donde el TEDH advirtió de que el concepto "vida privada" no podía quedar limitado al círculo personal en el que un individuo elige vivir su vida, sino que debe ir más allá, abarcando un círculo mayor en el que una persona se relaciona con otras; la sentencia *Gillan v. UK* [2010], donde la Corte de Estrasburgo afirmó que este derecho incluía la búsqueda de los orígenes personales, en relación con el desarrollo de la personalidad individual; el caso *Botta v. Italy* [1998] 26 EHRR 241, donde este precepto se enfocaba hacia el derecho a la autodeterminación personal; o el caso *Tysiac v. Poland* [2007] 22 BHRC 155 en el que se ponía de relieve el alcance a la integridad física o moral.

pues, en materia de Derechos Humanos, suelen emplearse definiciones escuetas en el articulado jurídico, principalmente para facilitar su aplicación al máximo de supuestos inimaginables. Así, se evita limitar el ámbito de protección mediante la introducción de notas características o requisitos que puedan inutilizar la aplicación del derecho a futuras circunstancias.

Es decir, mediante una redacción sucinta, el CEDH intenta consagrar el contenido mínimo o esencial de los derechos en términos suficientemente amplios para que sea el órgano legislativo estatal correspondiente quien los desarrolle mediante formulaciones concretas. Otra cuestión distinta es si, las legislaciones domésticas no incorporan más detalladamente y conforme a sus estándares nacionales estos derechos y libertades que, igualmente serán realizables y exigibles ante los Tribunales, pudiendo ello indicar una falta deliberada de su garantía pero no su inexistencia o ineficacia.

Un segundo motivo que subyace en la brevedad enunciativa de los derechos de la HRA así como del Convenio Europeo de Derechos Humanos es su aplicabilidad futura y su voluntad de permanencia, pues no hay que olvidar las heterogéneas tradiciones jurídicas que imperan en los diferentes estados nacionales y la evolución del contexto histórico y los sistemas jurídicos en los que resultará de aplicación un derecho subjetivo.

Así, mientras que el legislador español constriñe la protección a la esfera de la intimidad, el derecho inglés no tiene una noción equivalente por lo que, conceptos como el derecho a la vida privada difieren notablemente, aunque todos ellos estén relacionados con el derecho a la privacidad (el derecho al honor, el derecho a vivir sin rumores, alejados de la esfera pública…). Y, en consecuencia, el artículo 8 comprende aspectos como, por ejemplo, el derecho a desarrollar libremente una personalidad propia, sin injerencias de otros.

Por todo ello, y como se incidirá más adelante, la jurisprudencia del Tribunal Europeo de Derechos Humanos es muy valiosa y resulta esencial en la configuración de los derechos recogidos en la HRA, motivo por el cual este instrumento jurídico ha marcado un antes y un después para, en lo que aquí nos interesa, la protección de la privacidad en Reino Unido.

Pasando a examinar el contenido del artículo 8 de la HRA, una primera aproximación nos dice que el término "vida privada" comprende elementos tan importantes como la identificación del género, nombre, orientación sexual y vida sexual. La jurisprudencia ha matizado que en ella se integra también la salud mental, como un elemento esencial de la vida privada, asociado con el aspecto de la identidad moral[408].

No debe interpretarse este precepto como un derecho a no ser molestado, pues el individuo por naturaleza convive en sociedad[409], por lo que una noción del derecho a la privacidad que protegiese el individuo sólo frente a interferencias ajenas restringe su contenido potencial. Ahora bien, el artículo 8 exige "respeto" para la vida privada, lo que significa que no toda interferencia en ella supondrá una vulneración de este precepto si se cuenta con el consentimiento del individuo, cuya ausencia podría suponer una interferencia injustificada. Este consentimiento debe prestarse libremente y ser cierto, lo que implícitamente comporta que se preste conforme a las garantías que el derecho prevé para garantizar una elección válida.

Así por ejemplo, una condena penal no supone por sí misma una interferencia con la "vida privada", pues el Artículo 8 no protege al individuo frente a una pérdida de reputación que tiene lugar por una mala praxis del sujeto o cuando se trate de un acto u omisión que haya tenido lugar respecto de una persona con un cargo público en el ejercicio de sus deberes[410].

En cuanto a las instantáneas fotográficas o las videograbaciones, éstas dependen de varios factores: si se han tomado con el consentimiento del interesado, si se carece de dicho consentimiento pero se han tomado en la vía pública[411], si se trata de menores de edad[412], si se

---

[408] *Peck v. United Kingdom*, de 28 de enero de 2003, (App. 44647(98), [2003] ECHR 44, (2003) 36 EHRR 41, [2003] 36 EHRR 719.

[409] "*It would be too restrictive to limit the notion [of private life] to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also compromise to a certain degree the right to establish and develop relationships with other human beings*", *Niemietz v. Germany*, de 16 de diciembre, [1992] 16 EHRR 97.

[410] *Gillberg v. Sweden*, de 3 de abril de 2012, (App. 41723/06), [2012] (GC).

[411] *Friel v. Austria*, de 31 de enero de 1995, Series A Nº305 B, [1995] 21 EHRR 83.

[412] *Reklos v. Greece*, de 15 de enero de 2009, [2009] EMLR 16.

trata de un personaje público[413], si son necesarias por razones de interés público[414], si son convenientes para ilustrar una noticia[415]… es decir, conviene llevar a cabo una ponderación de derechos en tanto que su ejercicio produce incidencias en otras libertades fundamentales.

No obstante, el Tribunal Europeo de Derechos Humanos ha especificado que, pese a que el contenido esencial del artículo 8 trata de proteger a las personas de cualquier injerencia por parte de los poderes públicos, matiza que estas intromisiones deberán de ser arbitrarias[416]. Es decir, el precepto aludido no impide al Estado realizar determinadas interferencias siempre que tengan el propósito de mantener el respeto al ámbito privado y familiar de los sujetos entre sí cuando las circunstancias sociales y los intereses de otros individuales así lo aconsejen[417].

En otros casos, el derecho a la vida privada puede comprender la obligación de un Estado de proporcionar toda la información que posea sobre un individuo a fin de determinar aspectos fundamentales de su identidad y personalidad[418] o bien para proteger a su familia[419] o bien para conocer cual es el estado de su salud[420].

Así pues, el artículo 8 comporta obligaciones negativas pero también positivas para las autoridades públicas[421] que deben respetar los derechos comprendidos bajo el precepto y, al mismo tiempo, protegerlos activamente mediante la introducción de acciones públicas de toda índole[422]. Este aspecto dual le ha dado al precepto gran parte de su notoriedad, tanto en el

---

[413] *Von Hannover v. Germany*, de 24 de junio de 2004, [2004] 24 ECHR 294.

[414] *Peck v. United Kingdom*, de 28 de enero de 2003, (App. 44647(98), [2003] ECHR 44, (2003) 36 EHRR 41, [2003] 36 EHRR 719.

[415] *Gurgenidze v. Georgia*, de 17 de octubre, [2006] 71678/01.

[416] *Dickson v. United Kingdom* (App. 44362/04), 4 de Diciembre de 2007 [GC], [2008] 46 EHRR 927, ECHR 2007-XIII.

[417] *Babylonová v. Slovakia*, (App. 69146/01), 20 de Junio de 2006, [2008] 46 EHRR 183, ECHR 2006-VIII.

[418] *Gaskin v. United Kingdom*, de 7 de julio de 1989, [1989] 12 EHRR 36.

[419] *Guerra v. Italy* [1998] 26 EHRR 357, sobre el derecho de acceso a la información sobre el riesgo medioambiental.

[420] En *McGinley v. United Kingdom,* de 19 de febrero de 1998, [1999] 27 EHRR 1, se obligó al gobierno británico a facilitar a un empleado público los datos sobre los niveles de radioactividad a los que había estado expuesto por razón de su trabajo.

[421] Estas obligaciones positivas pueden ser de la más diversa índole pudiendo consistir, por ejemplo, en medidas legislativas encaminadas a garantizar el consentimiento informado (*MAK and RK v. United Kingdom*, de 23 de marzo de 2010, [2010] ECHR 363) o a la prevención de la violencia doméstica (*A v. Croatia*, de 14 de octubre de 2010, App. 55164/08).

[422] Así, en el caso *X and Y v. the Netherlands*, de 26 de marzo de 1985, ECHR 4 [1985] 8 EHRR 235, el TEDH afirmó: "*[Article 8] does not merely compel the state to abstain from interference: in addition to this primarily negative*

derecho europeo como en el doméstico pues, desde las primeras decisiones en virtud del artículo 8 que reconocían obligaciones positivas cuando se derivaban consecuencias graves para los derechos fundamentales, el aspecto positivo de éste ha representado una parte muy significativa de la jurisprudencia del TEDH[423].

Este carácter dual del precepto se manifiesta en tanto que abarca tanto acciones de los ciudadanos contra los poderes públicos como intereses entre particulares[424], en lo que se denomina efecto horizontal[425]. Esta extensión del artículo 8 hacia las disputas entre particulares ha tenido el apoyo de la jurisprudencia, siendo el caso *X v. The Netherlands* el más significativo llegando a afirmar que "las obligaciones positivas pueden consistir en medidas designadas para asegurar el respeto a la vida privada incluso en las relaciones privadas de los particulares entre ellos"[426].

Asimismo, el paraguas legal del artículo 8 extiende su protección hacía personas jurídicas en algunos casos[427], lo que ha sido un aspecto muy controvertido ya que el Derecho inglés, igual que ocurre con la difamación y la reputación, no reconoce esta protección jurídica más allá de las personas físicas[428]. Sin embargo, debe reconocerse la enorme amplitud y diversidad del precepto en cuestión hasta el punto de reconocerse su aplicabilidad a supuestos

---

undertaking, there may be positive obligations inherent in an effective respect for private and family live […] these obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of relations between individuals themselves".

[423] WADHAM/MOUNTFIELD/PROCHASKA. *Blackstone's guide to The Human Rights Act*, 1998, Oxford University Press, Oxford, 2015, p. 232.

[424] Respecto del debate que originó en su día esta cuestión entre la doctrina anglosajona, dice COOPER que pues que la *Human Rights Act* exige que el Reino Unido tenga en cuenta la jurisprudencia de Estrasburgo, sería contraproducente que no se incorporase el principio de horizontalidad pues, la consecuencia de no hacerlo, sería continuar considerando a los tribunales ingleses como una primera instancia ante el TEDH. Cfr. COOPER. "Horizontality: The Application of Human Rights Standards in Private Disputes", en *An Introduction to Human Rights and the Common Law*, (English/Havers eds.), Hart Publishing, Oxford and Portland (Oregon), 2000, pp. 53-69.

[425] Así lo afirma Lord Hoffman en la sentencia del caso *Campbell v. Mirror Group Newspapers Ldt* [2004] UKHL 22, "*I can see no logical ground for saying that a person should have less protection against a private individual than he would have against the state for the publication of personal information for which there is no justification*".

[426] *X and Y v. the Netherlands*, de 26 de marzo de 1985, ECHR 4 [1985] 8 EHRR 235.

[427] *Wieser and Bicos Beteiligungen v. Austria*, de 16 de enero, [2008] 46 ECHR 54.

[428] Así, por ejemplo, en el caso *Derbyshire County Council v. Times Newspapers*, de 7 de abril de 1993, [1993] AC 534, la Cámara de los Lores determinó que una autoridad pública no puede instar una demanda por ataques a su reputación.

tan extremos como la determinación de una calidad de vida suficiente de acuerdo con la dignidad humana y el desarrollo de la propia personalidad[429].

En otro orden de cosas, el artículo 8 protege dos tipos de información confidencial, por una parte el secreto profesional[430], y en segundo lugar, aquella información privada cuya publicidad pueda causar perjuicios a la persona. Sin embargo esta última faceta también incluye el derecho de toda persona a tener acceso sobre su información personal en según qué casos, pese a que ésta pueda tener consideración de confidencial[431].

Del mismo modo, el Tribunal Europeo de Derechos Humanos ha afirmado que el concepto "vida privada" es lo suficientemente amplio como para comprender en él las actividades de naturaleza profesional y empresarial[432] lo que tiene mucho sentido si pensamos que, es en el curso de su vida laboral, cuando la mayoría de gente tiene una oportunidad significativa, si no la más grande, de desarrollar relaciones con el mundo exterior.

Así, la jurisprudencia ha integrado dentro del término "vida privada" el derecho a un libre desarrollo de la personalidad, lo que incluye el derecho a escoger qué aspectos de la vida quieren mantenerse en una esfera más privada y cuales no[433]. Esto comprende asimismo, el derecho a relacionarse con otros seres humanos, lo que se extiende a un contexto laboral o profesional, pues justamente éste es el ámbito en el que las personas tenemos la mejor oportunidad para establecer relaciones con el resto del mundo.

Otro de los aspectos más importantes del precepto y de sumo interés para la presente disertación es la inclusión del derecho a la protección de datos personales bajo su disposición,

---

[429] Así se determinó en el caso *Pretty v. United Kingdom*, de 29 de abril de 2002, [2002] ECHR 423, en la que el TEDH aceptó la aplicabilidad del artículo 8 en un caso de asistencia al suicidio.

[430] Así lo dispuso la Corte de Estrasburgo en el caso *Kopp v. Switzerland*, de 25 de marzo de 1998, [1998] HRCD 356, en relación con la intervención de las llamadas telefónicas de un abogado con el propósito de investigar ciertos indicios criminales contra su mujer.

[431] Este último extremo se confirmó por el TEDH en el caso *Gaskin v. United Kingdom,* de 7 de julio de 1989, [1989] 12 EHRR 36, cuando al demandante se le denegó acceso a los informes que de su persona tenían las autoridades públicas, bajo cuya custodia había permanecido en la infancia.

[432] *Amann v. Switzerland*, de 12 de enero del 2000, [2000] 30 EHRR 843 y *Rotaru v. Romania*, de 4 de mayo del 2000, [2000] 8 BHRC 449.

[433] *Niemietz v. Germany,* de 16 de diciembre de 1992, (App. 13710/88), Series A nº 251-B, [1992] 16 EHRR 97.

como un elemento integrador de la vida privada de las personas. Así pues, otra de las acciones que puede comportar la vulneración del artículo 8 es recolectar datos personales sin consentimiento del interesado[434] o del mismo modo almacenarlos, tratarlos o procesarlos[435] así como cuando esto se lleva a cabo de manera encubierta por las autoridades públicas, siempre que no haya razones legales que lo justifiquen. Esto último ha comportado numerosos problemas al Reino Unido[436] que se arroga competencias no reglamentarias en estas áreas, lo que ha tratado de solucionar mediante la codificación en estos contextos, como por ejemplo la controvertida *Investigatory Powers Act 2000* sobre la que más adelante se incidirá.

Por supuesto también se incluye aquí la publicación de información personal de los individuos, problema que se ha visto gravemente acuciado con la irrupción de las nuevas tecnologías en la sociedad. Así, se supera el contexto tradicional de los medios de comunicación, que siempre y cuando un contenido tenga razones de interés público no rige la obligación de comunicar previamente al interesado que se va a hacer pública una información sobre su persona[437], y se abren paso nuevas conductas como la publicación en una red social de una fotografía de un grupo de amigos, sin el consentimiento de gran parte de éstos.

Así las cosas, el derecho a la protección de datos se deriva directamente del derecho a la vida privada del artículo 8 del CEDH. El TEDH conviene en que puede haber una interferencia en la vida privada de las personas cuando determinada información es automáticamente recogida y almacenada en ficheros por parte de las autoridades aunque también ha señalado que, de nuevo, hay una delgada línea que separa lo que se considera una actividad "pública" o "privada" pese a que existen nociones de lo que puede suponer una intromisión en el derecho a

---

[434] Como por ejemplo, obligar a un apersona a someterse a un análisis de sangre en un procedimiento de paternidad, en el caso *X v. Austria*, de 13 de diciembre de 1989, [1979] 18 D.R. 154 9, el TEDH estimó que, si bien esto era contrario al artículo 8, estaba justificado y era proporcional.

[435] *S and Marper v. United Kingdom*, de 4 de diciembre de 2008, (GC), (App. 30562/04 y 30566/04), [2008] ECHR 1851, [2009] 48 EHRR 1169.

[436] *Malone v. United Kingdom*, de 26 de abril de 1985, [1985] 7 EHRR 14, *Halford v. United Kingdom*, de 25 de junio de 1997, [1997] 24 EHRR 523, *PG v. United Kingdom,* de 25 de septiembre de 2001, [2001] Po LR 325 o *Copland v. United Kingdom* [2006] 43 EHRR SE5, entre otros.

[437] *Mosley v. United Kingdom*, de 10 de mayo de 2011, [2011] 10 ECHR 774.

la protección de datos: el almacenamiento de huellas dactilares, fotografías y material genético[438] así como las bases de datos médicas[439].

En cuanto al acotamiento de este derecho, el Tribunal ha manifestado que, teniendo en cuenta las circunstancias de cada caso particular, el derecho a tener una vida privada puede verse afectado con independencia de que los datos personales estén almacenados bajo los más altos estándares de seguridad[440] del mismo modo en que se puede infringir el derecho a la protección de datos cuando éstos continúen siendo almacenados, tiempo después, una vez transcurrido el propósito para el que fueron recolectados[441]. También se ha determinado la violación de estos derechos con independencia del interés público para el que fueron almacenados como por ejemplo, la investigación científica o la prevención de delitos[442].

No obstante, en los casos previos nos encontramos con el reconocimiento del derecho a la protección de datos frente a las autoridades públicas, lo que venía siendo la articulación más tradicional del derecho. Hoy en día, y sobre todo teniendo en cuenta el proceder actual de la economía, conviene mencionar que la protección de datos es un derecho ejercible frente a entidades privadas así como organismos autónomos que, por su desarrollo profesional o comercial, tienen almacenadas cantidades ingentes de datos personales.

Ahora bien, ni el derecho a la protección de datos personales ni el derecho a la vida privada ni ninguna otra de las facetas del artículo 8 de la *Human Rights Act 1998* (ni tampoco del CEDH) son absolutos sino que, al entrar en conflicto con otros derechos fundamentales como, por ejemplo, la libertad de expresión o información, exigen de una ponderación de derechos al caso concreto. Es por ello que, como se ha dicho anteriormente, se trata de un derecho de los denominados "cualificados", que pueden sufrir limitaciones en su disfrute en

---

[438] *S and Marper v. United Kingdom*, de 4 de diciembre de 2008, [GC], (App. 30562/04), [2008] ECHR 1851 [2009] 48 EHRR.

[439] *Z v. Finland*, 25 de febrero de 1997, (App. 22009/93), [1997] 25 EHRR 371.

[440] *Leander v. Sweden*, 26 de marzo de 1987, Series A Nº 116, [1987] 9 EHRR 433; o *Turek v. Slovakia,* de 14 de febrero de 2007, (App. 57986/00), [2007] 44 EHRR 861, ECHR 2006-II, entre otros.

[441] *Gardel v. France*, de 17 de diciembre de 2009, (App. 16428/05), ECHR 2009.

[442] *Avilkina and Others v. Russia*, de 6 de junio de 2013, (App. 1585/09) ECHR 2013.

situaciones excepcionales, conforme a la jerarquización que se previó en su configuración en la HRA.

ii. Límites

El derecho a la privacidad no es absoluto, está sujeto al respeto de las leyes y otros derechos y libertades reconocidos con los que pueda colisionar como, por ejemplo, el derecho a la libertad de expresión que, precisamente, es el derecho más invocado para justificar la invasión de la privacidad y que también está garantizado por el artículo 10 de la HRA y del CEDH.

El Tribunal de Estrasburgo se ha pronunciado en numerosos casos en los que ha existido una confrontación directa entre algunos de los derechos reconocidos en el CEDH, principalmente como ha ocurrido con el derecho a una vida privada y el derecho a la libertad de expresión[443], prevista en el artículo 10 del Convenio. Así ocurrió en el famoso caso *Von Hannover*[444] en el que la Princesa Carolina de Mónaco interpuso una demanda contra los Tribunales alemanes por permitir la publicación de unas fotografías que, según entendía la demandante, atentaban contra su derecho a la vida privada. A resultas de este caso, el TEDH insistió en que debía diferenciarse entre aquellas fotografías que se publican con la mera intención de satisfacer la curiosidad de los lectores sobre la vida de determinada persona, y aquellas que, pese a ser controvertidas, contribuyen al debate en una sociedad democrática, exponiendo cómo viven algunos personajes públicos, por ser una información de interés público.

En otra ocasión, en un asunto similar, el Tribunal de Estrasburgo consideró que, hacer pública una fotografía que acompaña a una información, cuando no hay nada relevante en ella ni nada aporta a lo que se está relatando, supone una intromisión en el derecho a la vida privada

[443] Sobre esta cuestión, resulta muy interesante el análisis llevado a cabo por ERDOS en torno al ensemblaje del derecho a la protección de datos con las libertades expresivas. Cfr. "Confused? Analysing the Scope of Freedom of Speech protection vis-à-vis European Data Protection", en *Oxford Legal Studies Research Paper,* nº 48, 2012.

[444] *Von Hannover v. Germany,* de 7de febrero de 2012, (Nº 2), (App. 40660/08 y 60641/08), [GC] ECHR 2012.

ya que dicha fotografía carece de valor por sí misma[445], lo que ejemplifica la divergencia de soluciones según las circunstancias concretas del caso.

En cuanto a la HRA, conviene destacar la distinción que se lleva a cabo entre los "*absolute rights*" (como el derecho a la vida o la prohibición de tortura, artículos 2 y 3 respectivamente) cuya protección es absoluta y sin excepciones o intromisiones de ningún tipo y los "*qualified rights*" (como los artículos 8 y 10) que permiten ciertas limitaciones cuando colisionan frontalmente con otros derechos reconocidos en el Convenio y el caso concreto lo justifique. Así, ambos derechos están considerados como derechos cualificados la cual cosa implica que su contenido puede verse restringido según las circunstancias del caso. Cada uno protege a las personas contra las interferencias del Estado u otras terceras personas, ambos derechos no son derogables en casos de emergencia y tampoco se expresan en términos absolutos.

La propia HRA, en su Sección 12, dispone que los Tribunales deben tener especial cuidado con la importancia del derecho a la libertad de expresión, disponiendo asimismo, algunas directrices en favor de los medios de comunicación[446]. Esta colisión de derechos queda patente también en la legislación relativa a los datos personales como la Data Protection Act 1998 que incluye ciertas exenciones entre sus principios de protección.

Debido al lobby de la prensa, con mucha tradición y fuerza en Reino Unido, se introdujo en la HRA dicha Sección 12 para tratar de equilibrar los eventuales conflictos que pudieran surgir entre el artículo 8 y el derecho a la privacidad, y el artículo 10 y el derecho a la libertad de expresión[447]. Y así añade expresamente que, a la hora de realizar una ponderación, los tribunales "deberán tener particularmente en cuenta la importancia del derecho del CEDH a la libertad de expresión" en los procedimientos relacionados con materiales o propósitos

[445] *Khuzhin and others v. Russia*, de 23 de octubre de 2008, (App. 1347/02).

[446] Por ejemplo, autoriza a los medios de comunicación la publicación de sus materiales siempre que puedan probar la existencia de un interés público.

[447] Así, el artículo 12 de la HRA es, en puridad, una norma procedimental que fue introducida debido a la presión ejercida por los propietarios de los medios de comunicación para evitar la aprobación de una ley sobre privacidad. PAUNER CHULVI. "Privacidad y periodismo: el escándalo Murdoch sobre escuchas telefónicas en News of the World", en *Revista de Derecho Político*, nº 88, 2013, p. 255.

periodísticos, literarios o artísticos. Con ello parece otorgársele cierta notoriedad o preponderancia a la libertad de expresión sobre el derecho a la privacidad, pese que en todo caso se requiere un juicio fundamentado por los tribunales en el caso concreto.

El discurso de los medios británicos, ya desde la aparición de la *Data Protection Act 1984*, ha girado en torno a la amenaza que podían suponer las normas protectoras de la información personal para la libertad de expresión. Con la promulgación de la HRA y ante el temor de que los tribunales pudieran crear un auténtico derecho a la privacidad basándose en el artículo 8 del CEDH, se introdujo la Sección 12 que deja constancia de la necesaria ponderación entre derechos cuando existe un conflicto pero que, sin embargo, no debería considerarse una novedad, pues ya los propios artículos 8 y 10 en sus respectivos párrafos segundos, dejan constancia de las necesarias limitaciones de sus contenidos en caso de que exista un interés superior amparado por otro precepto.

Esto se explica porque el artículo 8 tiene mucha incidencia en las acciones de difamación del Derecho inglés (hay que tener en cuenta que Reino Unido es el único estado parte en el Convenio que dirime las calumnias en los tribunales civiles) pese a que no se reconoce un derecho a responsabilidad civil en estos casos ni cubre la publicación de información verdadera pese a que sea personal. Esto ha supuesto divergencias con el artículo 8 del CEDH pero la doctrina inglesa ha mantenido que dicho precepto no es una herramienta para la creación de nuevos derechos, puesto que en Derecho británico, no se produce toda la cobertura legal que pareciera desprenderse de la normativa europea, basándose en la exigencia de que los derechos deban estar reconocidos previamente en la legislación doméstica.

Es por ello que, en la práctica, la prensa inglesa está dotada de ciertos privilegios, puesto que en la ponderación entre el derecho a la privacidad y a la libertad de información, ésta última sale ganando el 90% de las veces. Igual que ocurre con la revelación de secretos, el derecho inglés no se corresponde con el tenor literal del Convenio pues, a diferencia de éste, el

common law británico considera la protección de la reputación personal como un asunto de interés público[448], en lugar de un derecho individual, accionable mediante la difamación.

La libertad de expresión constituye un debilitamiento de la esfera de privacidad de las personas, pues el derecho a la vida privada puede colisionar frontalmente con el derecho de otra persona a expresar libremente una opinión o a hacer pública una información, como se puede constar en el *common law* desde los tiempos de WARREN y BRANDEIS.

Es inevitable que los derechos a la privacidad y a la libertad de expresión colisionen entre sí y necesariamente hay que buscar criterios viables y consistentes que permitan, en la práctica, resolver este tipo de situaciones. El CEDH facilita algunas pistas para llevar a cabo este tipo de ponderaciones pero no proporciona criterios precisos para llevarlas a cabo.

Las excepciones legales que recoge el CEDH en relación a las circunstancias por las que los derechos cualificados pueden verse limitados son, a grandes rasgos: "cuando sea conforme a la Ley o esté prevista por la Ley", cuando sea "necesario en una sociedad democrática", debido a una "necesidad social apremiante" o por razones de proporcionalidad.

En cuanto a la primera de las excepciones, el TEDH ha exigido que se demuestren tres extremos: que exista una previsión legal al respecto en el derecho doméstico o en cualquier instrumento comunitario o internacional, que la existencia de dicha previsión pueda conocerse por los ciudadanos (que sea accesible) y que la Ley se formule con la precisión suficiente para que el ciudadano pueda prever las circunstancias en las cuales se aplicará o pueda aplicarse la ley.

Las autoridades públicas, además de probar que dicha interferencia en un derecho del Convenio está recogida en un instrumento legal, deben demostrar que ésta es necesaria en una sociedad democrática lo que implícitamente exige que, sea proporcionada con el fin legítimo

---

[448] En *Reynolds v. Times Newspapers and others*, de 28 de octubre, [1998] 3 WLR 862, "*Reputation is an integral and important part of the dignity of the individual […] Once besmirched by an unfounded allegation in a national newspaper, a reputation can be damaged for ever, especially if there is no opportunity to vindicate one's reputation. When this happens, society as well as the individual is the loser. For it should not be supposed that protection of reputation is a matter of importance only to the affected individual and his family. Protection of reputation is conducive to the public good. It is in the public interest that the reputation of public figures should not be debased falsely*".

perseguido. El TEDH ha otorgado a los Estados miembros cierto margen de apreciación en la aprobación de estas circunstancias en las que, además, se exige la concurrencia de notas como pluralismo, tolerancia y "mente abierta"[449].

Respecto de la "necesidad social apremiante" ello exige que se justifique la interferencia producida en base a razones sociales que legitimen dicha decisión, sobre la que los tribunales nacionales tienen cierta discrecionalidad. Una vez más, ésta debe ir acompañada de proporcionalidad con la finalidad protegida[450] por lo que, cuanto menor sea la intervención más fácil será probar la urgente necesidad.

Por último, debe haber una proporcionalidad entre los medios empleados con los objetivos perseguidos con la limitación producida, produciéndose un necesario balance entre los intereses generales y la protección de un derecho fundamental de un individuo[451].

En el caso inglés esto se vuelve más complejo puesto que en su Derecho no existe el derecho a la privacidad como tal, lo que desde luego no evita resolver el conflicto pues, como el TEDH ha dicho en más de una ocasión[452], toda interferencia entre cualquiera de los derechos recogidos en el Convenio debe justificarse conforme al principio de legalidad, así como el respeto a la proporcionalidad y por razones de interés social.

De hecho, son varias las ocasiones en las que el TEDH ha recriminado al Reino Unido las carencias a la hora de proteger la privacidad de las personas[453] pues, con el argumento de que en el Derecho inglés no está reconocido expresamente un derecho a la privacidad, los tribunales ingleses tienden a ponderar los derechos del CEDH otorgándole a la libertad de expresión una posición jerárquica superior cuando existe conflicto de intereses[454]. Así, el

---

[449] *Handyside v. United Kingdom*, de 7 de diciembre, [1976] 1 EHRR 737.

[450] *R v. Ministry of Defence, ex parte Smith*, de 26 de julio, [1996] QB 517, the CAEW.

[451] *Sporrong and Lonnroth v. Sweden*, de 23 de septiembre, [1982] 5 EHRR 35.

[452] *Bladet Tromso and Stensaas v. Norway*, de 20 de mayo, [1997] 23 EHRR CD 40.

[453] Esto ocurrió en el caso *Spencer v. United Kingdom* 28851/95 y 28852/95 [1998] 23 EHRR CD 105 en el que el TEDH sentenció que la "*breach of confidence*" no era remedio suficiente para satisfacer los derechos de los demandantes.

[454] CLAYTON/TOMLINSON. *Privacy and Freedom of Expression*, Oxford University Press, Oxford, 2010, p. 34.

Tribunal ha dispuesto que los derechos y las responsabilidades que incorpora el artículo 10 del Convenio implican que, cuando no hay remedio accionable mediante el cual los interesados puedan obtener una reparación por la invasión de su privacidad sufrida, esto supone automáticamente la vulneración del artículo 8 del CEDH.

La jurisprudencia inglesa ha tenido que lidiar con el conflicto entre ambos derechos respecto de las siguientes cuestiones: en primer lugar, frente a acciones que han supuesto la revelación de secretos o la publicidad de información sensible, ya sea por parte de personas individuales como de los poderes públicos[455]. En segundo lugar, como consecuencia del empleo de nuevas tecnologías para la interceptación de comunicaciones o la obtención de imágenes de ámbito privado e incluso debido al espionaje[456]. Y por último, por actuaciones que, pese a invadir en cierto modo la privacidad, encuentran amparo en otro tipo de legislación como puede ser la laboral, el derecho de familia o el derecho penal[457].

4. Tratamiento de los conceptos objeto de estudio desde la perspectiva del *Common Law* británico

4.1. Concepto de privacidad

A pesar de que el Derecho inglés nunca ha reconocido expresamente un derecho general a la privacidad[458], su *common law* ha protegido la vida privada de las personas a través de varios instrumentos como la "*breach of confidence*" o el "*tort law*".

En el ordenamiento jurídico británico no es posible encontrar definición alguna del derecho a la privacidad[459], ni tan siquiera la doctrina es unánime en torno a este concepto[460].

---

[455] Entre otros, el caso *Woolgar v. Chief Constable of Sussex Police and Anor* [2000] 1 WLR 25 (CA).

[456] Como el caso de *Regina v. Brentwood Borough Council, ex parte Peck*, de 18 de diciembre, [1998] EMLR 697 (QBD).

[457] Por ejemplo, el caso *McKerry v. Teesdale & Wear Valley Justices*, de 29 de febrero, [2000] Div Ct.

[458] "[In United Kingdom] *the common law has not developed an overall remedy for the invasion of privacy*", *Wainwright v. Home Office,* de 16 de octubre de 2003, [2003] UKHL 53, 3 WLR 1137, Court of House Lords.

[459] El *Younger Committee*, pese a reivindicar su necesidad, expresó ya en 1972 las grandes dificultades que entrañaba definir la privacidad, entre otras cosas, por ser una percepción muy personal que varia en función de cada individuo "*The notion of Privacy has a substantial emotive content in that many of the things which we feel the need to preserve from the curiosity of our fellows are feelings, beliefs or matters of conduct which are themselves irrational*".

Sin embargo, sí que pueden distinguirse, a través de las figuras comprendidas en normas específicas y estatutos, así como mediante el desarrollo del *common law*, ciertas dimensiones de protección de la privacidad.

Así, en el derecho anglosajón, privacidad implica multiplicidad de cosas: el derecho a no ser molestado, a evitar la publicidad de ciertos aspectos personales, a la protección del copyright, a estar libre de injerencias por parte de las autoridades públicas, a la propiedad privada, a la confidencialidad, a un tratamiento de datos personales justo y adecuado a la Ley, a no ser fotografiado en estancias privadas, al secreto empresarial, etc.

Tradicionalmente en el Reino Unido se ha vinculado la protección de la privacidad con la protección de datos, porque es a través de la legislación específica –primero con la *Data Protection Act 1984* y después con la *Data Protection Act 1998*- como se ha concretado un derecho más amplio como es la privacidad que, sin embargo, sí que se ha esgrimido en ocasiones como una aspiración jurídica e ideal a perseguir. Mientras que la protección de datos es una obligación legal clara en la legislación británica, la privacidad, dotada de un contenido mucho más amplio, no goza de protección específica y, pese a ello, ambos conceptos han ido tradicionalmente aparejados por la legislación británica y en algunos casos incluso han sido empleados como sinónimos[461].

A nadie se le escapa lo difícil que resulta definir la privacidad, principalmente porque envuelve consideraciones muy personales, lo que no le confiere un estatuto inmutable, sino que su contenido varía en función de las personas y de las situaciones. Y claro está, resulta ciertamente intangible, difícil de medir y, en consecuencia, complejo de definir. Este trabajo se torna especialmente costoso para la doctrina británica, fundamentalmente porque en la

---

[460] Así lo expresa Raymond Wacks: "*This is, however, a vexed, contentious matter. It is, moreover, one that has engaged scholars from a host of disciplines. Thousands of pages have been devoted to the quest for definition, or at least for clarity. Each author trawls vainly through the multitude of preceding efforts to describe this elusive notion. Every new generation of privacy scholars fells bound to navigate anew these murky waters, relentlessly citing every prior definition in an exasperating pursuit of breakthrough. None materializes. Nor can it*". WACKS. *Privacy and Media Freedom*, Oxford University Press, Oxford, 2013, p. 19.

[461] BAMBERGUER/MULLIGAN. *Privacy on the Ground. Driving Corporate Behavior in the United States and Europe*, Massachusetts Institute of Technology Press, Cambridge, 2015, p. 150.

tradición jurídica del *common law* no existe históricamente un ámbito sólido para la protección de la privacidad personal, sino que ésta a menudo viene identificada como una cortapisa a la esfera de libertad personal, conceptos que a menudo entran en colisión y que en la doctrina británica se presentan inherentemente ligados.

Por todo ello, uno de los hitos más importantes en la protección de la privacidad por parte de la legislación británica, fue la aprobación de la *Human Rights Act 1998*, que supuso la incorporación a su orden juídico del Convenio Europeo de Derechos Humanos de 1951 y que permitió dotar a los tribunales británicos de herramientas efectivas para otorgar un reconocimiento directo y explícito a los derechos de privacidad personal.

Antes de la aprobación de la HRA, la legislación inglesa no era capaz de dar respuestas satisfactorias a problemas sociales cotidianos como puso de relevancia el caso *Kaye v. Robertson*[462] en 1991. Gorden Kaye era un famoso actor de televisión que durante un temporal sufrió daños graves en la cabeza, lo que obligó a hacerse cirugía y a pasar una larga temporada en el hospital. A causa de su fama, su estado de salud se convirtió en un asunto de interés para el público, se habló y debatió sobre ello en televisión y se publicó en la prensa. Pese a que el señor Kaye se encontraba ingresado en una habitación privada en el hospital, un reportero y un fotógrafo del *Sunday Sport* consiguieron acceder a ésta, ignorando la obligación de pasar por un registro previo, y tratando de hacerle una entrevista mientras fotografiaban al convaleciente así como los detalles de su habitación. Para evitar la publicación de dicho "fotoreportaje" el abogado del señor Kaye demandó al *Sunday Sport* frente a los tribunales, que ordenaron la imposibilidad de publicar nada que diese a entender razonablemente que el señor Kaye estaba conforme con dicha publicación pues, por el contrario, incurrirían en una falsedad dolosa. Sin embargo, el tribunal no pudo impedir la publicación del contenido de dicho "fotoreportaje" pues, de acuerdo con la ley británica, no había ninguna previsión legal al respecto[463] pese que

[462] *Kaye v. Robertson*, de 16 de marzo, [1991] FSR 62.

[463] Así lo reconoce la propia sentencia cuando afirma "*It is well-known that in English law there is no right to privacy, and accordingly there is no right of action for breach of a person's privacy. The facts of the present case are a graphic illustration of the desirability of Parliament considering whether and in what circumstances statutory provision can be made to protect the privacy of individuals*".

era notorio por el tribunal, que se estaba cometiendo una injusticia con el señor Kaye tal como dispuso en el fallo final de la sentencia: "*This case nonetheless highlights, yet again, the failure of both the common law of England and statute to protect in an effective way the personal privacy of individual citizens*".

Si bien es cierto que, en la actualidad, el señor Kaye tendría muchas menos dificultades para convencer a un Juez de que prohibiese la publicación de unas fotografías suyas en la cama de un hospital tomadas sin su consentimiento, esto no significa que en este transcurso de tiempo, ni siquiera desde la vigencia de la HRA, en el Derecho inglés se reconozca el derecho general a la privacidad.

Esto se ilustra también a través del caso *Wainwright v. Home Office*[464] en el que la Cámara de los Lores dejó claro que de ningún modo puede ejercitarse el derecho a la responsabilidad civil[465] frente a una invasión de la privacidad en el ordenamiento jurídico inglés. En este caso, dos personas que habían ido a visitar a un familiar en prisión denunciaron ante los tribunales que su privacidad había sido quebrantada cuando sin justificación alguna les cachearon desnudas en el penal como requisito de acceso, argumentación jurídica que fue rechazada por el Tribunal al sentenciar que no había lugar a responsabilidad civil alguna por no existir en el derecho anglosajón ningún principio general de invasión de la privacidad. La sentencia tiene presente la evolución del derecho británico desde el caso *Kaye v. Robertson* así como del reconocimiento de la privacidad como un valor inspirador, pero niega la existencia de un principio de legalidad, pues entiende que ésta no constituye por sí misma un principio general del Derecho.

La visión de las dos sentencias arriba expuestas es en cierto modo contrapuesta, pues si bien es cierto que en el derecho inglés no existe una previsión legal expresa que recoja un derecho a la privacidad, esto se deriva implícitamente de la HRA que, más allá de los pronunciamientos jurisprudenciales hasta el momento, incorpora al derecho británico el artículo

[464] *Wainwright v. Home Office*, de 16 de octubre, [2003] UKHL 53, 3 WLR 1137, Court of House Lords.

[465] En la sentencia judicial se hace mención a la inexistencia de "*general tort of privacy*".

8 del CEDH que sí que reconoce expresamente el derecho de toda persona a la vida privada y familiar, así como la inviolabilidad del domicilio y la correspondencia, y que sin duda dio el impulso final para el reconocimiento del derecho a la privacidad[466]. Se ejemplifica así la paulatina asunción por parte de la doctrina y la jurisprudencia del derecho a la privacidad así como las dificultades a la hora de insertarse en el *common law* y las contradicciones que se derivan de su reconocimiento en un sistema jurídico que tradicionalmente no contemplaba dicha figura.

a) Con anterioridad a la Human Rights Act 1998

La ausencia de una constitución escrita que consagrase el derecho a la privacidad o el reconocimiento de un derecho fundamental similar provocó, en la práctica, que los tribunales ignorasen las demandas ciudadanas en este sentido al considerar que no existía base para ello y que ello quedaba demostrado con la pasividad del Parlamento que no lo consideraba digno de regular[467].

Sin embargo, antes de que las disposiciones y la jurisprudencia del CEDH fuesen directamente aplicables en el Derecho británico, la privacidad se protegía de forma parcial y limitada a través de las causas de acción existentes en múltiples figuras del *common law* entre las que se incluían la difamación o la alteración del orden público, y también mediante la legislación específica en materia de datos personales, esto es, la *Data Protection Act 1984*.

Así, hasta la entrada en vigor de la HRA, aquellas acciones que perseguían garantizar la privacidad debían de acudir principalmente a las figuras de la *breach of confidence* (revelación de secretos), el *trespass* (allanamiento), la *nuisance* (perjuicio, molestias) o la *defamation and malicious falsehood* (difamación)[468].

---

[466] Esta visión fue compartida en la sentencia *McKennitt v. Ash*, de 20 de diciembre, [2006] EWCA Civ 1714, en la que se dispuso "*in order to find the rules of the English law of breach of confidence we now have to look at the jurisprudence of articles 8 and 10* ".

[467] Así se puso de manifiesto en el caso *Secretary of State for the Home Dept v. Waiwright* [2001] EWCA: "it is thus for Parliament to remove, if it thinks fit, the barrier to the recognition of a tort of breach of privacy that is at present erected".

[468] Esta lista no es un *numerus clausus*, existen otros mecanismos en el *common law* para proteger la privacidad como, por ejemplo en derecho contractual, mediante la inclusión de cláusulas de confidencialidad.

La *breach of confidence* supone revelar al público información confidencial sin autorización ninguna, rompiendo con el deber exigido, ya sea por contrato o por otras razones. Esta figura demanda siempre una ponderación con otros derechos, la libertad de expresión e información, lo que exige una determinación acerca de la existencia o no de interés público. Del mismo modo deben tenerse en cuenta las circunstancias concretas del supuesto de hecho pues, en la práctica, se diferencia entre el secreto empresarial y el secreto profesional, así como otro tipo de deberes de confidencialidad entre personas.

El *trespass*, al que traducimos como "allanamiento", engloba un conjunto de acciones que tienen en común el acceso, sin permiso del afectado, a una esfera privada de un individuo y que puede consistir desde la apropiación física de una propiedad ajena (por ejemplo, entrar en un ordenador sin permiso) hasta acceder física o virtualmente al lugar privado de alguien (como violar el domicilio de alguien o simplemente tomar fotografías una habitación de hotel o de hospital, como en el caso del señor Kaye).

Para que pueda ejercitarse una acción de *trespass* no es necesario que dicho acto haya producido daños, sino que es suficiente con probar que dicho acto produce una vulneración del espacio privado ajeno. Por ejemplo, si se graba a una persona en su jardín por encima de una valla, esto supone una vulneración de su privacidad, pese a que no le provoque daño físico alguno.

La *nuisance* es una figura del *common law* que tiene un carácter mixto, entremezclando elementos de las dos figuras anteriores, y que protege al individuo en relación con su propiedad, protegiéndole frente a cualquier interferencia en su disfrute cuando no reúna las condiciones necesarias para constituir un allanamiento (*trespass*) como podría ser la existencia de ruidos o molestias en una comunidad de vecinos[469].

[469] Así lo explicaba la sentencia *Bernstein v. Skyviews and General Ltd* [1978] QB 479: "*If a plaintiff were subject to the harassment of constant surveillance of his house from the air, accompanied by the photographing of his every activity, I am far from saying that the court would not regard such a monstrous invasion of his privacy as an actionable nuisance for which they would give relief*".

Así, mientras que la realización de una sola fotografía no constituiría una *nuisance* procesable, la observación y el acoso persistente sí que pueden ser una *nuisance*, como también lo sería recibir llamadas telefónicas no desaseadas constantemente. Ahora bien, conviene señalar que esta figura está inexorablemente ligada al concepto de propiedad, sólo los propietarios tienen derecho a reclamar una protección jurídica en este sentido, por lo que los meros usuarios quedan excluidos de esta garantía[470].

Por último, la *defamation* es una figura integrada en el derecho penal británico para proteger el honor cuando éste se menoscabe a través de un medio fijo, mediante imagen o por escrito (se asemeja razonablemente a lo que en nuestra tradición jurídica se conoce como libelo y calumnia), maliciosamente o se sustancie en hechos falsos.

La *defamation and malicious falsehood* son figuras que se usan en casos aislados y diversos pues abarcan, desde el uso de la imagen personal para promocionar una marca comercial sin autorización para ello hasta la realización de fotografías en base a un consentimiento viciado, cuando con ello se menoscabe la reputación del interesado. Es decir, la *defamation and malicious falsehood* está íntimamente relacionada con la prestación del consentimiento, así como con consideraciones de tipo moral. De hecho, en el caso Tolley[471] paradigmático de esta figura, el Tribunal llegó a afirmar: "the defensants had acted in a manner inconsistent with the decencies of life and in doing so they were guilty of an act for which there ought to be a legal remedy".

Esta figura se encuentra con dos limitaciones, por una parte el interés superior que merece la publicación de ciertos hechos, por lo que la publicación de hechos privados sobre un individuo cuando éstos sean ciertos, aunque concurran determinadas circunstancias del tipo, no resulta procesable. En segundo lugar, que las palabras o imágenes deben ser difamatorias para el demandante, por lo que su publicación puede disminuir considerablemente su reputación

[470] Así pues, esta figura resulta ciertamente controvertida al no ofrecer protección jurídica, por ejemplo a un cliente de un restaurante que resulte perturbado en el disfrute de sus derechos, que no tiene legitimación para demandar por *nuisance*. Así lo evidencia la sentencia *Hunter v. Canary Wharf Ltd* [1997] AC 655.

[471] *Tolley v. JS Fry & Sons Ltd* [1931] AC 333, HL.

para cualquier persona con "sentido común"[472] lo que inevitablemente incluye conceptos jurídicos indeterminados.

b) Con posterioridad a la Human Rights Act 1998

Una vez se dicta la *Human Rights Act* en 1998, se materializan las demandas de la sociedad británica que exigían una protección jurídica adecuada, de una esfera libre de cualquier injerencia en un sentido amplio, lo que tiene lugar expresamente con la reglamentación del derecho a la vida privada. Así, bajo la HRA, la naturaleza del derecho a la privacidad cambia radicalmente al ser protegido mediante una fórmula legal bajo la cual resulta directamente aplicable tanto para los individuos como para las autoridades públicas. A partir de este momento, la jurisprudencia del TEDH tiene un impacto directo en el Derecho británico, que queda directamente vinculado por su jurisprudencia así como por la fluctuación de sus interpretaciones acerca de los conceptos jurídicos incluidos bajo el paraguas del CEDH.

La revolución jurídica que supuso la HRA se explica, fundamentalmente, porque muchos de los derechos reconocidos en el CEDH, como el derecho a la privacidad, no habían tenido un reconocimiento previo o no se les había otorgado el estatus de derechos fundamentales bajo el Derecho anglosajón[473].

Así las cosas, a partir de la entrada en vigor de la HRA, bajo el amparo de su artículo 8, el derecho a la privacidad comienza a ser directamente invocable en la jurisdicción inglesa[474] lo que supuso un abono de cultivo para las disputas jurisprudenciales y es que, sin duda, dicho precepto del CEDH es el que más impacto ha ocasionado en la jurisdicción inglesa, aunque sólo sea por el número de veces que ha sido invocado.

Hay que decir que, a pesar de que de una lectura literal del artículo 8 del CEDH pueda extraerse que la privacidad es un derecho frente al Estado[475], como se ha podido comprobar

[472] TUGENDHAT/CHRISTIE. *The law of Privacy and The Media*, Oxford University Press, New York, 2002, p. 8.

[473] COLVIN. *Developing Key Privacy Rights*, Hart publishing, Portland, 2002, p.13.

[474] Cuestión discutida ampliamente en la sentencia *W (children)* [2001] EWCA Civ 757.

[475] La Sección 6ª del CEDH dispone que no deben haber interferencias por parte de los poderes públicos en relación con el derecho a la privacidad.

reiteradamente por la casuística[476], en el contexto británico el derecho a la privacidad no sólo es accionable verticalmente por una persona individual frente al Estado, sino que también tiene efectos horizontales indirectos, pudiendo ejercitarse entre particulares[477]. En cualquier caso, dicha afirmación debe ser matizada pues, como ya se ha dicho en otras ocasiones, el CEDH no crea por sí mismo un nuevo derecho a la privacidad en la medida en que no concede a los particulares un derecho a la responsabilidad civil (*tort law*) frente a su vulneración.

La legislación británica no ofrece pues una definición concreta de lo que es o no privado ni tampoco reconoce expresamente el derecho a la privacidad[478], pese a que muchas de las facetas de esta noción están protegidas por normativa específica y por el propio *common law*. Así, es recurrente en la doctrina la idea de que es mejor que la legislación no ofrezca una definición de privacidad para que su contenido no pueda desvirtuarse por el paso del tiempo[479]. Sin embargo, esto provoca en la práctica, que muchas conductas claramente atentatorias contra la privacidad y que no están recogidas en estatutos específicos, no gocen de protección legal alguna.

Si bien se reitera por la doctrina británica que privacidad es un término amplio no susceptible de una definición exhaustiva, con la interpretación del artículo 8 de la HRA que incorpora este derecho al ordenamiento de Reino Unido, los Tribunales británicos han perfilado y ampliado su significado, incluyendo elementos diversos que incluyen, desde aspectos eminentemente íntimos (como la identificación del género, el nombre, la orientación sexual o la vida sexual) hasta elementos con un competente más social, al entender que dicho precepto

[476] Por ejemplo, el caso *Campbell v. Mirror Group Newspapers Ldt*, de 6 de mayo, [2004] UKHL 22, Court House of Lords.

[477] De hecho, los artículos 8 y 10 del CEDH son, mayoritariamente invocados en disputas entre particulares o entre particulares y corporaciones y, en menor medida, frente al Estado.

[478] Así se puso de manifiesto en el sentencia *Wainwright v. Home Office*, de 16 de octubre, [2003] UKHL 53, 3 WLR 1137 (Court House of Lords), incluso con posterioridad a la entrada en vigor de la HRA y cuando los jueces emplean su articulado para proteger ciertos aspectos privados de los individuos.

[479] Parliamentary Joint Committee on Privacy and Injunctions, 2012: "*We conclude that a privacy statute would not clarify the law. The concepts of privacy and the public interest are not set in stone, and evolve over time. We conclude that the current approach, where judges balance the evidence and make a judgement on a case-by-case basis, provides the best mechanism for balancing article 8 and article 10 rights*".

protege también el derecho a la identidad y el desarrollo personal y el derecho a establecer relaciones con otros seres humanos y el mundo exterior[480].

Este último aspecto ha supuesto un punto de inflexión al extender la protección de la privacidad fuera de la esfera estrictamente personal, aplicándose a actividades de naturaleza profesional o empresarial, pues se ha defendido la existencia de una zona de interacción de una persona con otras, incluso en un contexto público, que puede estar englobado dentro del ámbito de la "vida privada"[481]. De este modo, se dispone que la protección de la vida privada se extiende más allá de las instalaciones privadas de una persona. Y lo mismo ocurre con los registros o ficheros de datos personales, que obtienen la protección de artículo 8 incluso cuando la información no ha sido recopilada por ningún método intrusivo o encubierto[482].

El alcance legislativo de la HRA va mucho más allá de una prerrogativa ciudadana pues su marco de protección impone obligaciones directas para los poderes y los particulares. La inclusión de la palabra "respeto" en el artículo 8, se ha interpretado por los tribunales británicos como una obligación positiva del Estado que tiene que disponer los instrumentos necesarios para impedir que los individuos sufran cualquier interferencia en su ámbito más privado por parte de otros individuos o las administraciones públicas[483].

De todo ello puede decirse que si bien es cierto que en el Reino Unido se carece de un concepto unitario y estandarizado de la privacidad, ésta se protege en muchas de sus facetas por las normas estatutorias, y principalmente a través de los instrumentos clásicos del *common law* como la *breach of confidence* o el *trespass* que no sólo no han caído en desuso sino que han servido para instrumentalizar las garantías introducidas por la HRA. El valor otorgado por dicha normativa a la jurisprudencia del TEDH, junto con el valor tradicional que se le brinda a

[480] *A v. B plc*, de 11 de marzo, [2002] 3 WLR 542.

[481] Por ello, las expectativas razonables de privacidad de una persona, aunque son un factor significativo, no es determinante pues hay ocasiones en que las personas se involucran en actividades a sabiendas de que son o pueden ser divulgadas públicamente.

[482] Resulta curioso como la *Data Protection Act 1998* no se refiera expresamente a la privacidad cuando la Directiva 95/46/EC, la cual implementa, sí que hace mención en reiteradas ocasiones al derecho de las personas a la privacidad, lo que se interpreta por la doctrina como una elección consciente orientada a preservar al máximo el alcance de dicho concepto.

[483] *Theakston v. MGN Ltd*, de 14 de febrero, [2002] EMLR 398.

jueces y tribunales británicos en el derecho anglosajón, dotan de una gran flexibilidad al concepto y garantía de la privacidad.

4.2. El concepto de protección de datos

Si bien el ordenamiento jurídico británico no contempla contundentemente y de forma expresa un derecho a la privacidad en sentido amplio, por el contrario y como se ha podido comprobar anteriormente, Reino Unido sí que goza de una legislación amplia y específica en materia de protección de datos cuyo contenido, pese a no reconocerse formalmente, está íntimamente relacionado con la protección de la privacidad, la cual se erige como una de las finalidades más importantes de dicha normativa.

A diferencia del ordenamiento jurídico español, en el Derecho anglosajón no se produce una diferenciación clara entre el derecho a la protección de datos y el derecho a la privacidad, principalmente porque este último derecho no está reconocido expresamente en ningún instrumento jurídico sino que se deriva de aspectos específicamente reconocidos como la inviolabilidad del domicilio, el secreto profesional o la protección de la vida privada familiar.

De hecho, los términos "*data privacy*" y "*data protection*" en el contexto jurídico anglosajón, son intercambiables y a menudo se usan como sinónimos[484], pese a que desde la tradición jurídica continental vislumbremos grandes diferencias. No obstante, si se quiere buscar alguna diferencia entre ambas nociones podría decirse que en la concepción británica, mientras que el derecho a la protección de datos versa sobre la protección de personas individuales (los sujetos objeto del tratamiento) contra el almacenamiento de numerosa información privada (que le identifique o le haga identificable) para su procesamiento y uso posterior (con fines publicitarios, por ejemplo, o para llevar a cabo decisiones automatizadas); el concepto de privacidad (ni siquiera debería hablarse aquí de un derecho porque en la tradición jurídica inglesa no está reconocido así en ninguna parte) comprende todas aquellas acciones encaminadas a proteger a las personas frente a la intromisión en su ámbito íntimo,

[484] DETERMANN. *Determann's Field Guide to Data Privacy Law*, Edward Elgar publishing, Cheltenham, 2015, p. 4.

como el derecho a la inviolabilidad del domicilio o la interceptación de sus comunicaciones privadas, entre otras.

Con la aprobación de la HRA se produjo una situación peculiar y es que, si bien se vislumbró la privacidad como un nuevo bien jurídico a proteger, no se le dotó a éste de autonomía propia, por lo que no se han sustanciado acciones que no vayan aparejadas a figuras legales legalmente reconocidas, como la *misuse of private information* o la *breach of confidence*, cuando se den las circunstancias para ello[485]. Sin embargo, una faceta de la privacidad que sí que ha contado con sustantividad propia en el ordenamiento jurídico británico ha sido la protección de datos, que ostenta una respuesta legal contundente en caso de existir contravención. A través de las sucesivas DPA, se ha consolidado un estatuto jurídico mediante el cual la información personal se protege en todo caso, cuando la persona tuviera una expectativa razonable de privacidad respecto de esta información, sin que sea necesario que las partes tuvieran una relación previa. Se incorporan así una serie de derechos en torno a la privacidad, mediante la protección de todo tipo de información privada (no constituye un *numerus clausus*) íntimamente relacionado con la dignidad y a la autonomía personal.

En cuanto a la noción de procesamiento, se encuentra ampliamente definido para incluir en él la obtención, registro, retención, uso o divulgación de la información, por lo que, en la práctica, cualquier acción con respecto a datos personales o mediante el uso de éstos, se engloba dentro de la definición de procesamiento.

Respecto de la información personal, aunque la definición de datos personales que hace la normativa británica se basa en la comprendida en la Directiva del 95, lo cierto es que la jurisprudencia del Reino Unido ha alterado el sentir general de este concepto mediante su interpretación, provocando algunas incoherencias de enfoque entre los tribunales británicos y las opiniones del Grupo de trabajo del artículo 29. Incluso la ICO, como autoridad de supervisión, ha emitido directrices sobre la interpretación de la definición de datos personales,

[485] Así, no hay un derecho a la "*breach of privacy*" pero sí puede sustanciarse una acción de "*breach of confidence*" cuando se quebrante el deber de confidencialidad exigido.

intentando alinear la jurisprudencia del Reino Unido y el documento del Grupo de trabajo del artículo 29 sobre esta definición[486].

Así, las decisiones de los tribunales británicos establecen que, para ser considerados datos personales, la información debe ser biográfica en un sentido significativo y debe centrarse en el individuo (en lugar de alguna transacción o evento en el que pueda haber figurado) por lo que, en términos generales, han interpretado la definición de datos personales de una manera más restrictiva que la dispuesta por la legislación[487].

Esto ha ocasionado problemas prácticos pues las organizaciones han tenido dificultades –y otras veces se han aprovechado maliciosamente de esta interpretación- para determinar qué constituye información personal, y eludir así las exigencias que la DPA impone a los *data controllers*[488].

4.3. Reflexión en torno a ambas nociones

El principio anglosajón "*remedies precede acts*" resume la lógica de su sistema jurídico formado por un intrincado de resoluciones jurisdiccionales que son fuente del derecho, a lo que se le añade leyes y estatutos sectoriales, conformando todo ello los derechos y libertades a proteger y perfilando su contenido.

Así, en esencia podría decirse que la gran mayoría del derecho inglés está formado por un conjunto de normas no escritas y no promulgadas o sancionadas, por lo que establecer paralelismos con nuestro sistema de Derecho civil es harto complicado. Sin embargo, también es cierto que el modelo británico, quizás por la influencia europea, está evolucionando hacia

[486] *Technical Guidance Note*, 21 de agosto de 2007.

[487] NOORDA/HANLOSER. *E-Discovery and Data Privacy. A Practical Guide*, Kluwer Law International, The Netherlands, 2011, p. 297.

[488] De este modo, por ejemplo, puede argumentarse que los correos electrónicos escritos por empleados contienen sólo información personal limitada, basándose en que los correos electrónicos no contienen información biográfica significativa y no están referidos a un individuo en particular. Así, pese a que un email contenga datos personales del remitente, puede considerarse que no incluye datos personales de los destinatarios o incluso ni siquiera de las personas a las que se refiera el contenido de dicho correo, por lo que no contaría con el paraguas de protección de la DPA.

una paulatina codificación, por lo que deben tenerse en consideración tanto las normas como las resoluciones judiciales a fin de tener una comprensión completa del sistema de protección.

Se trata de un sistema ambivalente en el que, si bien hace un par de décadas podría decirse que Reino Unido había abandonado nociones antiguas de privacidad gracias a la integración europea, incluso se caracterizaba a Reino Unido por haber realizado una interpretación estricta de la Directiva del 95 en comparación con otros de los Estados miembros, los últimos acontecimientos político-legislativos así como las prácticas empresariales emergentes, encaminadas hacía un retorno de la autorregulación, parecen desdecir lo anterior, regresando a unas prácticas y nociones de privacidad que se creían largamente superadas.

Los tribunales europeos, en más de una ocasión, han determinado que la ausencia del ejercicio de un derecho a la privacidad en la legislación anglosajona supone, en la práctica, una vulneración del derecho a la vida privada y, en consecuencia, una vulneración del artículo 8 del CEDH[489]. Lo que, sin embargo, no cuenta con el apoyo de los poderes públicos[490] ni tampoco de gran parte de la doctrina, que rechaza un reconocimiento expreso del derecho a la privacidad[491], cosa que queda patente en cada intento de legislar más profundamente sobre la materia y en cada resolución judicial a la que acusan de interpretar extensivamente el artículo 8 de la HRA

En definitiva, en el Reino Unido se da un fenómeno un tanto particular y es que, en materia de privacidad, se mantiene entre dos aguas[492], entre su tradición jurídico-histórica y las innovaciones legislativas y jurisprudenciales en torno a esta cuestión. Esto se evidencia muy

[489] *Steward-brady v. United Kingdom*, de 2 de Julio, [1997] 24 EHRR CD 38.

[490] En octubre de 2003, el Departamento de Cultura, Medios de Comunicación y Deportes del Gobierno británico en un informe llamado *Privacy and Press Intrusion* dispuso "*The Government strongly believes that a free press is vital to the health of our democracy […] there should be no laws that specifically seek to restrict that freedom, and Government should not seek to intervene in any way in what a newspaper or magazine chooses to publish. We therefore support self-regulation*".

[491] En palabras de Joshua Rozenberg: "*A privacy law in Britain would undoubtedly stop reporters telling the truth*". ROZENBERG. *Privacy and the Press*, Oxford University Press, New York, 2004, p. 32.

[492] "*One foot standing on American soil and one foot firmly planted on the Continent*", BAMBERGUER/MULLIGAN. *Privacy on the Ground. Driving Corporate Behavior in the United States and Europe*, ob. cit., p. 145.

claramente en relación al derecho de protección de datos pues, por una parte y legalmente, se encuentra limitada por el alto estándar de protección del que goza la materia en la legislación británica y europea, mientras que sigue claramente unida a un sistema menos intervencionista, ya sea por la tradición jurídica compartida del *common law* como por razones extralegales a través de sus operaciones transatlánticas, asemejándose con las nociones de privacidad más propias de Estados Unidos.

Algunos autores interpretan el escenario actual como una oportunidad perdida, entendiendo que el Parlamento británico ha fracasado en su intento de promulgar una legislación en materia de privacidad[493] pues, por una parte y pese a promulgar la HRA, ésta ha decepcionado en sus expectativas iniciales al no haber tenido toda la relevancia como fuente de un derecho general de privacidad en la legislación nacional del Reino Unido. Por otro lado, los tribunales nacionales británicos, quienes han tenido un papel decisivo en el reconocimiento y la aplicación de los derechos de privacidad, han decidido seguir con el camino ya marcado por el *common law* reinterpretando las figuras clásicas en torno a las que gira la protección del individuo y su esfera libre de injerencias.

Esto sin embargo, no ha regido para el derecho a la protección de datos, concepto autónomo para el derecho continental pero con inexorables ligámenes con la privacidad en la tradición jurídica del *common law*, dónde el ordenamiento jurídico británico ha sabido, hasta ahora, adoptar un sistema de protección de la información personal cuyos altos estándares no tienen nada que envidiar a los modelos de otros Estados miembros con mayor tradición proteccionista.

Es por ello, que el estancamiento de la evolución del derecho a la privacidad no debe interpretarse como un naufragio sino como una elección consciente, constituyendo una defensa de los valores jurídicos más tradicionales y tendencialmente liberales con dicha cuestión[494].

---

[493] KROTOSZYNSKI. *Privacy Revisited. A Global Perspective on the Right to Be Left Alone*, Oxford University Press, Oxford, 2016, p. 117.

[494] Sin embargo, gran parte de la doctrina no observa estos hechos como un fracaso sino como una decisión plenamente consciente, así lo dispuso el informe de 2010 del Departamento de Cultura, Medios de Comunicación y Deportes del Gobierno británico: "*given the infinitely different circumstances which can arise in different cases, and the obligations of*

La fluctuación del sistema de protección de la privacidad, obedece al devenir de la sociedad británica, inmovilista por naturaleza y altamente contradictoria. Así lo defiende MARKESINIS quien dice que la protección de la privacidad es un problema moderno, difícil e intrigante[495]. Reformulando su argumentación conforme a los tiempos que corren, puede decirse que estamos ante un problema moderno, porque las nuevas tecnologías han supuesto una vulneración sin precedentes en la vida privada de las personas, constituyendo incluso una fuente de peligros. Difícil, porque la solución no es única, depende de las circunstancias de cada caso y además entra en conflicto con otros derechos reconocidos por la Ley. Y es también intrigante porque el entorno en el que se producen las intromisiones a la privacidad está en una evolución constante[496].

4.4. Cuestiones accesorias: la protección del honor y la reputación

Principalmente por razones de extensión pero también por centrar el tema de la presente disertación, se ha hecho anteriormente mención al tratamiento de la privacidad y, en concreto, al sistema británico de protección de los datos personales. Sin embargo, y aunque no se vaya a profundizar en ello, no puede pasarse por alto el hecho de que el ordenamiento jurídico anglosajón contiene otros mecanismos de protección de otras facetas de la personalidad que claramente tienen una incidencia en la esfera de privacidad de las personas.

Así por ejemplo, mediante la acción de "*defamation*" se protege el honor y la reputación de las personas en el derecho anglosajón, derecho reconocido por el *common law*, así como por estatutos independientes -el último la *Defamation Act 2013*- y cuya protección se desprende también del artículo 8 de la HRA como un elemento más de la vida privada.

---

the HRA, judges would inevitably still exercise wide discretion […] for now matters relating to privacy should continue to be determined according to the common law, and the flexibility that it permits, rather than set down in statute". Del mismo modo, hay que decir que la Casa de los Comunes ha considerado en reiteradas ocasiones esta cuestión y siempre ha declinado crear un estatuto específico para la privacidad.

[495] MARKESINIS. "The Right to Be Let Alone versus Freedom of Speech", en *Public Law*, nº 1, 1986, p. 67.

[496] En los años 70, el *Younger Committee* ya recalcaba la evolución constante de este concepto "*The scope of privacy is governed to a considerable extent by the standards, fashions and mores of the society of which we form part, ante these are subject to constant change, especially at the present time*".

La relación entre la difamación y una acción por uso indebido o por la publicación de un hecho privado, suele ser más difícil de gestionar cuando se solicitan medidas cautelares y los hechos, pese atentar contra la fama de una persona, son ciertos. Los tribunales británicos no tienen previsto conceder ninguna acción por difamación cuando los hechos denunciados son verídicos, independientemente de si existe o no un interés público en su publicación[497], observándose aquí nuevamente la influencia del *common law* más tradicional, que dota dicha cuestión de una mayor liberalidad jurídica y lo asemeja más al tratamiento norteamericano de la cuestión.

Lo mismo ocurre con la explotación de la propia imagen, cuya protección se incluye ahora bajo el paraguas del artículo 8 de la HRA, en tanto que forma parte de la privacidad personal, pese a ser una figura reconocida tradicionalmente por el *common law*.

Se entiende que una persona puede oponerse, por ejemplo, a la publicación de unas fotos del interior de su casa tomadas sin su consentimiento, no sólo por lo concerniente a la privacidad sino también por el derecho de ésta a explotar esas imágenes en el Mercado, obteniendo beneficios por ello[498].

Del mismo modo, se protege el derecho de toda persona a oponerse a la explotación comercial de su imagen por terceras personas que carecen de permiso para ello, pues se protege el derecho de toda persona a hacer negocios legítimos con su propia imagen. Esto se contempla en el *common law* mediante la "*tort of passing off*" (que podría traducirse como la acción de usurpación o apropiación) que tutela el interés comercial en este caso, aunque también podría ejercitarse la "*breach of confidence*" cuando con ello se hubiera vulnerado un deber de confidencialidad.

[497] En el caso *Bonnard v. Perryman*, de 2 de enero, [1891] 2 Ch. 269, ya se acordó que no se adoptará ninguna medida cautelar para restringir la publicación de una información que pueda ser constitutiva de difamación antes del juicio en el que el demandado deberá acreditar su justificación.

[498] *Creation records v. News Group Newspapers Ltd*, de 29 de abril, [1997] E.M.L.R. 444.

Así, el derecho anglosajón diferencia entre aquellos casos en los que existe un interés comercial en la protección de la propia imagen, como el caso Irvin[499] relacionado con los derechos de explotación de imagen de un piloto de Fórmula 1; y aquellos otros en los que el interesado sólo busca proteger su privacidad personal, como el caso de la escritora JK Rowling[500] y la publicación de unas fotografías de sus hijos. Y se prevén mecanismos para la protección de los derechos y las libertades personales en uno y otro caso.

Sin embargo, resulta curioso cómo, cuando en un caso por difamación el interesado argumenta además la existencia de un peligro que para su privacidad comporta determinada acción, esto pueda incluso dificultar más sus probabilidades de éxito en el juicio posterior pues, aunque sin duda tal comportamiento puede tener consecuencias en la vida privada de las personas, no existe un procedimiento específico para ello, y bajo las formas previstas para la acción de difamación, puede que no se conceda la protección que se pretenda desde el inicio[501].

Así pues, se observa de nuevo la paradoja del tratamiento que se hace de la privacidad en el ordenamiento jurídico británico y de cómo, tanto a la jurisprudencia como a la doctrina, le resulta difícil encajar el nuevo modelo que para su protección se deriva de la aprobación de la HRA, con las figuras tradicionales de protección en el *common law*. No obstante, y aunque de un modo global no se reconozca un derecho global y explícito a la privacidad, queda patente la protección sectorial de muchas de sus facetas, tal como se evidencia en los ejemplos anteriores.

5. La incidencia del euroescepticismo en la protección de los derechos y libertades de la ciudadanía.

La *Human Rights Act 1998* ha facilitado tejer un marco normativo preeminente en el ordenamiento jurídico británico, pero no puede decirse que esté suficientemente asentado y menos aún consolidado a tenor de los vientos con que se ha agitado la bandera del *Brexit*. El euroescepticismo más o menos difuso que pudiera impregnar la sociedad británica, junto al

[499] *Edmund Irvine Tidswell Ldt v. Talksport Ldt*, de 25 de marzo, [2002] EWHC 367.

[500] *Murray v. Big Pictures (UK) Ltd*, de 7 de mayo, [2008] EWCA Civ 446.

[501] *RST v. UVW*, de 11 de septiembre, [2009] EWHC 2448 (QB).

antieuropeísmo declarado de una minoría muy activa que alimentaba sus razones, toma cuerpo en forma de decisión, difícilmente revocable, a través de los resultados del referéndum celebrado el 23 de junio de 2016.

Aproximadamente el 52% de quienes ejercieron su derecho al voto escogió abandonar la Unión Europea, es decir, hacer realidad el denominado *Brexit*, un término sintético de gran rotundidad mediática utilizado para referirse a la salida de Gran Bretaña de las instituciones comunitarias, pero cuyos múltiples matices y drásticas consecuencias se han empezado a vislumbrar a posteriori, cuando se han iniciado las negociaciones para su compleja puesta en práctica. Entre tales matices y efectos colaterales, los de orden jurídico referidos a derechos y libertades ciudadanas no copan los titulares de los noticiarios como sí lo hacen los de orden económico, pese a que resulta evidente que éstos están en juego, sobre todo si nos atenemos al uso que se ha hecho de ellos a lo largo del proceso de desafección europeísta.

En las élites políticas y económicas europeas –incluyendo entre ellas una parte significativa de las británicas–, conocedoras de la complejidad y consecuencias del *Brexit* y por ello mismo convencidas de que tales factores eran el antídoto que daría lugar a su rechazo, se recibió el resultado del referéndum como inesperado, es decir, sin contar con un plan trazado para tal eventualidad. Sin embargo, el contexto político de los años precedentes en el Reino Unido hacía bastante verosímil esa posibilidad al ir arraigando un sentimiento antieuropeo como expresión de malestar –y excusadora atribución de responsabilidades externas– ante cualquier pérdida o declive de la sociedad británica.

Este sentimiento adquirió expresión política al manifestarse de una manera declarativa (que entonces no llegó a interpretarse como una predisposición decisiva), en las elecciones al Parlamento europeo celebradas en mayo de 2014. Con una participación del 35’6% (inferior a la media europea del 42’54%), la primera fuerza política del Reino Unido fue el UKIP (*United Kingdom Independence Party*), al obtener el 26’77% de los votos. Este partido, con un acento xenófobo muy marcado, tenía hasta ese momento una presencia residual dentro del espectro político británico, pero en esta cita electoral amplió su campo de voto al hurgar en el clima de descontento blandiendo una incierta pero efectista premisa: solventar los males de la nación

pasa necesariamente por la salida del Reino Unido de las instituciones eurocomunitarias. El éxito del mensaje había minado al Partido Conservador por su propia derecha, aunque también tomó prestados votos de otros caladeros, incluso de la orilla opuesta, dado su reduccionismo y la transversalidad del malestar sobre capas demográficas medias inseguras y capas bajas desfavorecidas. La reacción del líder conservador, el Primer Ministro David Cameron, fue lanzar una estrategia de atracción del electorado *torie* desencantado con sus políticas, para que su voto no enraizase en el UKIP.

Con esa finalidad, Cameron se propuso disputarle al UKIP el monopolio de su discurso enarbolando posiciones de mayor contundencia crítica frente a la acomodaticia ambigüedad de las posturas euroescépticas sostenidas hasta el momento por su formación. En esta estrategia se inserta la formulación y presentación pública del informe programático "*Protecting Human Rights in the UK. The conservative's proposals for changing Britain's Human Rights Laws*"[502], donde se planteaban una serie de críticas al marco legal del Reino Unido emanado de Estrasburgo en esta materia. Tales críticas no ponían su acento en cuestiones de tipo jurídico sino más bien en cuestiones ideológicas o políticas interpretables en términos electoralistas, con apelaciones más bien enmarcadas dentro del espectro propio del UKIP, tratando así de retener o reconquistar votantes atraídos por esa formación[503].

Se explicaría de este modo que, para subrayar una defensa esencialista de la soberanía británica, el documento llegara a propugnar la salida del Reino Unido del Consejo de Europa de una manera drástica, rechazando con ello la jurisdicción del Tribunal Europeo de Derechos Humanos y como consecuencia, suprimiendo la *Human Rights Act 1998* del ordenamiento jurídico británico[504], con las graves consecuencias que este escenario supondría no sólo en términos jurídicos, políticos y sociales, sino en merma de derechos individuales de ciudadanía.

Es con este ejemplo como la experiencia británica puede mostrarnos el que una política de gestos y propuestas reduccionistas y grandilocuentes –populistas, se las denomina en la

[502] Véase, https://www.conservatives.com/~/media/Files/Downloadable%20Files/HUMAN_RIGHTS.pdf.

[503] Cfr. CORRECHER MIRA. *Principio de legalidad penal: ley formal vs. law in action*, ob. cit., p. 204.

[504] Cfr. ELLIOTT. *Public law,* Oxford University Press, Oxford 2014, p. 736.

actualidad–, surgida por simple estrategia en la disputa de la base electoral de partidos de un mismo espectro ideológico, devenga en una línea programática radicalizadora y más aún, en una coyuntura concreta que impele a la puesta en práctica, amenace con hacerse realidad afectando a cuestiones de muy diversa índole y distinto calado –en este caso el hecho de desvincularse de la jurisdicción de Estrasburgo–, como parte de un todo cuyo planteamiento, de simple adhesión o rechazo, no admita precisiones ni medias tintas.

Recordemos que el plato fuerte de la estrategia de los conservadores de cara a las elecciones generales de 2015 fue la promesa de celebración de un referéndum sobre la permanencia en la Unión Europea. La formación como tal no se decantaba por abandonarla, pero, como se ha ejemplificado, había abonado un contexto beligerantemente crítico hacia ella para evitar la patrimonialización electoral de esta postura por parte del UKIP. El resultado de la contienda certificó el acierto electoral de la estrategia de los *tories* permitiéndoles mantenerse en el poder con significativa ventaja sobre los laboristas y, al tiempo, contener eficazmente las expectativas fagocitadoras del UKIP[505]. Pero esa victoria conllevaba una hipoteca de alcance insospechado y de imposible devolución.

Nos referimos a que las filas del Partido Conservador, aun siendo las vencedoras de la contienda, una vez dejado atrás su tradicional y confortable euroescepticismo, pasarían a ser rehenes del sentimiento antieuropeo tan frívolamente abonado, y al final se verían obligadas a actuar como las fuerzas responsables de abrir la llave al *Brexit*, ejecutando, paradójicamente, las pretensiones de sus otras competidoras. De nada sirvió que Cameron al convocar el prometido referéndum, sostuviese un discurso a favor de la permanencia británica en el seno de la Unión Europea. El contexto, el clima crítico y esencialista que su propia acción política había favorecido, le restó convicción y credibilidad, contribuyendo, podría decirse, a la victoria de los partidarios de abandonar las instituciones comunitarias. A efectos prácticos, poco importó la dimisión inmediata de Cameron como primer ministro, puesto que las consecuencias de este resultado no se circunscriben a una cuestión de política interna siendo por ahora muy

[505] El recuento de votos otorgó la victoria al Partido Conservador cuyo porcentaje de votos fue del 36,9%, seguido por el Partido Laborista que obtuvo el 30,4% de los votos. Por su parte, el UKIP obtuvo el 12,6% de los sufragios.

difíciles de calibrar más a allá de entrever la complejidad aparejada a la insólita separación de un importante -aunque peculiar y dudosamente comprometido- socio comunitario. A su sucesora, Theresa May, le ha tocado dar cumplimiento al mandato de las urnas, según se está viendo, con un estrecho margen de maniobra, es decir, en clave rupturista, dada la presión mediática que ha acompañado el proceso y que, apalancada en el signo del resultado, parece no menguar fiscalizando cada paso negociador con las autoridades comunitarias y cada aspecto sectorial que la separación ponga en juego.

Para cerrar este apartado, es justo apuntar que el hecho de abandonar la Unión Europea no ha de implicar necesariamente la ruptura del Reino Unido con el tratado internacional por el que un determinado país reconoce la autoridad jurisdiccional del Tribunal Europeo de Derechos Humanos, puesto que es posible suscribirlo –ergo, en este caso, mantener su vigencia– sin pertenecer a la misma, como ocurre, paradójicamente, con Turquía, eterno aspirante a socio europeo que no se distingue, precisamente, por ser un ejemplo en materia de derechos humanos. Por tanto, sobre el papel, esa posibilidad existe, pero el panorama o escenario en que se ha de desenvolver, por lo hasta ahora expuesto, no resulta proclive ello. Está por ver si con unos posicionamientos políticos tan mediáticamente condicionados, se impondrá finalmente un estatus similar al de Turquía, como parece ser la intención que impregna la *Repeal Bill*[506] presentada por el gobierno de Theresa May.

En resumen, hemos visto cómo el euroescepticismo británico ha derivado en un antieuropeísmo capaz de determinar la ruptura con la Unión Europea y, como parte de dicho escenario, capaz a su vez de deslegitimar primero y amenazar con su rechazo después, la jurisdicción de Estrasburgo en materia de derechos humanos, todo ello en un clima político y mediático torticero, usando el pronunciamiento sobre determinados supuestos para acusarla de atacar gravemente la soberanía británica. Es aquí donde enlazamos con la fundada advertencia que abría este apartado, válida para cualquier país comunitario, respecto del peligro efectivo que una desafección europeísta puede conllevar en materia de derechos humanos al amenazar

[506] *The Repeal Bill: White Paper*, 30 de mayo de 2017. Disponible en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/604516/Great_repeal_bill_white_paper_accessible.pdf

el sistema de protección de derechos y libertades resultante del Convenio Europeo de Derechos Humanos.

5.1. El futuro del marco normativo presentado después del *Brexit*

Si las circunstancias histórico-legislativas del Reino Unido hacen de él un caso paradigmático, aún lo será más cuando finalmente se ejecute la desconexión total de éste de la Unión Europea.

En el momento de redacción de estas líneas, el Gobierno británico parece inclinarse por una salida total de las instituciones europeas lo que supondría renunciar a ser parte del Convenio Europeo de Derechos Humanos, con el pretexto de que los mismos derechos les serán aplicables mediante la *Human Rights Act 1998* (la cual, según las últimas informaciones, parece estar a salvo), si bien no en los mismos términos, pues con el afán de ganar en soberanía, dejarán de someterse a una autoridad europea superior (TEDH) en cuanto a su interpretación.

Con esto se pretende ejemplificar la complejidad de la situación política y legislativa que está por venir. No hay duda de que el futuro inmediato pasa por negociar los términos de cada uno de las normas aplicables en la actualidad como consecuencia de la pertenencia a la UE y mitigar así sus efectos ante la desconexión.

Sin entrar a valorar la idoneidad de los mecanismos empleados a la hora de garantizar la seguridad jurídica de los ciudadanos británicos, lo cierto es que hay numerosas normas que dejarán de tener vigencia en un escenario futuro si no se buscan fórmulas jurídicas que solucionen esta situación.

Hay que recordar que la gestación del Reglamento General de Protección de Datos encontró oposición por parte de algunos países europeos, siendo los representantes del Reino

Unido los que más firmemente mostraron su rechazo a dicha norma argumentando el incremento de las dificultades para el tráfico comercial y las trabas a la libre competencia[507].

En función de lo que tarde en demorarse la desconexión efectiva del Reino Unido y de la solución por la que se opte, la aplicación del GDPR tendrá una mayor o menor brevedad en su vigencia, pues cuando el Reino Unido abandone definitivamente la Unión Europea, dejará de ser un Estado miembro para pasar a considerarse un tercer Estado, y las transferencias de datos que lleven a cabo desde un país miembro hacia Reino Unido y viceversa, tendrán la consideración de "transferencias internacionales".

Hay quien defiende la adopción de una opción mixta, esto es, que Reino Unido, como país independiente, formase parte del Espacio Económico Europeo[508], en cuyo caso debería de adoptar igualmente las disposiciones del Reglamento por comprender ésta una de las materias relevantes en los acuerdos del EEE. Así, mientras Reino Unido podría continuar beneficiándose del mercado único, no tendría la obligación de cumplir con ciertas políticas europeas a las que estaba adscrito hasta ahora y con las que siempre se ha mostrado en desacuerdo como, por ejemplo, la Política Pesquera Común.

Sin embargo, este escenario parece poco probable, principalmente si tenemos en cuenta que uno de los motivos que han precipitado al Reino Unido al *Brexit* es el anhelo de una mayor soberanía así como su disconformidad con ciertas decisiones europeas, por lo que cuesta imaginarse al Reino Unido como socio de un Espacio Económico Europeo en el que no va a tener ningún papel decisivo para la adopción de acuerdos pero donde, sin embargo, se le va a exigir el cumplimiento de ciertos estándares[509]. Otra cosa sería que, en su inclusión en el EEE, se negociase un trato privilegiado por tratarse de un antiguo socio europeo.

---

[507] Conviene recordar en este punto que Reino Unido es un país líder en materia de comercio electrónico al por menor. Resulta difícil pues, obviar la ironía de su postura beligerante cuando, después de los acontecimientos por todos conocidos, Reino Unido ha tomado la decisión de poner fin al mercado interior europeo.

[508] JAY. *Guide to the General data Protection Regulation*, Sweet & Maxwell, London, 2017, p. 1, para. 006.

[509] Su poder de negociación se verá drásticamente reducido al perder la condición de Estado miembro y al quedar fuera de la toma de decisiones y debates que tengan lugar en el Consejo Europeo y en el Parlamento Europeo.

Lo más probable pues, es que Reino Unido tome la consideración de "tercer estado" por lo que, entre otras muchas cosas, se pondría fin al libre flujo de datos entre el país británico y los Estados miembros en los términos actuales. Esto, sin embargo, no significaría el fin de la transferencia de datos entre ambas partes, pues podría iniciarse un proceso mediante el cual se evalúe el nivel de protección de los datos en dicho territorio que, en caso de ser favorable –y considerarse un país "seguro" por parte de la Comisión Europea- permitiría el flujo de datos entre ambos territorios (como también se produce con los Estados Unidos, a través del acuerdo *Privacy Shield*).

Este procedimiento está expresamente previsto en el artículo 45 del GDPR[510] que dispone los diferentes parámetros que la Comisión debe tener en cuenta para evaluar la adecuación del nivel de protección, entre otros: la legislación pertinente, el acceso de las autoridades públicas a los datos personales o los recursos administrativos y demás acciones judiciales previstas para el reconocimiento de los derechos y libertades de los interesados, objeto del tratamiento.

Asimismo, otro de los factores a tener en cuenta en dicho examen está relacionado con la existencia de autoridades independientes de control encargadas de supervisar el cumplimiento en materia de protección de datos, con poderes de ejecución suficiente, y que dichos órganos estén en contacto directo con los organismos europeos de control así como con los dispuestos en los distintos Estados miembros. Habrá que ver pues, el papel que desempeñará la ICO una vez consumado el *Brexit*.

Esta protección será revisada periódicamente, al menos cada 4 años, que es el periodo de vigencia máximo que se le otorga a esta certificación de seguridad. No obstante, mientras dicha evaluación se lleva a cabo y teniendo en cuenta, sobre todo, las circunstancias especiales que rodean al Reino Unido, el artículo 46 prevé el flujo de datos entre terceros países, a falta de decisión por parte de la Comisión, cuando el tercer país en cuestión hubiera ofrecido garantías

[510] Artículo 45.1: "*Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica*".

adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas que quedan detalladas en el mismo precepto y que es de suponer que están implementadas en Reino Unido dado que, hasta ahora, ha contado con el paraguas de la legislación de la Unión Europea en dicha materia.

De todas formas, conviene hacer hincapié en que, mientras se redactan estas líneas, el proceso de negociación entre la Unión Europea y Reino Unido sigue su camino -no con demasiado éxito, debe reconocerse- y las noticias que se obtienen de ésta y otras materias se suceden con cuentagotas. Sin embargo, atendiendo a los hechos hasta ahora acaecidos, el Gobierno británico ha presentado varios documentos sobre los que fija su posición sobre asuntos claves, siendo uno de éstos, la transferencia de datos personales entre los Estados miembros y Reino Unido[511]. En ellos el Gobierno afirma su deseo de mantener la cooperación con la UE en materia de protección de datos para que el flujo de información entre ambos no se vea interrumpido, esgrimiendo principalmente, razones comerciales y de seguridad.

La británica *Data Protection Act 1998*, debido principalmente al tiempo transcurrido desde su promulgación, se encuentra un tanto desfasada en materia de protección de los derechos y libertades de los ciudadanos, especialmente en materia de los consumidores y usuarios, dado los significativos avances tecnológicos que se han sucedido en el transcurso de los años desde su publicación y como éstos han incidido en cuestión de datos personales. Esta norma, tenía previsto modificarse antes de la entrada en vigor del GDPR para ajustar sus preceptos a los nuevos estándares europeos, igual que el resto de los Estados miembros, por lo que el Gobierno británico redactó una *Data Protection Bill* contemplando el nuevo marco normativo, en tramitación parlamentaria mientras se redactan estas líneas[512].

a) Opción primera: declararse país seguro

[511] Disponible para consulta en https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/639853/The_exchange_and_protection_of_personal_data.pdf

[512] Una vez dicha norma entre en vigor, ésta se convertiría en la *Data Protection Act 2018*, derogando la *Data Protection Act 1998*, en vigor mientras se lleva a cabo la elaboración de esta disertación.

El objetivo del Gobierno británico, según ha explicado el Ministerio de Industrias Digitales y Creativas, es adoptar una legislación propia que incorpore las novedades introducidas por el GDPR para, una vez consumado el *Brexit*, disponer de unas disposiciones legales equiparables[513] con la Unión Europea[514] de modo que no se limite el tráfico de datos personales entre ambos.

Para eso han aprobado un texto normativo, la *Data Protection Bill*, en el que han incorporado derechos reconocidos en el Reglamento como el de acceso a los datos, a su traslado y a su borrado, incluyendo el derecho al olvido, así como incorporando prerrogativas nuevas como la facultad de solicitar el borrado automático de todo lo publicado en las redes sociales con una edad menor a los 18 años (bautizado popularmente como el "derecho a la inocencia").

En la *Data Protection Bill* se amplía la noción de "datos personales" al integrar en este concepto el ADN de las personas, la dirección IP de los usuarios así como los cookies de Internet. La vocación continuista del texto se observa en la adopción del criterio de "*accountability*" impuesto en el texto europeo en el que se basa, y que tiene como premisa exigir a las empresas que traten con información personal una responsabilidad activa en su gestión, anticipándose a los hechos y demostrando permanentemente que están cumpliendo la Ley.

Se incorporan también en el texto medidas proteccionistas con los consumidores y usuarios, dotando la *Information Comissioner's Office* de mayores poderes para defenderlos, así como regulando la existencia de la figura del Delegado de Protección de Datos (*Data Protection Officer*). Con el objetivo de disuadir a las grandes empresas del mal uso de la

[513] Hay que tener en cuenta que, bajo las últimas interpretaciones de la normativa europea, ya no es suficiente una legislación "adecuada" sino que ésta debe ser "equivalente" cosa difícil de lograr a menos que se adopte íntegramente el contenido del GDPR.

[514] Debe considerarse el alto estándar que se viene exigiendo por la Unión Europea en relación con la transferencia de datos personales a terceros países, como se vio en la famosa resolución STJUE (Gran Sala), de 6 de octubre de 2015, *Maximillian Schrems v. Data Protection Commissioner,* Asunto C-362/14.

información personal de sus clientes, se ha previsto un incremento notable de las multas que pueden acarrear sus acciones.

La opción de incorporar a la legislación doméstica del Reino Unido las previsiones dispuestas en el GDPR para así conseguir una equivalencia legislativa entre ambos territorios, con la intención de esquivar la catalogación como país no seguro una vez se consolide el *Brexit* y Reino Unido pase a considerarse un tercer país es, sin duda, una opción válida aunque hace aguas de cara al futuro. Con el tiempo, esto obligaría a la legislación británica a incorporar incondicionalmente aquellas modificaciones que vayan surgiendo en materia de protección de datos en la UE, aún sin participar de las discusiones ni en las negociaciones, lo que, dada la naturaleza de las relaciones institucionales y la beligerancia con la que los británicos han defendido hasta ahora sus divergencias en materia de protección de datos, resulta francamente poco creíble.

Como ya se ha dicho, el artículo 45 del Reglamento dispone cuales son los extremos a considerar por la Comisión Europea de cara a evaluar el nivel de protección adecuado de un tercer país o una organización internacional[515], entre los que se incluyen la legislación general y sectorial pertinente (punto que, como se verá después puede comprometer a Reino Unido), la existencia y funcionamiento de autoridades de control independiente o los compromisos internacionales asumidos en esta materia (lo que significaría que, un acuerdo bilateral entre

[515] Artículo 45.2: "*Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos:*

a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales".

Reino Unido y Estados Unidos -por ejemplo- con unos estándares más bajos que los de la normativa europea, podrían perjudicar un acuerdo con la UE).

Sin embargo, otro de los escenarios posibles es que el Reino Unido modifique el sentido de su nueva *Data Protection Act* una vez se despoje de las exigencias europeas, inclinándose por escoger fórmulas más acordes con su tradición jurídica del *common law*, menos proteccionista para la privacidad de los ciudadanos y más acorde con el liberalismo económico. No hay que olvidar que, el libre mercado y la mejora de la competencia, han sido dos de los argumentos principales esgrimidos por los partidos políticos que se posicionaron a favor del *Brexit*, así como que el organismo británico regulador en materia de protección de datos -el ICO- ha criticado con dureza las disposiciones del GDPR al considerarlo un obstáculo para las operaciones comerciales del siglo XXI.

Así las cosas, no parece descabellado pensar que, más allá de los esfuerzos iniciales por evitar toda disparidad con las directrices europeas en materia de protección de datos, en el futuro el Reino Unido adopte políticas y normativas dirigidas a obtener rédito económico de los datos personales.

Si bien esta vía comportaría que el Reino Unido no pudiera ser considerado como "país seguro" a los efectos del GDPR, lo cierto es que en la práctica, nada obstaría a los británicos a obtener a fuerza de negociación, un acuerdo internacional con la Unión Europea para la transferencia internacional de datos, como el que ésta tiene en vigor con los Estados Unidos (el llamado "*Privacy Shield*"[516]).

i. Primer obstáculo

Otra de las cuestiones determinantes a la hora de examinar la adecuación del Reino Unido a los estándares de privacidad europeos es su legislación doméstica en materia de protección de datos. Precisamente este punto es el que compromete más a los británicos, principalmente por la *Investigatory Powers Act 2016* (popularmente conocida como *Snooper's*

[516] En este escenario, Reino Unido debería adoptar sus propios acuerdos con aquellos territorios con los que quiera mantener un flujo de datos, como la Unión Europea o como Estados Unidos, con su propia versión del *Privacy Shield*, como por ejemplo, ha hecho Suiza.

Charter), ley que implanta prerrogativas desorbitadas y de dudosa legalidad hacia el Gobierno y que, de facto, permite la vigilancia masiva de los ciudadanos.

Habrá que comprobar si la permanencia de esta legislación después del *Brexit* es compatible con el estándar de protección exigido, cosa que parece muy alejada de las actuales propuestas políticas y jurídicas de la Unión Europea[517]. De hecho, conviene señalar cómo el TJUE dispuso hace escasos meses que el almacenamiento indiscriminado de datos es incompatible con las normas europeas[518], y lo hizo precisamente, declarando que la ley británica *Data Retention and Investigatory Powers Act 2014* (DRIPA), antecesora de la actual *Investigatory Powers Act 2016* que la derogó, carecía de las salvaguardas mínimas y, en consecuencia, resultaba incompatible con la UE .

La nueva legislación -cuya tramitación fue muy polémica dada la premura de su discusión-, aumenta considerablemente las prerrogativas de las autoridades británicas frente a la legislación anterior, cuyas extralimitaciones llevaron al TJUE a declararla contraria a las leyes de la Unión. Entre otras previsiones, la *Investigatory Powers Act 2016* obliga a los proveedores de servicios de Internet y a los operadores de telefonía móvil a almacenar los datos de la actividad online de sus clientes durante un periodo de 12 meses (esto se extiende a cualquier empresa que tenga un servicio de comunicación como *WhatsApp* o *Instagram*). Junto a ello, se permite a las autoridades acceder a los ICRs[519] sin orden judicial y por parte de un gran espectro de organismos públicos que poco o nada tienen que ver con la investigación de

---

[517] Cfr. JAY. *Guide to the General data Protection Regulation*, ob. cit.

[518] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 21 de diciembre de 2016, en los Asuntos acumulados C-203/15 y C-698/15 (*Tele2 Sverige AB v. Post- och telestyrelsen; Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*), cuyos remitentes (los tribunales sueco y británico, respectivamente) solicitaban del TJUE conocer la compatibilidad de sus normativas nacionales con el derecho de la Unión, especialmente, con el artículo 15.1 de la Directiva sobre la privacidad y las comunicaciones electrónicas (Directiva 2002/58/CE del Parlamento 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), en relación con los artículo 7, 8, 11 y 52.1 de la Carta de Derechos Fundamentales de la Unión Europea. El fallo del Tribunal, ante el argumento británico de la necesidad de actuar bajo la amenaza terrorista global, sostiene que ninguna legislación nacional puede exceder los límites de lo que es considerado estrictamente necesario pues esta conducta de ninguna manera puede quedar justificada en una sociedad democrática.

[519] *Internet Connection Records*, es donde queda almacenado digitalmente la actividad en Internet de cada usuario, las páginas web que visita, el dispositivo utilizado para ello, su dirección IP, la cantidad de datos descargados o compartidos… entre otra mucha información.

delitos trascendentes -que es el argumento principal para la implantación de esta normativa: la seguridad nacional- y se les dota de una herramienta a la que llaman "filtro", capaz de cruzar los datos de cualquier ciudadano.

Es decir, no sólo no hay cambios sustanciales con respecto a la anterior regulación, que permitía examinar a cualquier que se considerase sospechosos (concepto jurídico indeterminado donde los haya), sino que se agilizan los trámites para ello al prescindir, en la mayoría de los casos, de la obligatoriedad de una orden judicial.

Esta legislación seguramente será invalidada en el futuro más inmediato, de hecho ya se están dando los primeros pasos[520], y si a esto le sumamos que en sus preceptos se incluyen disposiciones claramente contrarias a los tratados internacionales en materia de derechos humanos de los que es parte Reino Unido –como por ejemplo, medidas que permiten deportar a personas a países donde está vigente la tortura-, sus días parecen contados. Asimismo, dicha normativa parece incompatible con la Directiva 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos[521].

[520] Recientemente, en una decisión del 30 de enero de 2018, la Corte de Apelación del Tribunal Superior de Justicia de Londres (*High Court of Justicie Queen's Bench Division*), ha dispuesto que la DRIPA (The Data Retendion and Investigatory Powers Act 2014), cuyo contenido se reproduce y amplia en la *Investigatory Powers Act 2016*, era en muchos aspectos "inconsistente con el derecho de la Unión Europea", apoyándose en la Sentencia que el TJUE dictó en 2014 sobre la DRIPA y que supuso su derogación - *Digital Rights Ireland Ltd v. Minister for Communications and Others; Kärntner Landesregierung v. Michael Seitlinger and Others*, asuntos acumulados C-293/12 y C-594/12-, poniendo de relieve como esta norma se utilizó para acceder a los datos personales de personas que no estaban siendo investigadas por ningún crimen trascendente, así como la inexistencia de una autoridad supervisora independiente. Caso *Secretari of State for the Home Department v. Watson & Others*, C1/2015/2612 & 2613, [2018] EWCA Civ 70, Court of Appeal (Civil Division). Ante estos hechos, se da por sentado que la *Investigatory Powers Act 2016* cuya adecuación a la normativa europea se someterá a examen por los tribunales ya requeridos para ello, adolecerá de los mismos defectos, por lo que deberá modificarse para respetar los estándares europeos en materia de privacidad, si es que así lo desean las autoridades británicas una vez consolidado el *Brexit*.

[521] Esta norma establece en su articulo 35 que la UE deberá dar permisos para la transferencia de dichos datos siempre y cuando un país ofrezca garantías a los mismos. El artículo 37, por su parte, dispone las distintas herramientas para garantizar una transferencia de datos adecuada, entre los que se incluyen certificaciones, la adhesión a códigos de prácticas o la adopción de *Standard Form Contracts*.

Así las cosas, nada parece seguro para el futuro de Reino Unido en materia de protección de datos, pues esta ley junto con otros extremos comentados, podrían suponer hechos determinantes para declararlo territorio no seguro, cosa que no parece tan descabellada si tenemos en cuenta que con el mismo argumento, en el famoso caso *Schrems*[522], el TJUE invalidó en 2015 el acuerdo *Safe Harbor* para la transferencia internacional de datos entre Estados Unidos y la UE[523].

ii. Segundo obstáculo

Por otra parte, tampoco ayuda el hecho de que el Parlamento británico haya decidido, mediante votación mayoritaria, dejar de aplicar la Carta de Derechos Fundamentales de la UE[524] que, a grandes rasgos, es el instrumento jurídico que reafirma el contenido dispuesto en el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Públicas así como las Cartas Sociales adoptadas por la UE y por el Consejo de Europa y que, además, ratifica a los países firmantes en su compromiso de cumplimentar la jurisprudencia del Tribunal de Justicia de la Unión Europea y del Tribunal Europeo de Derechos Humanos, ofreciendo una mayor seguridad jurídica dentro de la UE.

Esta decisión es una de las pocas excepciones a la presunta voluntad continuista de los británicos, aunque parece que el contenido de esta Carta va a incorporarse a la legislación británica post-*Brexit* mediante la adopción como propios de los derechos y principios reconocidos hasta el momento por la jurisprudencia de los tribunales europeos en referencia a la Carta, claramente esta solución no ofrece garantías suficientes en términos de seguridad jurídica.

De hecho, en cuanto a la protección de datos personales este nuevo escenario añade dificultades a la intención del Gobierno británico de crear un entorno jurídico equivalente a la

[522] STJUE (Gran Sala), de 6 de octubre de 2015, *Maximillian Schrems v. Data Protection Commissioner,* Asunto C-362/14.

[523] Mediante ésta, se anula la Decisión de la Comisión 2000/520/CE, de 26 de julio, que, con arreglo a la Directiva 95/46/UE, establecía el nivel adecuado de protección de las garantías internacionales entre ambos territorios.

[524] 2000/C 364/01.

protección que proporciona la Unión Europea a través del GDPR que, además, hace constantes referencias a la Carta a lo largo de su articulado.

La Carta, cuyo artículo 8[525] contiene una previsión específica relativa al derecho de protección de datos, es un texto fundamental en tanto que ha supuesto un paso más en la regulación de esta materia, mucho más allá del artículo 16 del TFUE, el artículo 8 del Convenio Europeo de Derechos Humanos, o la propia Directiva 95/46/CE –ahora derogada-, todos ellos instrumentos dedicados a la protección de este mismo extremo. Conviene recordar que, desde que la Carta obtuvo el estatus de Tratado Internacional en 2009, muchas decisiones del Tribunal de Justicia de la Unión Europea –así como de los propios tribunales británicos- se han basado en sus disposiciones, asimismo su criterio interpretativo se ha convertido en indispensable a la hora de evaluar solicitudes de transferencias internacionales de datos con terceros países[526]. El cumplimiento de la Carta pues, podría ser un elemento más que determinante para que la Unión Europea considerase a Reino Unido como un "país seguro" en materia de protección de datos.

b) Opción segunda: adoptar Binding Corporate Rules

La segunda de las opciones que podría emplearse tras la salida del Reino Unido de la Unión Europea sería adoptar las llamadas *Binding Corporate Rules* (BCRs) que han sido traducidas al castellano como "normas corporativas vinculantes".

Las normas corporativas vinculantes son, a grandes rasgos, un conjunto de reglas -una especie de código de conducta pero con carácter vinculante- específicas sobre el tratamiento de

[525] Artículo 8, Protección de datos de carácter personal: "*1. Toda persona tiene derecho a la protección de los datos de carácter personal que le 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 le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente*".

[526] Como ejemplo, el Dictamen 1/15 del Tribunal de Justicia (Gran Sala) de 26 de julio de 2017 acerca de la idoneidad sobre la transferencia de los datos del registro de nombres de pasajeros entre la UE y Canadá, en el que el TJUE dispuso que para juzgar los hechos sólo iba a tener en cuenta el artículo 8 de la Carta de Derechos Fundamentales de la UE porque ésta establecía las condiciones de tratamiento de datos de una manera más específica que el propio artículo 16 del TFUE: "En efecto, si bien es cierto que ambas disposiciones declaran que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan, únicamente el artículo 8 de la Carta prescribe de manera más específica, en su apartado 2, las condiciones en que tales datos pueden ser objeto de tratamiento", para. 120 .

los datos personales que lleva a cabo un grupo empresarial, normalmente multinacional, mediante el cual dicha corporación garantiza ante los organismos reguladores que la transferencia internacional de datos entre miembros del mismo grupo empresarial o de una unión de empresas dedicadas a una actividad económica conjunta cumple[527] con la normativa europea con independencia de que el país de destino garantice o no un nivel adecuado de protección de esos datos de acuerdo con los parámetros de la legislación del país de origen de los mismos[528].

Esta opción, que en la práctica ya estaba en funcionamiento[529], se recoge expresamente en el GDPR[530] para el caso de que la Comisión disponga que un tercer país, parte de su territorio o una organización internacional, ya no garantice un nivel de protección adecuado lo que, consecuentemente, llevaría a la prohibición de transferir datos entre éste y la Unión Europea "*salvo que se cumplan los requisitos del presente Reglamento relativos a las transferencias basadas en garantías adecuadas, incluidas las normas corporativas vinculantes*"[531].

El artículo 47 del Reglamento dispone que la autoridad de control competente aprobará normas corporativas vinculantes siempre que se cumplan los requisitos que a continuación enumera y que van, desde garantizar el derecho a no ser objeto de decisiones basadas exclusivamente en un tratamiento automatizado, hasta tener previsto un procedimiento de reclamación ante la autoridad competente, pasando por la obligación de realizar auditorías

[527] Por ello, las BCRs deben conferir derechos ejercitables a los sujetos objeto del tratamiento de datos, que legitiman éstas.

[528] Las normas corporativas vinculantes se definen en el art. 4. 20) del GDPR como "*las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta*".

[529] Sin embargo, ha ido evolucionando rápidamente a lo largo de los últimos años pues, en la práctica, se ha convertido en una vía de escape para ciertas empresas multinacionales cuyas transferencias no cumplen las exigencias europeas, lo que ha ocasionado que tanto la doctrina como los gobiernos exijan la adopción de medidas efectivas para asegurar un estándar aceptable en materia de protección de datos. Así, se están empezando a exigir vincular estos mecanismos a conceptos como "*accountability*" o la responsabilidad social corporativa, entre otros. MOEREL. *Binding Corporate Rules, Corporate Self-regulation of Global Data Transfers*, Oxford University Press, Oxford, 2012, p. 147.

[530] Sin embargo este sistema no es nuevo, ya se encontraba previsto en la Directiva 95/46/CE que ahora el GDPR deroga, así como, por ejemplo, en nuestra LOPD de 1999.

[531] Consideración preliminar 107.

periódicas. En todo caso, respecto de las normas corporativas vinculantes, la Comisión podrá especificar la forma y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control.

Sin embargo, se evidencian problemas prácticos a la hora de adoptar BCRs pues para su implementación, se requiere la autorización previa de todas las agencias nacionales de protección de datos lo que plantea el problema de qué estatus tendrá la ICO británica después del *Brexit*. En principio no parece lógico que continúe gozando de la misma posición jurídica que hasta ahora, pues quizás no desde un principio, pero con el paso del tiempo y la evolución jurídica, puede no ofrecer las mismas garantías que sus homólogos europeos. No obstante, para salvar este obstáculo, podrían adoptarse acuerdos de reconocimiento mutuo de procedimientos entre las agencias estatales de protección de datos de los Estados miembros y la ICO, pero para ello debería existir cierta equivalencia entre los estándares de protección de la normativa británica y la europea.

c) Opción tercera: emplear Standard Form Contracts

Una última solución -aunque más antigua[532] y parcialmente efectiva- sería la autorización de las transferencias internacionales de datos en base a cláusulas contractuales tipo, estandarizadas por distintas Decisiones de la Comisión Europea, y que se prevén en el artículo 46 del GDPR, junto con las normas corporativas vinculantes, para el caso de ausencia de una decisión por la que se constate la adecuación de la protección de los datos en un tercer país, con el objeto de tomar medidas que traten de compensar dicha situación.

Para este supuesto se prevé la adopción de cláusulas tipo de protección de datos adoptadas por la Comisión[533] o por una autoridad de control capaz de asegurar la observancia

[532] Este mecanismo era el que empleaba la Agencia Española de Protección de Datos antes del 2009, cuando la agencia empezó a autorizar transferencias internacionales de datos en base a *Binding Corporate Rules*.

[533] Hasta la fecha la Comisión Europea ha publicado dos tipos de contratos con cláusulas tipo: en primer lugar, de protección para las transferencias de datos realizadas desde organismos de control en la Unión Europea, hacia otros establecidos fuera de ésta o del Espacio Económico Europeo, y en segundo lugar, para cuando el destino de los datos sea una entidad de procesamiento de datos no europea. Ambos tipos de contratos se encuentran disponibles en: https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

de los requisitos de protección de datos y derechos de los interesados, así como que sean adecuados a los estándares de protección dentro de la Unión, incluida la exigibilidad por parte del interesado de sus derechos así como de las acciones legales efectivas, lo que le permitiría obtener la reparación o una indemnización tanto en la Unión Europea como en un tercer país. Dice el GDPR que "*en particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde le diseño y por defecto*"[534].

Es decir, se trata de un acto jurídico creado al amparo del Derecho de la Unión o de los Estados miembros por el cual se vincula al encargado respecto del responsable y se establece el objeto, la duración, la naturaleza y la finalidad del tratamiento de determinados datos personales, así como las obligaciones y los derechos del responsable.

La posibilidad de que el responsable o el encargado del tratamiento recurran a cláusulas tipo de protección de datos adoptadas por la Comisión o una autoridad de control no debe obstar para que los responsables o encargados incluyan éstas en un contrato más amplio -como un acuerdo entre dos encargados- o para que añadan otras cláusulas o garantías adicionales, siempre que mantengan los niveles de protección de los interesados. El Reglamento, hace hincapié en la conveniencia de complementar los contratos tipo con otras garantías de protección, pues es consciente de la limitada seguridad jurídica que éstas ofrecen como mecanismo efectivo de control, motivo por el cual la Comisión se reserva, en todo caso, las competencias de ejecución.

Conviene comentar en este punto que el GDPR ha introducido grandes cambios respecto del régimen de transferencias internacionales anterior, por ejemplo, en relación a los exportadores de datos, pues por primera vez se permite que éste sea tanto un responsable como un encargado del tratamiento, acabando con la disparidad de criterios de las legislaciones nacionales de los Estados miembros que, en muchos casos, limitaba las exportaciones a aquellos que eran responsables del tratamiento. A partir de ahora, se dinamizan las

[534] Consideración preliminar 108.

transferencias internacionales mediante la subcontratación a terceros países de prestadores de servicios establecidos en la UE lo que, en términos de seguridad, no es lo más propicio.

Esta vocación del GDPR de estimular las transferencias se observa también en la reducción de los supuestos en los que es necesaria autorización y notificación previa de las transferencias internacionales[535]. Mientras que la normativa anterior obligaba a los exportadores de datos a solicitar a la autoridad nacional de control una autorización previa (que les era concedida sólo si conseguían acreditar las garantías suficientes) para poder transferir datos a importadores establecidos en terceros países que no gozaban de un nivel adecuado de protección, el GDPR permite que las transferencias se realicen sin necesidad de autorización ni notificación previa, excepto para casos contados como, por ejemplo, que las garantías se aporten mediante un contrato ad hoc o se trate de una situación en la que prime el interés legítimo del responsable del tratamiento.

No obstante todo lo anteriormente expuesto, desde un punto de vista eurocentrista y en cuanto a la protección de los derechos y libertades, no hay que perder de vista que, en algunos casos, el GDPR será de aplicación a ciertas compañías británicas con independencia de la determinación que tome finalmente el Reino Unido, dado que el objeto del nuevo Reglamento es preservar los derechos y las mismas garantías a los ciudadanos europeos frente a todas las compañías que se dediquen al tratamiento de datos personales en la UE aún cuando éstas no se encuentren domiciliadas en suelo europeo. Así pues, lo único cierto después del *Brexit* es que el GDPR será de aplicación a las empresas británicas que procesen datos personales de los europeos o que monitoricen su comportamiento en suelo europeo, por extensión del principio de territorialidad instaurado en el artículo 3 del GDPR.

[535] Por ésta y otras cuestiones expuestas a lo largo de este trabajo, cuesta creer que el fin último del GDPR sea ampliar el margen de derechos y garantías de los ciudadanos europeos frente a sus datos pues, salvo destacables excepciones, el propósito general parece ser lograr una armonización de las legislaciones con el fin de no obstaculizar el mercado interior ni la libre competencia.

5.2. Consideraciones finales

La evolución del sistema de protección de la privacidad por parte del Reino Unido ha sufrido grandes fluctuaciones en cuanto al estado de la cuestión y su protección hasta el punto de que, habiéndose situado a la cabeza de la protección de datos personales, hoy parece adoptar posturas diametralmente opuestas. De hecho, Reino Unido es actualmente uno de los países del mundo que más vigilada tiene a su sociedad, más aún con la aprobación de algunas normas de urgencia en materia de terrorismo altamente controvertidas, como la derogada DRIPA.

Mientras que se encuentran vestigios de la protección del derecho a la privacidad en jurisprudencia inglesa que data del siglo XVIII[536], desde los últimos quince años, estamos asistiendo a una degradación de dicho sistema de protección por parte de las políticas del Reino Unido, agravada aún más por la coyuntura actual derivada del *Brexit*, así como su posible salida de instrumentos como el CEDH.

Lo acontecido en el Reino Unido es una muestra de la susceptibilidad de los sistemas jurídicos a sufrir variaciones en función de las necesidades sociales, culturales y económicas, pero también en función de las prioridades políticas del momento. Partiendo de dicha premisa, resulta paradójico como, ahora más que nunca, en el entorno global y digital en el que nos insertamos y que proporciona constantemente nuevas amenazas para la privacidad, el Reino Unido ha resuelto -bien por razones ideológicas aparejadas a lograr un mayor control social, bien plegándose a la lógica del beneficio y otras consideraciones neoliberales-, desincentivar el estándar de protección que había conseguido instaurar para la privacidad de sus ciudadanos[537].

A raíz de las últimas innovaciones tecnológicas, los acontecimientos terroristas de los últimos tiempos y el rumbo neoliberal de las recientes políticas públicas, puede decirse que el Reino Unido ha sufrido un cambio sustancial en cuanto a la privacidad se refiere[538] -perceptible

[536] *Entick v. Carrington* [1765] EWHC KB J98 95 ER 807, King's Bench, 2 de noviembre de 1765.

[537] Resulta interesante poner en relación las decisiones políticas y legislativas que se derivan del estándar existente de privacidad con el nivel de democracia efectiva. Cfr. SCHWARTZ. "Privacy and Democracy in Cyberspace", en *Vanderbilt Law Review*, Vol. 52, 1999.

[538] Así lo advirtió ya en 2004, Richard Thomas, el responsable de la ICO cuando dijo que reino Unido se estaba convirtiendo en una sociedad vigilada, en sus propias palabras: "*sleepwalking into a surveillance society*".

incluso antes de ratificarse en su decisión de abandonar la Unión Europea-, alejándose cada vez más de los estándares europeos y su proteccionismo, e inclinándose hacia el modelo norteamericano y su principio de no intervención[539].

De hecho, el Gobierno británico posee en la actualidad unos poderes de vigilancia y recopilación de información mucho mayores que en cualquier momento de su historia y, en muchos aspectos, más amplios que los disponibles para las autoridades en países democráticos comparables[540]. Pero no se trata sólo de los poderes públicos sino que, en connivencia con éstos, cada vez son más las compañías privadas que están almacenando datos personales con finalidad de negocio o con propósitos que hoy por hoy se desconocen[541].

Cabe decir también que, la tradición de la prensa amarillista en Reino Unido es tal, que constituye un *lobby* ciertamente relevante en la sociedad británica[542]. Todas las políticas legislativas propuestas encaminadas a conseguir una regulación más idónea e incluso hermética de la privacidad, se han dado de bruces con la fuerte oposición de las asociaciones de prensa y de reporteros gráficos británicos, bajo el argumento de que dichas medidas supondría el fin del periodismo "libre" que se viene ejerciendo en la actualidad[543].

---

[539] "*In the United Kingdom, our interviews with privacy leaders revealed a privacy field that straddles the Atlantic in a deeply liminal state: one foot standing on American soil and one foot firmly planted on the Continent*", BAMBERGUER/MULLIGAN. *Privacy on the Ground. Driving Corporate Behavior in the United States and Europe*, ob. cit., p. 145.

[540] MATHIESON. *Privacy Law Handbook*, The Law Society, London, 2010, p.7.

[541] Reino Unido se ha erigido como uno de los países del mundo que más cámaras de seguridad, públicas y privadas, cuya justificación principal gira en torno a razones de seguridad nacional, protección pública y detección y prevención del crimen. La denominada *surveillance* reviste distintas formas, desde circuitos cerrados de televisión, hasta la monitorización de los teléfonos móviles, pasando por los registros de salud o las fichas policiales, todas ellas formas atentatorias contra la privacidad de los ciudadanos.

[542] En el examen de ciertos métodos periodísticos empleados por algunos medios británicos, afirma PAUNER CHULVI la existencia de "no sólo un modo de hacer periodismo basado en prácticas ilegales sino también un maridaje entre política y medios de comunicación que fuerza los límites éticos en democracia". Cfr. "Privacidad y periodismo: el escándalo Murdoch sobre escuchas telefónicas en News of the World", en *Revista de Derecho Político*, nº 88, 2013, p. 247.

[543] Parece paradójico que esto continúe sucediendo hoy en día, después del escándalo Murdoch que puso en evidencia los métodos periodísticos de algunos de los tabloides británicos y la correlación entre la corrupción política y la corrupción periodística en el Reino Unido. Para un análisis más pormenorizado de dicho caso, BURDEN. *News of the world? Fake Sheikhs & Royal Trappings*, Eye Books, London, 2008.

Pese a que el ejercicio de acciones que pueden resultar invasivas de la privacidad en el Reino Unido, son conformes con la legislación vigente en materia de protección de datos, siempre hay excepciones en base a conceptos jurídicos indeterminados que, además, se ven afectados por normas especiales con gran incidencia en la materia, como la polémica *Investigatory Powers Act 2016*. De hecho, como ya se ha visto, son reiteradas las veces en las que los tribunales europeos han recriminado al Reino Unido la ineficacia práctica del derecho a la privacidad.

Los argumentos británicos para justificar dicha realidad se basan tradicionalmente en la inexistencia en su legislación de un reconocimiento expreso del derecho a la privacidad cuestión que, si bien se ha tratado de suplir con figuras jurídicas que sólo otorgan una protección parcial e inefectiva de este derecho, con la entrada en vigor del GDPR deberían verse prácticamente superadas.

Así las cosas, el nuevo escenario político que se presenta para Reino Unido es incierto pues, una vez deje de estar sometido a los criterios europeos en materia de protección de datos, mucho más conservadores que los estándares tradicionales del ámbito jurídico del *common law*, puede que los ciudadanos vean revertidas las protecciones que les brindaba la legislación europea de acuerdo con la nueva tendencia británica, encaminada hacia una liberalización de la privacidad. A tenor de todo el examen realizado de la cuestión y atreviéndose a especular sobre el futuro, no resulta difícil imaginar que, una vez el Reino Unido deje de contar con el paraguas europeo, pueda inclinarse por basar su legislación doméstica en otros criterios –como, por ejemplo, sus raíces del *common law* que nunca desaparecieron-, produciéndose una regresión en el modelo de protección de ciertos derechos relacionados con la privacidad.

6. Recapitulación

I. La evolución del modelo de protección de la privacidad en el Reino Unido reviste ciertas peculiaridades, en primer lugar, por la dicotomía de su sistema legal, que aúna dos corrientes aparentemente contrapuestas, esto es, de un lado su tradición jurídica del *common law*, íntimamente ligado al precedente judicial y, de otro, un positivismo jurídico creciente a

raíz de la integración europea, adoptando el principio de soberanía nacional mediante el cual se legitima al Parlamento para legislar en cualquier ámbito del Derecho.

En segundo lugar, este particular fenómeno se une al hecho de que el Reino Unido no cuenta con una constitución escrita, sino con lo que ha sido llamado "*unwritten constitution*", que otorga fuerza vinculante al *common law*, a las disposiciones normativas de origen parlamentario así como a los tratados internacionales, y es a través de estos instrumentos y siguiendo el criterio orientador de la *rule of law*, que se provee a la ciudadanía de derechos y libertades exigibles.

Las concretas particularidades del sistema constitucional anglosajón permiten la mutabilidad de su contenido, adaptando sus reglas y principios a las circunstancias concretas de cada momento histórico. La variabilidad del sistema de valores anglosajón queda patente también en la configuración de los derechos y libertades ciudadanas así como en su sistema de garantía, lo cual se plasma igualmente en la evolución del modelo británico de protección de la privacidad.

II. Se pueden distinguir tres etapas importantes en este sentido: un primer estadio, marcado por la promulgación de la *Data Protection Act 1984* (cuyo contenido se amplió mediante la *Data Protection Act 1998*, que incorporaba las exigencias europeas de la Directiva 95/46/CE) que reconoce un derecho a la protección de datos, como algo intrínsecamente ligado a la identidad y a la privacidad, e introduce un sistema adecuado para su garantía, proporcionando herramientas jurídicas a los tribunales que, hasta el momento, sólo concedían exigua protección a la privacidad a través de algunas figuras tradicionales del *common law* como la *breach of confidence*, la *defamation* o la *nuisance*.

La segunda fase viene determinada por la aprobación de la *Human Rights Act 1998*, mediante la cual se incorporaron a la legislación británica los derechos y libertades garantizados por el Convenio Europeo de Derechos Humanos de 1950 que, a partir de entonces, resultan directamente aplicables, así como la jurisprudencia del Tribunal Europeo de

Derechos Humanos interpretando dichos preceptos, dejando éste de ser un órgano de segunda instancia.

La HRA convirtió el CEDH en Derecho vinculante para los poderes públicos británicos, proclamando los derechos recogidos en la nueva norma como una suerte de declaración de derechos fundamentales para su ciudadanía. El artículo 8 de ambos textos, reconocen el derecho a la vida privada, lo que supuso un punto de inflexión para su protección.

La tercera y última de las fases que ha incidido en la cuestión de estudio viene integrada por múltiples acontecimientos y, de hecho, su futuro está aún por determinar. Por una parte, se ha detectado una disminución notable del modelo británico de protección de la privacidad, a consecuencia de la legislación dictada en los últimos quince años, cuyo exponente máximo encontramos en la *Data Retention and Investigatory Powers Act 2014* (DRIPA) declarada contraria al Derecho de la UE.

Por otra parte, debido al euroescepticismo consolidado con los resultados del referéndum celebrado el pasado 23 de junio de 2016 que supuso los inicios del *Brexit* y que plantea numerosos retos futuros, entre ellos, determinar la situación en la que se verá abocado el Reino Unido en materia de transferencias internacionales de datos, pues a partir de su desconexión de la UE, puede pasar a considerarse "tercer estado" a efectos de la normativa europea. Asimismo, el Gobierno británico parece decidido a abandonar el CEDH lo que pondría en peligro el esquema normativo determinado por la *Human Rights Act 1998*.

Y, mientras tanto, el GDPR ha entrado en vigor también para el Reino Unido, motivo por el cual, el Gobierno británico redactó una *Data Protection Bill* contemplando el nuevo marco normativo europeo, en tramitación parlamentaria mientras se redactan estas líneas.

III. Se ha convenido en situar la creación del derecho a la privacidad en el *common law*, en el artículo que en 1890 escribieron WARREN y BRANDEIS en el *Harvard Law Review* titulado "*The right to privacy*". Sin embargo, la evolución de este nuevo derecho se desarrolló de forma distinta en la vertiente americana y anglosajona de dicho sistema jurídico.

Históricamente, el *common law* anglosajón no reconocía ningún derecho a la privacidad ni tampoco contemplaba un derecho de responsabilidad civil, sin embargo, sí que ofrecía remedios parciales, principalmente, a través de las figuras de la *breach of confidence* (revelación de secretos), el *trespass* (allanamiento), la *nuisance* (perjuicio, molestias) o la *defamation and malicious falsehood* (difamación).

En el Derecho anglosajón, las referencias jurídicas de lo que en la actualidad definimos como derecho a la privacidad, están íntimamente relacionadas con la protección de la información personal de los ciudadanos y tuvieron sus comienzos en los años setenta, a raíz de la incipiente introducción de los ordenadores en la sociedad.

IV. Hubo que esperar hasta el Convenio del Consejo de Europa de 1981 para la protección de datos personales para que el Reino Unido estableciese los pilares de lo que sería el derecho a la protección de datos moderno, a través de la *Data Protection Act 1984*. Esta norma fue una de las primeras leyes en materia substancial de protección de datos en todo el mundo, cuyo objetivo primero era establecer el régimen jurídico sobre la tenencia y procesamiento automatizado de información.

Uno de los aspectos clave de esta Ley fue el establecimiento de los principios fundamentales en los que se debía cimentar toda actuación relacionada con los datos personales, conformado por ocho puntos de contenido muy general. En cuanto a las garantías, consagró por vez primera los derechos de información, acceso, rectificación y borrado de datos personales, obligó a aquellos que almacenaban datos personales a inscribirse en un registro específico, creó una autoridad de control independiente para su supervisión (*The Office of the Data Protection Registrar*) e implantó unos órganos jurisdiccionales especiales para tratar asuntos en materia de protección de datos (el *Information Rights Tribunal*), entre otras.

Si bien la *Data Protection Act 1984* fue una legislación precursora en materia de protección de datos y su aplicación estaba produciendo efectos satisfactorios, su derogación por la *Data Protection Act 1998* respondió a exigencias europeas, por la implementación de la Directiva 95/46/CE, así como debido a la evolución de la tecnología en ese lapso de tiempo.

Por ello, se reproduce el esquema normativo y se comparte mucha de la terminología con la legislación anterior aunque, asimismo, se incorporan nuevos derechos subjetivos en torno a la protección de los individuos, se integran nuevos derechos de acceso y a ser informado respecto de las decisiones automatizadas y se establece como regla general, la prohibición de exportar datos a terceros países.

V. La *Human Rights Act 1998* supuso un punto de inflexión para el proceder del sistema legal anglosajón, pues de alguna manera vino a paliar la ausencia de una *Bill of Rights* en el ordenamiento constitucional británico que, hasta entonces, dejaba en manos del *case law* la protección de los derechos y libertades de la ciudadanía.

A través de los derechos recogidos en la HRA, se produce una equivalencia, tanto conceptual como normativa, con los derechos y libertades reconocidos por el Convenio Europeo de Derechos Humanos, reformulando las relaciones entre el Parlamento y los órganos jurisdiccionales en la interpretación y aplicación de las leyes, así como para la protección de la privacidad, reconocida en su artículo 8, que pasa a protegerse como mecanismo adicional al derecho de protección de datos.

Además de convertir en vinculante el contenido del CEDH, la HRA impone a todos los poderes públicos la obligatoriedad de actuar, en el ejercicio de sus funciones, de forma compatible con los derechos del CEDH, lo que incluye también a la judicatura. A partir de entonces, los órganos jurisdiccionales del Reino Unido tienen la obligación de interpretar la legislación de conformidad con el Convenio y así como acatar en todo lo posible la jurisprudencia emanada del Tribunal Europeo de Derechos Humanos.

Ello supuso igualmente un paso decisivo en la protección de la privacidad, mediante el reconocimiento del derecho a la vida privada en su artículo 8, derecho que, hasta entonces, no gozaba de soporte legal específico en la legislación británica y que a partir de dicho momento, se instituyó como un bien jurídico a proteger, bajo una fórmula legal bajo la cual resulta directamente aplicable, tanto para los individuales como para las autoridades públicas.

Destaca la jurisprudencia del TEDH y su forma de interpretar el artículo 8 que ha sido esencial en la formación y aplicación jurídica del derecho a la privacidad por los tribunales británicos y que, asimismo, ha contribuido a perfilar y ampliar su significado.

VI. En cuanto al escenario actual e inmediatamente futuro, más allá de destacar la disminución del alto estándar de protección del que gozaba la privacidad en el Reino Unido a raíz de los últimos años –permitiendo actualmente la vigilancia masiva de los ciudadanos mediante políticas que claramente abogan por la limitación del espacio privado de las personas- conviene plantear soluciones frente a los retos más inmediatos que se plantean para el Reino Unido una vez se consolide el *Brexit*, especialmente respecto de la naturaleza de las relaciones que tendrán lugar entre la Unión Europea y el Reino Unido, que podría pasar a considerarse un "tercer estado" a efectos de la normativa europea de protección de datos.

Esto, sin embargo, no significaría el fin de la transferencia de datos entre ambas partes, pues pueden adoptarse distintas vías para ello. En primer lugar, podría iniciarse un proceso mediante el cual se evalúe el nivel de protección de los datos en territorio británico que, en caso de ser favorable y considerarse un país "seguro" por parte de la Comisión Europea, permitiría el flujo de datos entre ambos territorios.

El Gobierno británico parece inclinarse por esta solución, manteniendo de cara al futuro los estándares europeos que ahora tratan de incorporar mediante la *Data Protection Bill*. Sin embargo, el Reino Unido tiene vigente algunas normas domésticas que podrían dificultar esta vía y, a ello, debe añadírsele su aparente voluntad de abandonar el CEDH y la Carta de Derechos Fundamentales de la UE, así como la beligerancia con la que recibieron en su día al GDPR.

Una segunda opción, sería adoptar las llamadas *Binding Corporate Rules*, posibilidad que recoge expresamente en el Reglamento europeo pero que, sin embargo, podría comportar ciertos problemas prácticos pues para su adopción, se requiere la autorización previa de todas las agencias nacionales de protección de datos, por lo que deberá estarse al estatus que ostentará la ICO británica después del *Brexit*.

La tercera y última solución, pasa por emplear *Standard Form Contracts*, es decir, la autorización de las transferencias internacionales de datos en base a cláusulas contractuales tipo, que se regulan en el artículo 46 del GDPR. Sin embargo, el mismo Reglamento hace hincapié en la conveniencia de complementar los contratos tipo con otras garantías de protección, pues es consciente de la limitada seguridad jurídica que éstas ofrecen como mecanismo efectivo de control.

VII. La evolución del Derecho no tiene porqué encontrar límites en tanto que el comportamiento humano está en permanente evolución, es una cuestión de voluntad política y demanda ciudadana. Así, y tal como evidencia la evolución del sistema británico, un ordenamiento jurídico no es neutral sino que obedece a unos intereses políticos concretos que dan respuesta a determinados intereses económicos, sociales y culturales cambiantes, lo que permite la completa evolución de todo un sistema de protección jurídica, en este supuesto en concreto, de la privacidad y el derecho a la protección de datos personales.

VIII. Asimismo, la construcción del derecho a la protección de datos personales, en el sistema jurídico y la evolución que ha experimentado la garantía de la privacidad en él, teniendo en cuenta las dificultades añadidas a consecuencia de las peculiaridades propias de un sistema originario del *common law* y sus obligaciones codificadoras derivadas de la integración europea, ha servido de ejemplo para elaborar los presupuestos positivos de esta tesis doctoral.

En primer lugar, porque el caso del Reino Unido reafirma el carácter evolutivo, no sólo del ordenamiento jurídico, sino del sistema legal, cuando así lo requieren las circunstancias sociales, políticas e incluso culturales cambiantes, como ocurre en la actualidad con los desafíos que plantea el paradigma del *Big data*.

En segundo lugar, porque su concepción del "*right to privacy*", en tanto que comprende de forma integral las nociones de intimidad y vida privada, se adecúa al concepto de privacidad que se ha tratado de refundamentar en este trabajo, sobre el cual se asienta el derecho al olvido desarrollado en estas páginas, como presupuesto indispensable para garantizar la seguridad jurídica y los derechos fundamentales en la vigente *posmodernidad*.

CAPÍTULO III. EL DESARROLLO DEL DERECHO AL OLVIDO: CONCEPTO Y PRINCIPIOS INSPIRADORES

1. Sobre el derecho al olvido digital como garantía para la protección de la esfera personal del sujeto: presupuestos metodológicos para su desarrollo

Sirva este apartado como consideración preliminar para reforzar la vocación propositiva de esta tesis doctoral. Como se ha expuesto previamente, el desarrollo del derecho al olvido como derecho fundamental supone una exigencia para el Estado social y democrático de Derecho, en tanto que éste debe adecuar sus presupuestos estructurales al cambio de paradigma que representa el *Big data*. En este sentido, se ha expuesto de qué manera el surgimiento de los derechos fundamentales, siendo el derecho al olvido digital representante de dicha categoría, responde a la existencia de conflictos sociales, originados a consecuencia del desarrollo de nuevos paradigmas que reordenan el marco de convivencia en un Estado, siendo la revolución digital una muestra palmaria de esta situación.

De acuerdo con lo expuesto, se ha considerado la necesidad de desarrollar este derecho de nueva generación a partir de una *refundamentación* de la privacidad amparada en dos pilares. En primer lugar, la delimitación del concepto, siguiendo la confrontación entre intimidad y vida privada, que se torna en complementariedad a partir de una comprensión dialéctica de su significado, desarrollando una noción integral de privacidad que pueda adaptarse a los nuevos retos que plantea la protección de la esfera personal del sujeto en el contexto del *Big data*. Seguidamente, esta delimitación conceptual ha venido acompañada de un contenido sustantivo para reforzar la *refundamentación* presentada en estas páginas. Ésta ha venido orientada por la consideración de la privacidad como un estándar de garantía indispensable para la protección del libre desarrollo de la personalidad del sujeto. En este sentido, se ha considerado la privacidad como un estadio previo necesario para asegurar las condiciones materiales imprescindibles para el ejercicio de la libertad por la ciudadanía. Así las cosas, la privacidad se convierte en un estándar que, en el ámbito propio de la "modernidad líquida", siendo difusa la diferenciación del binomio público v. privado, establece una marco

de referencia para la protección de la esfera personal del sujeto en un Estado social y democrático de Derecho.

Partiendo de estos presupuestos, resulta posible el desarrollo del derecho al olvido como derecho fundamental, insertándolo dentro de esta categoría en tanto que las posibles vulneraciones de la privacidad cometidas en el contexto del *Big data* suponen una lesión al libre desarrollo de la personalidad de la ciudadanía, a su propia capacidad para autodeterminarse dentro de su esfera personal de libertad y, en última instancia, a su dignidad personal. Esta necesidad vendría además reclamada por el propio concepto de seguridad jurídica, entendida como regularidad estructural del ordenamiento jurídico, puesto que corresponde al Estado establecer las condiciones objetivas de previsibilidad para que la ciudadanía pueda actuar en el medio social, revestido en la actualidad de una vertiente digital innegable, como muestra del nuevo paradigma acontecido por el *Big data*, sin temor a las intromisiones de terceros.

De acuerdo con lo expuesto, prosiguiendo con los presupuestos metodológicos planteados en la actual disertación, este trabajo culmina con el presente Capítulo, donde se ofrece una categorización del estatus legal del derecho al olvido, partiendo de la *refundamentación* del concepto de privacidad que orienta este trabajo y siguiendo conforme a la estructura clásica de los derechos subjetivos. De este modo, esta tesis doctoral pretende asumir una voluntad propositiva, contribuyendo a la caracterización de este derecho como derecho fundamental, respondiendo así a las demandas sociales que requieren de un mayor despliegue de medios jurídicos para la protección de la esfera personal del sujeto.

2. Origen

2.1. Demanda social como respuesta al *Big data*

Para examinar el origen del derecho al olvido deberíamos remitirnos artículo de WARREN y BRANDEIS que en 1890 escribieron en el *Hardvard Law Review*[544], y que ha sido examinado en el Capítulo anterior con motivo del análisis de la evolución del "*right to*

[544] Cfr. "The Right to Privacy", ob. cit.

privacy" en el *common law*. Dicho artículo, haciendo crítica de las prácticas amarillistas de algunos periódicos de la época, reivindicó la existencia del "*right to be let alone*" -popularizando la expresión acuñada en origen por COOLEY[545]-, quien construyó sobre la base jurídica del derecho a la privacidad[546].

Este texto, escrito hace más de 100 años, revela una preocupación hoy en día de plena actualidad, debido al imparable avance de las tecnologías de la comunicación y la información, la masificación de Internet, la gran dimensión del *Big data* y el uso indiscriminado de los algoritmos, y que no es otra que la necesidad de establecer mecanismos jurídicos capaces de dotar de garantías a los ciudadanos frente a los riesgos o lesiones que puedan sufrir sus derechos fundamentales a manos de la tecnología.

Si bien es cierto que la "*privacy*" anglosajona ha proporcionado una base jurídica para la protección de la libertad individual frente al uso masivo de datos personales, en nuestra tradición jurídica continental encontramos diversos elementos sobre los que hoy puede asentarse -aunque en menor medida- una nueva cultura garantista en base al derecho al olvido digital. Como destaca SIMÓN CASTELLANO, la tradición jurídica civilista contiene principios, derechos y valores que podrían ser interpretados como auténticos fundamentos o pilares del derecho al olvido, entre ellos, el principio de responsabilidad civil por culpa que permite resarcir el daño ilegítimo sufrido, la figura jurídica de la amnistía, la prescripción de oficio de los antecedentes penales, la anonimización o disociación de los datos personales contenidos en las resoluciones judiciales[547]. Igualmente, la prescripción adquisitiva –artículo 1.940 CC- como la extintiva –artículos 1.955 CC y ss- , demuestran que los derechos tienen un tiempo para ejercitarse y que cuando éste se agota, se olvidan las acciones y las antiguas

[545] COOLEY. *A treatise on the Law of Torts*, Callaghan, ob. cit., p. 29.

[546] La reflexión de dicho artículo se ha convertido en célebre por ser perfectamente predicable a día de hoy "*The common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?*". WARREN/BRANDEIS. "The right to privacy", ob. cit., p. 220.

[547] Cfr. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, Barcelona, 2015, pp. 103 ss.

titularidades. Mediante dicha figura se procura adaptar el Derecho al hecho, a la realidad, exigiendo que se olvide lo que durante mucho tiempo no ha encontrado el modo de realizarse.

Así, la incorporación en nuestro ordenamiento jurídico de una regulación acerca de la cancelación de los antecedentes delictivos, refuerza el principio legal por el cual se cree en la capacidad de volver a empezar sin estar condicionado por los errores del pasado, del mismo modo que la anonimización de las sentencias judiciales[548] y otras resoluciones administrativas son medidas que pretenden garantizar al sujeto su derecho a la intimidad, a la reinserción y, en definitiva, al libre desarrollo de su personalidad[549].

Decía ya DÍEZ-PICAZO en el año 1979, cuando aún ni se atisbaba la revolución digital de lo que sería Internet, que la publicación de la biografía de una persona todavía viva exige su consentimiento y por ello, debe exigirlo también cualquier investigación sobre su vida anterior, el apoderamiento de sus datos y el archivo de los mismos[550]. Del mismo modo, es posible encontrar referencias al derecho al olvido hace ya 30 años de la mano de SALVADOR CODERCH[551] que reflexionaba acerca de los límites de la memoria pública colectiva sobre la intromisión a la intimidad, a propósito del comentario de la famosa sentencia *Sidis v. F. R. Publishing Corp*[552].

En cualquier caso, con independencia de que la doctrina discrepe acerca de cual fue el germen del derecho al olvido, como se verá a continuación, lo cierto es que la primera referencia a éste se encuentra en la sentencia del Tribunal de Justicia de la Unión Europea de

[548] Sin embargo, como señala BERROCAL LANZAROT, esta cuestión no es pacífica pues existe gran disparidad de criterios pues, mientras que dicha anonimización alcanza a las resoluciones dictadas por el Tribunal Supremo, la Audiencia Nacional, los Tribunales Superiores de Justicia y las Audiencias Provinciales, ello no se produce respecto de las resoluciones judiciales del Tribunal Constitucional, el Tribunal Europeo de Derechos Humanos ni del Tribunal de Justicia de la Unión Europea. Cfr. *Derecho de supresión de datos o derecho al olvido*, Editorial Reus, Madrid, 2017, p. 204.

[549] MARTÍNEZ OTERO. "El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja" en *Revista de Derecho Político*, nº 93, 2015, p. 112 ss.

[550] DÍEZ-PICAZO. *Derecho y masificación social. Tecnologia y derecho privado (dos esbozos)*, Civitas, Madrid, 1979, p. 114.

[551] SALVADOR CODERCH. *¿Qué es difamar? Libelo contra la Ley del Libelo*, Civitas, Madrid, 1987, p. 98.

[552] U.S. Court of Appeal for the Second Circuit - 113 F. 2d 806 (2d Cir. 1940), 22 de julio de 1940.

13 de mayo de 20014, popularmente conocida como "*caso Google*"[553] -*leading case* en la materia- de igual modo que, no es hasta la promulgación del Reglamento (UE) 2016/679 de protección de datos personales, que se encuentra una formulación expresa del derecho al olvido –formalmente codificado como "derecho de supresión"-.

El carácter gradual de la aparición y formulación en el Derecho de una herramienta jurídica capaz de posibilitar el olvido digital obedece a la demanda de la sociedad de una mayor protección de sus derechos fundamentales frente a los nuevos usos y aparatos electrónicos, siendo la relación entre ambos factores, inversamente proporcional. Como afirma MAYER-SCHÖNBERGER "en un amplio abanico de cambios sociales incentivados por a innovación tecnológica, destaca la conversión de la frágil memoria humana en una potente memoria digital"[554], situación que ha requerido una respuesta por parte del ordenamiento jurídico, y que se ha ofrecido en forma de derecho al olvido.

El siglo XXI se caracteriza por una omnipresencia de las nuevas tecnologías en todos los aspectos de la vida individual y colectiva, constituyendo un enorme cauce de desarrollo de la condición humana en todas sus esferas y provocando, en un periodo de tiempo relativamente corto, el cambio en el modo de comunicarse, del sistema de consumo y hasta en los patrones culturales y las pautas de comportamiento.

Este conjunto de factores, inherentes al desarrollo de la sociedad y aparejado a un gran número de ventajas y efectos positivos, ha tenido una repercusión directa en los derechos humanos cuyo alcance y ejercicio se ha visto perturbado. La proliferación de datos personales que ocasionan las tecnologías del *Big data* así como la memoria virtual y permanente que ha originado Internet, suponen un almacenamiento, procesamiento y transferencia de información personal que, en ocasiones, vulnera el derecho a la privacidad de los sujetos.

Mientras que históricamente la sociedad olvidaba como regla general y sólo recordaba por defecto, hoy la tecnología lleva a la humanidad a la memoria como principio general y al

[553] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

[554] Cfr. *Delete. The Virtue of Forgetting in the Digital Age*, Princeton University Press, New Jersey, 2011, p. 135.

olvido por omisión[555] pues las nuevas tecnologías están diseñadas para recordar eternamente, extendiendo los límites de la memoria humana más allá de la capacidad de las personas, en lo que FROSINI calificó de "juicio universal permanente"[556].

Frente a este nuevo escenario en que las nuevas herramientas tecnológicas han "contaminado libertades" y creado serios riesgos para los derechos fundamentales[557] se ha hecho necesaria una respuesta por parte de la disciplina jurídica capaz de establecer unas garantías de tutela para los ciudadanos ante la eventual agresión tecnológica de sus libertades pues, si bien el Derecho puede en ocasiones estar concebido para orientar el comportamiento de los ciudadanos, en el terreno de los derechos humanos dicho proceso se invierte y es el Derecho el que debe adaptarse a los cambios sociales y modificar el sentido de sus postulados para ponerlos en consonancia con la nuevas realidad jurídica[558]. Así, el legislador contemporáneo afronta el gran reto de constitucionalizar nuevos derechos que satisfagan la demanda social de protección frente a las presentes y futuras amenazas[559].

La disrupción digital ha hecho necesario crear mecanismos jurídicos para combatir las amenazas a la privacidad procedentes de los nuevos fenómenos tecnológicos e informáticos que, en un primer estadio, se vio sustentada por el reconocimiento y desarrollo del derecho a la protección de datos personales. Sin embargo, la expansión de la digitalización masiva de la información así como su almacenamiento han dificultado enormemente un ejercicio óptimo de los derechos de acceso, rectificación, cancelación y oposición, alterando los mecanismos jurídicos de protección hasta dejarlos ineficaces.

Así, en la llamada era "*post-privacy*", el derecho al olvido ha nacido para combatir dicha problemática y permitir a los interesados el cifrado y borrado online de sus datos personales cuando éstos sean perjudiciales para sus derechos fundamentales. De este modo, se refuerza el

[555] RALLO LLOMBARTE. *El derecho al olvido en Internet. Google versus España*, Centro de Estudios Políticos y Constitucionales, Madrid, 2014.

[556] FROSINI. *Cibernética, derecho y sociedad*, Tecnos, Madrid, 1982, p. 178.

[557] Cfr. PÉREZ LUÑO. *Nuevas tecnologías y derechos humanos*, Tirant lo Blanch, València, 2014.

[558] ATIENZA. *El sentido del Derecho*, Ariel, Barcelona, 2003, p. 164.

[559] TRONCOSO REIGADA. *La protección de datos personales en busca del equilibrio*, Tirant lo Blanch, València, 2010.

derecho de toda persona a preservar una esfera libre de injerencias ajenas, con las consecuencias que esta decisión implica sobre la libertad personal de conciencia y el libre desarrollo de la personalidad, así como el derecho a conocer los datos propios que figuren en ficheros de terceros, y el acceso a los archivos dónde se encuentren recogidos sus datos personales, lo que avanza significativamente con el derecho al olvido que añade a todo lo anterior, la posibilidad de que el sujeto interesado mande suprimir toda aquella información digital que afecte a su privacidad.

Las nuevas vías de comunicación y de acceso a la información constituyen hoy en día una forma irrenunciable de libertad por lo que, si bien es cierto que una sociedad democrática exige el libre acceso y circulación de una información plural que ciertamente proporciona Internet, no por ello deben quedar los ciudadanos inermes ante el almacenamiento, tratamiento y difusión de hechos, datos y noticias que pueden afectar directamente a su ámbito más privado.

En definitiva, el derecho al olvido nace por la preocupación creciente de la ciudadanía ante la inmensa capacidad de Internet y las nuevas tecnologías de almacenar información y de hacerla perenne, convirtiendo la vida privada en una parcela universal e indefinidamente accesible para cualquiera, para colmar con ello las expectativas humanas de que se pueda olvidar y empezar de cero[560].

2.2. Desarrollo jurisprudencial de su contenido

El Derecho al olvido, como la mayoría de derechos fundamentales, tiene su origen en la creación jurisprudencial. Ello se debe, principalmente, a que la mayoría de los derechos fundamentales se estructura en los ordenamientos jurídicos con cierta imprecisión, en forma de principios si se quiere, en lo que se ha llamado "textura abierta"[561]. Así pues, el papel de la

[560] DE TERWANGNE. "The Right to be Forgotten and Informational Autonomy in the Digital Environment" en *The ethics of memory in a digital age. Interrogating the right to be forgotten* (Ghezzi/Guimares Pereira eds.), Palgrave Macmillan Memory Studies, UK, 2014, pp. 82 ss.

[561] Esta vaguedad inherente a los preceptos que recogen derechos fundamentales no es casual, sino que obedece a una lógica garantista según la cual, su contenido se maximiza al ser susceptible de un mayor consenso social, ajeno a las discrepancias que pudieran surgir del pluralismo ideológico y, de otro lado, se adapta mejor a la realidad social de cada momento.

jurisprudencia resulta primordial a la hora de definir y concretar el contenido y el alcance de los derechos fundamentales, integrando las lagunas ocasionadas por la generalidad del lenguaje[562].

En la actualidad, los jueces ya no pueden considerarse como meros intérpretes de la ley sino, de acuerdo con ÁLVAREZ GARCÍA "su función ha trascendido la mera subsunción y ha asumido, cada vez más, tareas creadoras"[563] sin descuidar, en ningún caso, su obligación de sumisión a la Ley así como al principio de legalidad y de seguridad jurídica[564]. En esta materia fue pionero indiscutible el Tribunal de Justicia de la UE que, en el *caso Google*[565] que a continuación se analizará, reconoció por vez primera el derecho al olvido digital, íntimamente relacionado con el derecho a la protección de datos personales y en el contexto de la indexación por parte los motores de búsqueda.

Esta correspondencia entre la interpretación-aplicación de la norma ha sido explicada por ZACCARIA como "una relación de dependencia de la ley pero, al mismo tiempo, de necesaria innovación; mejor dicho, de innovación a partir de la dependencia: de innovación porque la relación hermenéutica entre interpretación y aplicación, entre interpretación de los enunciados normativos y de las circunstancias de hecho, abre la ley a significados incesantemente renovados; de dependencia, ya que este hallazgo de nuestros significados normativos evoluciona siempre a partir del punto de observación de la ley"[566].

---

[562] Debe respetarse, en cualquier caso, el núcleo esencial de derecho jurídico protegido, aquél que le dota de efectividad. Este deber vincula asimismo al legislador, que de ningún modo puede desfigurar una institución constitucionalmente garantizada.

[563] Cfr. ÁLVAREZ GARCÍA. *Sobre el principio de legalidad*, Tirant lo Blanch, València, 2009, p. 175.

[564] En caso contrario, existe el riesgo de ruptura entre la función judicial y la función legislativa, de modo que una sentencia extremadamente creativa, dejaría de ser "ley" entre las partes para convertirse en "ley" con efectos generales, con consecuencias indeseables para la seguridad jurídica. Cfr. GARCÍA PASCUAL. *Legitimidad democrática y poder judicial*, Edicions Alfons El Magnànim, València, 1997, p. 159.

[565] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

[566] Cfr. "La libertad del intérprete: creación y vínculo en la praxis jurídica", en *Razón jurídica e interpretación* (Messuti, Ed.), Thomson-Civitas, Navarra, 2004, p. 132.

Ante un clima de cambio social, cultural y económico, el Derecho no puede permanecer estático pues su función es adaptarse a los presupuestos de aplicación para no provocar indefensión a los ciudadanos. La labor jurisprudencial debe pues, en cierta medida, cubrir los espacios de vacío legal no contemplados por el legislador, ya sea por la misma técnica legislativa o por el surgimiento de nuevos condicionantes socioeconómicos, pues ciertamente no parece plausible dejar sin protección intereses colectivos más amenazados. Como señala RODRÍGUEZ MOURULLO, "la jurisprudencia ha de ser concebida como una permanente discusión de problemas […] por lo tanto, su estructura total ha de ser determinada desde el problema, buscando puntos de vista para su solución"[567].

Con los argumentos anteriores no se pretende defender la jurisprudencia como fuente del derecho, pues ello sería contrario a los principios de seguridad jurídica así como de legalidad propios de nuestra cultura legal continental, pero sí legitimar de algún modo, la función creadora del Derecho como potestad inherente a la labor interpretativa de los tribunales, a quienes debe de recocérseles unos márgenes interpretativos que, por una parte, permitan suplir las deficiencias propias de la actividad legislativa y, de otra, adaptar el derecho a la realidad cambiante, posibilitando con ello una mayor garantía de los derechos fundamentales.

a) Análisis del caso Google como leading case:

El llamado *caso Google* –también conocido como *caso Costeja*- tuvo lugar a consecuencia de la Sentencia del Tribunal de Justicia de la Unión Europea dictada el 13 de mayo de 2014[568] la cual, sin duda, supuso un hito en la construcción del derecho al olvido, al constituirse como el *leading case* en la materia, dado que dio lugar al primer pronunciamiento jurisprudencial sobre la cuestión y puso nombre a una nueva garantía jurídica para la protección de los datos personales que estaba aún por determinar.

Puesto que la repercusión de dicha resolución fue de una enorme magnitud y ello ha dado lugar a numerosa literatura y comentarios doctrinales sobre ello, en este apartado se

[567] Cfr. *Aplicación judicial del Derecho y lógica de la argumentación jurídica*, Civitas, Madrid, 1988, p. 45.

[568] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

procederá a describir brevemente los hechos que ocasionaron dicha sentencia así como los pronunciamientos jurisprudenciales más relevantes para que, sin incurrir en una extensión innecesaria, permita al lector ponerse en situación y comprobar el trazado progresivo que ha llevado a cabo el derecho al olvido[569].

Dicha sentencia resuelve el litigio existente entre *Google Spain S. L*. (en adelante, *Google Spain*) y *Google Inc*. frente a un ciudadano español (Sr. Costeja) y la Agencia Española de Protección de Datos después de que esta última resolviese favorablemente la reclamación formulada por el demandante contra las compañías anteriores y la empresa La Vanguardia Ediciones S. L. La reclamación vino motivada porque el demandante, como se publicó en el periódico La Vanguardia el año 1998, fue condenado por impagos y, en 2009, transcurridos más de diez años y con la situación económica subsanada, dicha información seguía disponible en la versión digital de dicho periódico y era accesible con la mera introducción en el buscador *Google* de los nombres y apellidos del demandante, mostrándose la noticia del impago entre los primeros resultados, perjudicando ello a la tarea profesional del demandante, el cual entendía que ello constituía una información inexacta puesto que dicho embargo carecía ahora de virtualidad al estar resuelto y al no mantener el demandado ninguna relación en la actualidad ni con las deudas ni con las empresas embargadas.

Contra dicha pretensión, la AEPD resolvió estimar la reclamación formulada por el demandado[570], instando a *Google Spain* y a *Google Inc*. a adoptar las medidas necesarias para retirar los datos de su índice e imposibilitar así el acceso a los mismos. Frente a lo cual, los representantes tanto de *Google Spain* como de *Google Inc*. interpusieron un recurso contencioso-administrativo, solicitando ante la Audiencia Nacional (AN, en adelante) que se estimase éste y se declarase nula la resolución dictada esgrimiendo principalmente tres

[569] Para un examen en profundidad de la materia, RALLO LLOMBARTE. *El derecho al olvido en Internet. Google versus España*, ob. cit.

[570] Resolución nº R/01680/2010 de la AEPD, de 30 de junio de 2010.

argumentos: falta de legitimidad pasiva, inexistencia de tratamiento de datos personales e imposibilidad técnica de cumplir con dicho requerimiento[571].

Por su parte, la AN dada la complejidad del caso, estimó oportuno elevar una cuestión prejudicial al Tribunal de Justicia de la Unión Europea (TJUE en adelante)[572] al amparo del artículo 267 del Tratado de Funcionamiento de la Unión Europea, frente al cual se formularon las siguientes cuestiones:

> ***1.*** *Por lo que respecta a la aplicación territorial de la Directiva 95/46/CE y,*
>
> *consiguientemente de la normativa española de protección de datos:*
>
> *1.1 "¿Debe interpretarse que existe un "establecimiento", en los términos descritos en el art. 4.1.a) de la Directiva 95/46/CE , cuando concurra 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*

[571] En primer lugar, *Google Spain* entendía que la legitimidad procesal le correspondía a *Google Inc*., con domicilio social en Estados Unidos, por ser ésta la que prestaba efectivamente el servicio de búsqueda en Internet, alegando que *Google Spain* se limitaba a la venta de espacios publicitarios en Internet, manifestando pues que, tanto la AEPD como la AN, carecían de competencia territorial. En segundo lugar, negaba estar llevando a cabo ningún tratamiento de datos, alegando que su actividad era "neutral" en tanto que sólo aglutinaba en su buscador enlaces acerca de lo que otras páginas web publicaban, sin ninguna responsabilidad sobre su contenido. Argumentaba, además, que se estaba vulnerando su derecho a la libertad de expresión e información así como de empresa. Por último, *Google Spain* refutaba disponer de los medios técnicos necesarios para ejercitar la supresión solicitada.

[572] Por Auto de la AN, Sala de lo Contencioso-Administrativo, de 27 de febrero de 2012.

respeto al derecho de protección de datos, aun cuando dicha colaboración se realice de forma voluntaria?

1.2 ¿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?

1.3 ¿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?

1.4. 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?"

***2.** Por lo que respecta a la actividad de los buscadores como proveedor de contenidos en relación con la Directiva 95/46/CE de Protección de Datos:*

2.1. "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 ?

2.2. 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?.

2.3. 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 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?.

2.4. 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?".

***3.** Respecto al alcance del derecho de cancelación y/oposición en relación con el derecho al olvido se plantea la siguiente pregunta:*

3.1. "¿Debe interpretarse que los derechos de supresión 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 perjudicarle o desea que sea olvidada, aunque se trate de una información publicada lícitamente por terceros?".

Dejando a un lado las conclusiones del Abogado General, dignas de un examen más pormenorizado que, por razones de extensión, no puede llevarse a cabo en esta disertación[573], a consecuencia de las preguntas realizadas por la AN, en su Sentencia de 13 de mayo de 2014, el TJUE resolvió dichas cuestiones afirmando, a rasgos generales y sin entrar a reproducir dicho pronunciamiento jurisprudencial, la existencia de un derecho al borrado de nuestra información en Internet: "*para respetar los derechos que establecen estas disposiciones, siempre que se cumplan realmente los requisitos establecidos en ellos, el gestor de un motor de búsqueda está obligado a eliminar de la lista de resultados obtenida tras una búsqueda efectuada a partir del nombre de una persona vínculos a páginas web, publicadas por terceros y que contienen información relativa a esta persona, 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*" (FJ 3º).

Así las cosas, el TJUE afirmó rotundamente que el tratamiento de datos personales por los buscadores en Internet puede afectar a los derechos fundamentales de las personas relativos al respeto de la vida familiar y la protección de los datos personales, de forma significativa, cuando la búsqueda se lleva a cabo a partir del nombre de una persona física, pues ello permite al internauta hacerse una configuración apriorística de una persona en base a la lista de resultados ofrecidos (puntos 38-40 y 80). Por ello, debe entenderse esta sentencia como una declaración del principio general de prevalencia del derecho a la protección de datos de carácter personal, sobre cualquier aspecto o limitación tecnológica, pues toda implementación de herramientas o dispositivos tecnológicos habrá de permitir siempre el ejercicio de este derecho fundamental en sus distintas manifestaciones[574].

El Tribunal de Luxemburgo, hacía hincapié en el alto nivel de protección otorgado al derecho de protección de datos por la Directiva 95/46/CE, el artículo 8 CEDH y los principios

[573] Para un análisis detallado de las conclusiones del Abogado General, el Sr. Niilo Jäaskinen, SIMÓN CASTELLANO. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, Barcelona, 2015.

[574] PLAZA PENADÉS. "Doctrina del Tribunal de Justicia de la Unión Europea sobre protección de datos y derecho al olvido" en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 35, 2014, p. 18.

generales de Derecho comunitario, al cual otorga un alcance constitucional derivado del contenido de los artículos 7 y 8 CDFUE que reconocen, respectivamente, el derecho a la vida privada y a la protección de datos personales. Así pues, uno de los aspectos más destacables de dicha resolución, como afirma RALLO LLOMBARTE es que "el TJUE no limita su interpretación a un mero juicio de legalidad comunitaria enjuiciando la vigencia de la Directiva sino que recurre al marco constitucional europeo preservando el valor jurídico de la CDFUE y garantizando la vigencia del derecho a la protección de datos en ella consagrado"[575].

Dado que en el caso en cuestión la información ofrecida por el buscador era lícita y veraz, el Tribunal estimó que, incluso en estos casos, ésta puede resultar desproporcionada y, en consecuencia, provocar una intromisión ilegítima en los derechos del afectado. Así, dispuso que un tratamiento de datos puede devenir incompatible con el Derecho, no sólo cuando los datos sean inexactos sino también cuando éstos sean "*inadecuados, no pertinentes o excesivos*" en relación con los fines del tratamiento, o cuando no estén actualizados o se conserven por un tiempo superior al necesario (punto 92). Es decir, incluso tratándose de datos o informaciones exactas, verídicas o lícitas, podría considerarse su uso como inadecuado lo que obligaría al motor de búsqueda a eliminar de los resultados tal información puesto que el tratamiento de datos debe ser legítimo durante todo el periodo en que se lleve a cabo (punto 94).

En cuanto a la responsabilidad en el tratamiento de este tipo de datos, el pronunciamiento del TJUE entraña también novedades dado que extendió a los gestores de los buscadores de Internet dicha responsabilidad, incluso cuando no estén domiciliados en España pero realicen su actividad por medio de un establecimiento permanente sito en ella -como lo es una filial que se dedica a llevar a cabo actividades comerciales y publicitarias para con la primera[576]- por lo que, se permitiría a los particulares dirigirse directamente ante los buscadores en Internet para ejercer los derechos de rectificación y oposición de sus datos (punto 60, FJ 2º).

[575] Cfr. "De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018)", ob. cit., p. 598.

[576] Resolvió así la STJUE que la filial para venta publicitaria de Google en España (*Google Spain*) era un establecimiento que llevaba a cabo tratamiento de datos, pues su actividad estaba indisociablemente ligada a la de su filial en Estados Unidos *Google Inc*. (puntos 55 y 60), rechazando la argumentación del motor de búsqueda en dicho sentido.

De esta forma el Tribunal por una parte, se avanzó a lo dispuesto posteriormente por el GDPR en cuanto a la aplicación territorial de la normativa europea, sometiendo a la legislación, no sólo a los actores europeos, sino también a todos aquellos que desempeñen su actividad en su territorio y, por otra parte, extiendiendo la aplicación de la normativa de protección de datos a los motores de búsqueda en tanto que almacenan, indexan y ponen a disposición del público información publicada por terceras personas.

La relevancia jurisprudencial de esta resolución debe entenderse desde una óptica garantista y la necesidad de hacer evolucionar el Derecho al mismo compás que la sociedad. En un momento en que la desconexión tecnológica parece ya imposible, deben darse respuestas jurídicas a los problemas que ocasionan las nuevas herramientas tecnológicas respecto de los derechos y las libertades de sobra consolidados.

La jurisprudencia del TJUE constituye una referencia precisa sobre los enormes riesgos potenciales para la privacidad del individuo que derivan tanto del uso de servicios y dispositivos tecnológicos (telefonía móvil, Internet y redes sociales) en los que se almacena abundante información personal sin que el principio de territorialidad estatal pueda satisfacer las garantías necesarias para evitar la lesión en la vida privada. Por ello, la fuerza expansiva extraterritorial de los pronunciamientos del TJUE ha sido un factor clave a la hora de proteger los derechos de los ciudadanos europeos más allá de las fronteras de la Unión, como se ha podido observar en diversas resoluciones[577].

Puede afirmarse así que, a partir de una ley –principalmente la Directiva 95/46/CE-, y dentro de las limitaciones establecidas en su propio marco legal –el derecho a la protección de datos personales-, así como del principio de legalidad, no hay obstáculo para que los tribunales, en su labor jurisprudencial y dentro de los límites de la hermenéutica jurídica, lleven a cabo cierta autoría en el desarrollo legal –la gestación del derecho al olvido, en este caso-. Ciertamente, "el derecho no es, en ningún caso, algo completamente dado, ni tampoco algo completamente creado de la nada: encuentra continuas articulaciones y re-determinaciones tras

[577] Cfr. RALLO LLOMBARTE. "De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018)", ob. cit., p. 664.

procesos sucesivos de concretización dictados por la razón práctica que consisten en aplicar y utilizar el derecho en los distintos casos de la vida que se presentan"[578].

Esta sentencia comportó, en cierto modo, un cambio de paradigma para la seguridad de los usuarios en relación con el empleo de datos personales por parte de los buscadores web. Sin ir más lejos, se reconoció el derecho al olvido por vez primera, sentándose las bases para su reconocimiento expreso en la normativa europea de protección de datos, que se consagraría tiempo después en el artículo 17 del GDPR, bajo la denominación "derecho de supresión". Aunque, francamente, no sería justo considerar dicho pronunciamiento jurisprudencial como impecable pues, ciertamente, no está exento de críticas, fallos e imperfecciones que, principalmente versan sobre una concepción incompleta o distorsionada del funcionamiento mismo de Internet[579].

Frente a dicha sentencia fueron muchas las voces doctrinales que estimaron un exceso garantista en el pronunciamiento y presagiaron un futuro negativo para la Sociedad de la Información, reivindicando la necesidad de imponer límites[580]. Sin embargo, con el paso del tiempo se ha podido observar como dicho pronunciamiento judicial no ha ocasionado un cambio en la lógica empresarial de los motores de búsqueda -ni siquiera se ha visto mermada su actividad económica-, sino que simplemente se les ha obligado a adoptar las medidas mínimas exigibles para el cumplimiento efectivo de los derechos de los ciudadanos, lo que principalmente han llevado a cabo habilitando unos formularios online para el ejercicio del derecho de supresión, mientras que continúan haciendo de los datos personales de sus usuarios un negocio privado. En efecto, no se les ha impuesto el establecimiento de filtros ni la interposición de mecanismos de control previo, sus obligaciones se reducen a la contestación

[578] Cfr. ZACCARIA. "La libertad del intérprete: creación y vínculo en la praxis jurídica", ob. cit., p. 80.

[579] Por ejemplo, no parece lógico exonerar de toda responsabilidad al editor de la página web fuente en dicho supuesto sin aplicar ningún protocolo de exclusión, mientras se le atribuye todo el peso al motor de búsqueda que sólo recoge el contenido de dicha web y lo pone a disposición de sus usuarios. La información acerca del embargo sigue a disposición de cualquiera en la fuente original así como los datos personales del interesado, cuando ha quedado acreditado la falta de interés legítimo en la conservación y difusión de dicha información y los perjuicios que ocasiona al afectado.

[580] Por todos, SIMÓN CASTELLANO. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, ob. cit.

de las peticiones de los usuarios, de forma individualizada (examinando el supuesto en concreto y sólo respecto de las URL denunciadas por el interesado así como del uso concreto de los términos efectuados para la búsqueda), quedando las autoridades de control y los Tribunales como garantes en caso de negarse dicha desindexación o de producirse conflicto entre intereses.

A modo de conclusión, la sentencia del *caso Google* articula por vez primera lo que se venía defendiendo desde hacía mucho tiempo por la doctrina: la protección de los derechos fundamentales no puede quedar supeditada a las restricciones tecnológicas. Y es por ello que puede afirmarse que el TJUE se ha convertido en un auténtico juez garante de la privacidad ante la evolución tecnológica global como se ha podido observar en muchas de sus resoluciones como el *Caso Digital Rights* en relación con la Directiva de conservación de datos, el *Caso Facebook*, respecto del *Safe Harbour* o, como se acaba de comentar, el *Caso Google*, para el derecho al olvido[581].

b) El papel de la jurisprudencia española en la configuración legal del derecho al olvido

En nuestro sistema jurídico, durante los últimos años han abundado los pronunciamientos en torno al derecho al olvido, encontramos algunas sentencias tanto del Tribunal Supremo como de la Audiencia Nacional, así como por parte de las Audiencias Provinciales, y, más recientemente, del propio Tribunal Constitucional que, como también se verá a continuación, ha considerado el derecho al olvido como un derecho fundamental más[582]. Sin embargo, muchas de estas resoluciones tratan cuestiones accesorias o no aportan demasiado al debate por lo que, para no ampliar innecesariamente la extensión del presente trabajo ni incidir en reiteraciones, a continuación se limitará a comentar algunas de las sentencias más relevantes en la materia, siendo conscientes de que se prescinde de muchas de ellas.

[581] ARENAS RAMIRO. "El derecho a la protección de datos personales en la jurisprudencia del TJCE", en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, Vol. 4, 2006, p. 97.

[582] STC 58/2018, de 4 de junio.

i. Audiencias Provinciales

La primera sentencia dictada por los órganos jurisdiccionales españoles que reconoce la existencia de un derecho al olvido digital es la sentencia de 11 de octubre de 2013 de la Audiencia Provincial de Barcelona[583], dictada a raíz de la demanda interpuesta como consecuencia de la difusión de unos antecedentes penales cancelados, que concluye "*debemos de partir tanto del derecho al olvido, que como hemos dicho la jurisprudencia de varios países lo ha reconocido, basándose en el derecho a la privacidad o como parte de los derechos de la personalidad. Una vez pagado lo debido, la sociedad debe ofrecerle la posibilidad de rehabilitarse e iniciar una nueva vida sin tener que soportar el peso de sus errores del pasado el resto de su vida*" (FJ 5º).

Dicha resolución, que incorpora el elemento de la privacidad en consonancia con la significación que se viene defiendo a lo largo de la presente disertación, entremezcla asimismo, pronunciamientos relativos a la protección de datos personales así como sobre el derecho al honor, reputación, intimidad y libre desarrollo de la personalidad, reconociendo un derecho al olvido digital a favor del titular de los datos personales al entender la Audiencia que la publicación de sus datos personales, plenamente identificables, eran innecesarios para la difusión de dicha noticia en cuestión.

Igualmente, en el caso concreto, se vincula el derecho al olvido con el derecho a la intimidad, pues se entiende que esta última resulta menoscabada como resultado de dicho tratamiento de datos, "*No se trata de modificar la noticia impresa ni la hemeroteca escrita, sino de que, en lo que ha sido el iter del proceso, en la transposición en la página web resultaba del todo innecesario en noticia de 27 de febrero de 1985 reiterar los nombres y apellidos de las actoras, en su derecho al honor, intimidad personal y familiar, prestigio profesional, y protección de datos que por el tiempo ya no son vigentes*" (FJ 8º).

Esta primera resolución, cuya importancia resulta vital a la hora de establecer los cimientos de lo que luego ha sido una jurisprudencia consolidada en materia del derecho al

[583] SAP Barcelona 486/2013, de 11 de octubre, Sección 14.

olvido fue, sin embargo recurrida, como más tarde se examinará, primero ante el Tribunal Supremo que estimó en 2015 parcialmente el recurso presentado y, finalmente, en amparo ante el Tribunal Constitucional, que el 4 de junio de 2018 dictó su primera resolución relativa al derecho al olvido.

La segunda sentencia que reconoce el derecho al olvido en nuestra jurisdicción se dictó asimismo por idéntico órgano -aunque diferente Sección- el 17 de julio de 2014[584], la cual versaba sobre la solicitud de interrupción del tratamiento de datos personales llevada a cabo por parte de un motor de búsqueda web.

En dicho caso, se reconoció formalmente el derecho al olvido digital sobre la base de los derechos de cancelación y oposición del sujeto, inherentes a su derecho a la protección de datos personales. Y lo hizo teniendo presente el reciente fallo del TJUE en el *caso Google*, por lo que, a su imagen y semejanza considera al motor de búsqueda demandado sujeto responsable de un incorrecto tratamiento de datos personales "*esta actividad de los motores de búsqueda desempeña un papel decisivo en la difusión global de dichos datos en la medida en que facilita su acceso a todo internauta que lleva a cabo una búsqueda a partir del nombre del interesado, incluidos los internautas que, de no ser así, no habrían encontrado la página web en la que se publican estos mismos datos*" (FJ 13º).

Así, el tribunal reconoce que el motor de búsqueda demandado incurrió en una vulneración del derecho al olvido, pese a señalar la existencia de otros derechos fundamentales relacionados: el derecho al honor y el derecho a la intimidad, "*en cuanto al derecho al honor, la información de que una persona fue condenada por cometer un delito contra la salud pública -obtenida aquí a partir de la información sobre el indulto de la pena impuesta por el delito-, puede afectar, sin duda, objetivamente, a la buena reputación de la persona y hacerle desmerecer en la consideración ajena, al ir en su descrédito o menosprecio* […] *También puede hallarse afectado en el caso el derecho fundamental a la intimidad, aunque la*

[584] SAP Barcelona 364/2014, de 17 de julio, Sección 16.

información sobre la que se reclama reserva no sea propiamente de aspectos de la esfera íntima del actor"(FJ 5º).

Y, en consecuencia, insta al responsable del tratamiento a eliminar de la lista de resultados la información relativa a los antecedentes penales del interesado, por ser éstos, datos especialmente sensibles que carecen de relevancia, dado el transcurso de tiempo producido, incluso cuando dichos datos no se eliminen de la webmaster (FJ 21º).

ii. Audiencia Nacional

Como se ha visto anteriormente, la Audiencia Nacional también se ha pronunciado sobre el derecho al olvido, de hecho, al elevar al TJUE las cuestiones prejudiciales previamente comentadas, dio lugar a la famosa STJUE del *Caso Google*. En el marco de dicho procedimiento conviene comentar, y concluir con ello la narrativa de dicho pronunciamiento, que en la sentencia dictada a raíz de dicho procedimiento[585], la AN estableció que *Google Spain* es el responsable del tratamiento de los datos de sus usuarios en España por estar estrechamente ligada su función publicitaria y de soporte con el tratamiento de datos efectuados por su filial *Google Inc*., de la cual *Google Spain* es representante legal en España y, por ende, le resulta de aplicación la normativa española de protección de datos.

La sentencia, siguiendo el pronunciamiento de la STJUE, concluyó que los buscadores de internet efectúan un tratamiento de datos de carácter personal por lo que están obligados a hacer efectivo el derecho de cancelación del interesado que se opone a que se indexe y sea puesta a disposición de los internautas determinada información a él referida, pese a que se encuentre en páginas de un tercero, cuando ello permita relacionarlo con la misma. Señala además, que los datos personales obtenidos por el buscador pueden afectar a la dignidad de las personas y lesionar derechos de un tercero, por lo que aquél se convierte en responsable del tratamiento de los datos y a él le corresponde, en su caso, adoptar las correspondientes medidas en aplicación de la LOPD para hacer efectivo el derecho de supresión requerido por el afectado (FJ 6º).

[585] SAN 5129/2014, de 29 de diciembre.

En cuanto a la legitimación pasiva, la AN desestimó dicho motivo de impugnación al considerar que *Google Spain* tiene la legitimación pasiva necesaria para responder de sus actos ante el tribunal español "Se *reconoce la legitimidad pasiva a Google Spain, S.L. ya que su actividad de gestión publicitaria está unida de forma indisociable a la del buscador de nacionalidad americana. Por otro lado, la presencia de esta entidad en España permite la aplicación de la legislación europea, y por ende, de la legislación española de protección de datos*" (FJ 5º).

Respecto de la alegación de *Google Spain* referida a que la resolución de la AEPD tiene un objetivo imposible de cumplir –eliminación del índice de resultados proporcionado por el buscador de determinados enlaces-, señala la AN "*la unidad material y funcional que conforma con Google Inc. conlleva su responsabilidad en el cumplimiento de la obligación, trasladándola al gestor del motor de búsqueda y contribuyendo a su realización, dada la relevancia de su participación en el funcionamiento del servicio de búsqueda en Internet que se ofrece a los internautas. De hecho, así se ha venido a reconocer, en el caso que nos ocupa, por Google Spain, S.L. que ha procedido al bloqueo provisional de resultados de la consulta a nombre del reclamante. En consecuencia, procede desestimar este motivo de impugnación, así como la alegación consistente en que la resolución recurrida tiene un contenido de imposible cumplimiento*" (FJ 10º).

Por último, en cuanto a la alegación de vulneración de la libertad de empresa, señala la AN que, siguiendo la interpretación del Tribunal Constitucional en esta materia, la libertad de empresa nunca puede lesionar derechos fundamentales, sino que se encuentra sujeta a límites. Así, "*el derecho a la libertad de empresa no puede justificar una violación del derecho a la protección de datos (regulado en la Sección Primera del Capitulo 2º de la Constitución) cuando resulta que el derecho a la libertad de empresa se contempla en la Sección Segunda y no goza de la misma protección reforzada que menciona el articulo 53.2 de la Constitución*" (FJ 11º).

La relevancia de esta sentencia de 29 de diciembre de 2014, no estriba en ser la primera en pronunciarse sobre el derecho al olvido –encontramos un precedente en la SAN 5236/2014,

de 2 de diciembre[586]- sino en incorporar por primera vez la doctrina del TJUE en el *caso Google* en nuestra jurisdicción. Después de dicha resolución, la Audiencia Nacional hizo públicas las primeras dieciocho sentencias relativas al derecho al olvido, que resolvían los recursos contencioso-administrativos interpuestos por *Google Spain* contra las resoluciones estimatorias de la AEPD y cuyo fallo, en base a la doctrina de la STJUE del *caso Google*, fue estimatorio en catorce de dichos casos[587].

Otras muchas sentencias de la Audiencia Nacional han venido a consolidar la doctrina del derecho al olvido digital a nivel nacional: SAN 2562/2017, de 19 de junio[588], SAN 3257/2017, de 13 de julio[589], SAN 3029/2017, de 18 de julio[590], SAN 3260/2017, de 25 de julio[591], etc. Esta última, resuelve un recurso contencioso-administrativo interpuesto por Google contra la RAEPD de 6 de noviembre de 2015, que desestima el recurso de reposición interpuesto por la misma parte contra la RAEPD de 12 de febrero del mismo año, donde la AEPD estimó la reclamación formulada por la interesada contra *Google Inc*. e instó a dicho buscador a que adoptase las medidas necesarias para evitar que el nombre de la afectada quedase vinculado en la lista de resultados de un enlace a una noticia de un periódico digital en la que la afectada se asociaba a una lista de participantes de una manifestación del movimiento 15-M así como a otras URL que exponían aspectos personales de su vida académica y profesional.

Una peculiaridad de dicha sentencia judicial se encuentra en el hecho de que, pese a dictarse en el orden jurisdiccional contencioso administrativo, la Audiencia lleva a cabo un examen hermenéutico acerca de los bienes jurídicos en conflicto, centrado principalmente en los llamados derecho de la personalidad, materia que se aborda habitualmente en la jurisdicción

[586] Nº recurso 363/2010.

[587] Un examen más detallado de los pronunciamientos jurisdiccionales de dichas resoluciones lo encontramos en DI PIZZO CHIACCHIO. *La expansion del derecho al olvido digital. Efectos de "Google Spain" y el Big Data e implicaciones del nuevo Reglamento Europeo de Protección de Datos*, ob. cit., pp. 171 ss.

[588] Nº recurso 1842/2015.

[589] Nº recurso 4/2016.

[590] Nº recurso 1568/2015.

[591] Nº recurso 114/2016.

civil, y claro está, en la doctrina constitucional. Así, siguiendo los criterios del TJUE para llevar a cabo la ponderación entre bienes jurídicos en colisión, la AN concede cierta preeminencia al derecho al olvido de la demandante teniendo en cuenta los siguientes parámetros: la falta de interés general de la información[592], la naturaleza privada de la recurrente[593] y el transcurso de un tiempo prudencial – 3 años- desde los acontecimientos[594](FJ 5º).

Mediante dicha resolución pues, se reitera que el derecho a la protección de datos personales tiene un objeto mucho más amplio que el derecho a la intimidad, al extender su garantía a la esfera de los derechos de la persona que pertenecen al ámbito de la vida privada, más allá del núcleo constitucional reservado para la intimidad, incluyendo así a cualquier tipo de dato personal ya sea éste íntimo o no, lo cual está directamente relacionado con el planteamiento que se viene defendiendo a lo largo de la tesis doctoral acerca de la configuración del derecho de privacidad como base ideal para el ejercicio del derecho al olvido.

iii. Tribunal Supremo

El primer pronunciamiento del Tribunal Supremo sobre el derecho al olvido, se llevó a cabo mediante la STS 545/2015, de 15 de octubre, dictada por la Sala de lo Civil contrariamente a lo que se pudiera pensar pues, mediante dicha resolución, se pone fin a una reclamación llevada a cabo inicialmente ante la AEPD, esto es la vía administrativa, para el borrado de determinados datos personales contenidos en una hemeroteca digital.

---

[592] "*A efectos de la ponderación de derechos e intereses hay que examinar si la afectada es portavoz o líder de un movimiento o de una manifestación de apoyo a dicho movimiento, como alega la recurrente, lo que dotaría relevancia a la información desde el punto de vista subjetivo*".

[593] "*Tampoco se trata de una persona de relevancia pública, ni siquiera en el ámbito del apoyo al movimiento 15M o a "Indignez-vous-Genève", sin que se haya aportado por la actora ninguna otra noticia sobre la participación de dicha Sra. en apoyo a dichos movimientos, ni la manifestación convocada en mayo de 2011 parece tener especial trascendencia dentro del conjunto de movimientos y actuaciones que se engloban o apoyan el 15M*".

[594] "*En cuanto al factor tiempo, debe tenerse en cuenta que han pasado más de tres años desde la publicación de la noticia hasta que se ejerció el derecho de oposición/cancelación, lo que puede considerarse un plazo razonable en el presente caso, teniendo en cuenta que no se trata, como se acaba de señalar, de un portavoz o líder, ni de una figura de relevancia pública, ni de una manifestación que tuviera especial trascendencia*".

Una vez agotada la vía ante la AEPD, y en lugar de interponer recurso ante la Audiencia Nacional, se interpusieron dos demandas (acumuladas posteriormente en el mismo procedimiento) ante la jurisdicción ordinaria que, finalmente dieron lugar a dicha resolución del Tribunal Supremo.

Esta primera sentencia, reafirma la estrecha vinculación existente entre los datos personales de una persona y su derecho al honor y a la intimidad y, en relación a ello, afirma la existencia de un derecho al olvido "*el llamado "derecho al olvido digital", que es una concreción en este campo de los derechos derivados de los requisitos de calidad del tratamiento de datos personales* […] *dicho derecho sí ampara que el afectado, cuando no tenga la consideración de personaje público, pueda oponerse al tratamiento de sus datos personales que permita que una simple consulta en un buscador generalista de Internet, utilizando como palabras clave sus datos personales tales como el nombre y apellidos, haga permanentemente presentes y de conocimiento general informaciones gravemente dañosas para su honor o su intimidad sobre hechos ocurridos mucho tiempo atrás*" (FJ 8º).

A tal efecto, lleva a cabo un ejercicio de ponderación entre el derecho al olvido y las libertades informativas, teniendo para ello especial consideración el tiempo trascurrido desde la publicación de los datos "*El factor tiempo tiene una importancia fundamental en esta cuestión, puesto que el tratamiento de los datos personales debe cumplir con los principios de calidad de datos no solo en el momento en que son recogidos e inicialmente tratados, sino durante todo el tiempo que se produce ese tratamiento. Un tratamiento que inicialmente pudo ser adecuado a la finalidad que lo justificaba puede devenir con el transcurso del tiempo inadecuado para esa finalidad*" (FJ 4º).

Sin embargo, aclara lo que un sector doctrinal venía denunciando tras el surgimiento del derecho al olvido con la STJUE de 13 de mayo de 2014, y es que dicho derecho "*no ampara que cada uno construya un pasado a su medida* […] *Tampoco justifica que aquellos que se exponen a sí mismos públicamente puedan exigir que se construya un currículo a su gusto, controlando el discurso sobre sí mismos, eliminando de Internet las informaciones negativas,*

"posicionando" a su antojo los resultados de las búsquedas en Internet, de modo que los más favorables ocupen las primeras posiciones" (FJ 8º).

La importancia de esta resolución no sólo reside en el reconocimiento expreso de un derecho la olvido, sino en que, a raíz de ello, el Tribunal Supremo se pronuncia acerca de la inalterabilidad de las hemerotecas como límite al derecho al olvido, operante fundamentalmente en dos aspectos. En primer lugar, estimó el Alto Tribunal que los medios de comunicación no deben de suprimir de sus hemerotecas digitales los nombres y apellidos que aparezcan en una noticia pues defiende que las hemerotecas y la integridad de los archivos digitales gozan de la protección de la libertad de información, sin que pueda alterarse su contenido borrando datos, ni siquiera sustituyendo los nombres por sus iniciales. A tal efecto, señaló: "*El llamado "derecho al olvido digital" no puede suponer una censura retrospectiva de las informaciones correctamente publicadas en su día. 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*" (FJ 3º).

En segundo lugar, consideró adecuado que los medios de comunicación no deban desindexar una información de sus buscadores internos, cuando se efectúe una búsqueda introduciendo el nombre y los apellidos de una persona, "*Tampoco puede admitirse la condena consistente en la adopción de medidas técnicas que impidan la indexación de los datos personales a efectos de su consulta por el motor de búsqueda interna de la web. Estos motores de búsqueda internos de las hemerotecas digitales solo sirven para localizar la información contenida en el propio sitio web una vez que el usuario ha accedido a dicho sitio web. No son por tanto asimilables a los motores de búsqueda de Internet tales como Google, Yahoo, Bing, etc. La Sala considera que una medida como la acordada en la sentencia supone un sacrificio desproporcionado de la libertad de información protegida en el art. 20.1.d de la Constitución*" (FJ 4º).

Esta sentencia, que ha servido mucho tiempo como directriz para delimitar el derecho al olvido así como sus posibilidades de ejercicio, ha visto recientemente derogada su doctrina –y

con ella la del Tribunal Supremo- acerca de los límites del derecho al olvido en relación con la actuación de las hemerotecas digitales, por parte del Tribunal Constitucional, como a continuación se examinará.

Después de esta resolución, el Alto Tribunal dictó muchas otras, en su mayoría reproduciendo tanto su doctrina anterior como la del TJUE en torno al derecho al olvido y a sus límites, pudiendo destacarse entre ellas, algunos pronunciamientos novedosos que ayudaron a configurar la figura del derecho al olvido, aún incipiente. Entre ellas, la STS 574/2016, de 14 de marzo, que supuso un cambio de pronunciamiento respecto de la jurisprudencia del TJUE en torno a la responsabilidad de los motores de búsqueda cuando éstos tienen su domicilio social en un tercer país, mientras que llevan a cabo un tratamiento de datos personales en un país de la Unión Europea –importante a afectos de quedar sometido a la legislación europea de datos personales- mediante una empresa filial.

Mediante dicha resolución, la primera en esta materia formulada por la Sala Tercera, se resuelve el recurso de casación interpuesto por *Google Spain* contra la SAN 5129/2014, de 29 de diciembre, analizada páginas atrás, que desestimó el recurso de contencioso-administrativo formulado por el mismo recurrente frente a una resolución de la AEPD que estimaba la petición de cancelación de los datos personales de un particular contenidos en un blog así como los vínculos obtenidos a partir de la búsqueda de su nombre y apellidos en *Google Search*.

Señala la Sala que, pese a que se da una unidad material entre la empresa madre situada en EEUU con su empresa filial, que presta servicios en España, no se puede exigir a ambas igual responsabilidad al tener funciones sensiblemente distintas, "*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. No obstante, ello no implica que Google Inc. sea responsable del tratamiento en solitario* […] *Carecería de lógica alguna excluir a Google Spain, S.L. de cualquier responsabilidad en el tratamiento de los datos personales que lleva a cabo Google Inc., tras afirmar que este tratamiento se sujeta al Derecho Comunitario precisamente por haberse llevado a cabo en el marco de las actividades de su establecimiento en España, del que es*

titular Google Spain, S.L., y más aún tras aceptar la relevancia de su participación en la actividad conjuntamente desempeñada por ambas, en relación con el funcionamiento del motor de búsqueda y el servicio que mediante el mismo se presta a los internautas, que conlleva el tratamiento de datos personales que nos ocupa" (FJ 5º).

Pese a la unidad existente entre ambas empresas, niega el TS que exista corresponsabilidad en el presente caso, "*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*" (FJ 8º). Además, señala la sentencia que, pese a que pudiera apreciarse corresponsabilidad entre ambas, ello no supondría automáticamente una solidaridad en el cumplimiento de las obligaciones pues una de ellas es responsable de las actividades que lleva a cabo, lo que implica una doble consecuencia "*primera, la necesidad de precisar el alcance de la participación en el tratamiento de cada corresponsable, para identificar el alcance de sus obligaciones ; y segunda, que la exigencia de su cumplimiento ha de efectuarse por el interesado a quien resulte responsable en cada caso*" (FJ 9º), no pudiendo dirigirse el interesado indistintamente contra a cualquiera de ellos.

Así pues, el debate procesal llevado a cabo por la resolución, supone un elemento esencial a afectos de determinar la legitimación pasiva de dicha entidad en el procedimiento administrativo, por lo que el cambio jurisprudencial del TS, altamente cuestionable y contrario a la línea jurisprudencial de la Sala Primera[595], constituye un hecho ciertamente relevante a efectos del derecho al olvido que se viene tratando, aunque no en su vertiente material.

[595] De hecho esta resolución motivó la publicación de una nota informativa sobre el ejercicio del derecho al olvido, de 15 de marzo de 2016, por parte de la AEPD aclarando a tal efecto que, los interesados que obtuvieron fallos estimatorios de sus pretensiones sobre el ejercicio del derecho al olvido por parte de la AEPD que viesen anulados éstos a consecuencia de dicha sentencia y debido a la interpretación restrictiva de la Sala Tercera del TS acerca de la legitimación procesal de los motores de búsqueda, podrían volver a ejercitar los mismos derechos, en primer lugar, ante el responsable del tratamiento en cuestión y, en segundo lugar, frente a la AEPD.

Estos pronunciamientos contradictorios entre las distintas Salas del Tribunal Supremo, continuaron sucediéndose en el tiempo[596] prácticamente hasta la promulgación del GDPR que parece asentar ciertos criterios al respecto. En relación a la interpretación de dicho aspecto procesal controvertido, destacan asimismo, los pronunciamientos del Tribunal Supremo en sus STS 1280/2016, de 5 de abril y STS 574/2016, de 14 de marzo dictadas respectivamente por su Sala de lo Civil y Contencioso-Administrativa -cuyos pormenores se analizarán más adelante, en relación a otros apartados[597]-, que suponen un hito insólito en nuestra jurisprudencia al interpretar de forma completamente divergente y contrapuesta, en el transcurso de pocos días, el concepto de "tratamiento de datos de carácter personal", dando lugar a pronunciamientos ciertamente contradictorios.

Por último, destacar un pronunciamiento más reciente por parte del Alto Tribunal en torno al derecho al olvido, mediante la STS 446/2017, de 13 de julio (Sala de lo Civil) donde el recurrente ejercita dicho derecho en relación con la publicación de una fotografía suya que fue tomada a raíz de su detención y enjuiciamiento por varios delitos, entre ellos, el delito de asesinato de los cuales resultó absuelto al destruirse, debido a un error, todas las pruebas de cargo por el Juzgado que las custodiaba[598].

Frente a dicha solicitud, el Tribunal Supremo entiende que resulta improcedente declarar el derecho al olvido en tanto que la pretensión del recurrente, de retirar la información litigiosa, incluyendo su imagen, de todos los archivos informáticos que la pudieran alojar, así como de los buscadores web y las redes sociales, "*no tiene encaje en los supuestos analizados por la reciente jurisprudencia de esta sala con respecto al llamado 'derecho al olvido digital', entendido como una concreción del derecho a la protección de datos de carácter personal que protege, instrumentalmente, los derechos de la personalidad*" (FJ 1º).

[596] Sin ir más lejos, pocos días después, el 5 de abril, se promulgó la STS 210/2016 en la que la Sala Primera atribuyó a *Google Spain* la responsabilidad acerca de un tratamiento automatizado de datos personales llevado a cabo por *Google Search*, admitiendo, asimismo, su legitimación pasiva procesal *ad causam*.

[597] Vid. *infra* Cap. III. 6.2, en relación a la legitimación procesal pasiva de los motores de búsqueda.

[598] Esta resolución se publicó días después de dictarse la STS 426/2017, de 6 de julio, que versaba sobre los mismos hechos pero en procedimientos distintos, seguidos entre el mismo demandante y distintas partes demandadas, en concreto, dos periódicos que habían publicado tal fotografía.

Su argumentación, se basa en su doctrina clásica acerca de la distinción entre la responsabilidad de los motores de búsqueda y los editores web, al entender que el tratamiento de datos llevado a cabo es sensiblemente diferente en ambos casos, "*no corresponde a la empresa editora del periódico sino a las empresas titulares de los buscadores de Internet (contra las que no se ha formulado ninguna acción en este litigio) responder por mostrar en la lista de resultados los enlaces a las páginas web donde se contiene la información cuando se utilizan como términos de búsqueda los datos personales del afectado*" (FJ 3º).

También discute el tribunal, cosa que consideramos desacertada, que una imagen pueda ser considerada un dato personal a efectos de la LOPD y recuerda que, en el eventual ejercicio de ponderación entre los bienes jurídicos en conflicto, "*las hemerotecas digitales gozan de la protección de la libertad de información al satisfacer un interés público en el acceso a la información, razón por la cual las informaciones publicadas lícitamente no pueden ser objeto de cancelación o alteración*".

Destaca asimismo la resolución que, en el presente caso tampoco ha desaparecido el interés público de la noticia en tanto que dicha noticia venía referido al enjuiciamiento de unos hechos de extraordinaria gravedad e impacto social, que seguía teniendo una notoria actualidad en dicho momento y el escaso tiempo transcurrido -2 años- no convertía en desproporcionada la publicidad de dichos datos personales, por lo que "*el derecho al olvido digital no puede suponer una censura retrospectiva de las informaciones correctamente publicadas en su día*" (FJ 6º).

Ante lo anterior, y siguiendo con su línea jurisprudencial, el TS concluyó que "*el 'derecho al olvido' no ampara la alteración del contenido de la información original lícitamente publicada, en concreto, el borrado del nombre y apellidos o cualquier otro dato personal que constara en la misma. Tampoco ampara la supresión de la posibilidad de búsqueda específica de la noticia en su integridad del propio buscador interno de la hemeroteca digital*" (FJ 5º).

De este modo, se observa la evolución de la jurisprudencia del Alto Tribunal acerca del derecho al olvido cuyo origen jurisprudencial, así como debido a la inconcreción llevada a cabo en su consagración en el GDPR, ha hecho del todo imprescindible la interpretación de su contenido, alcance y ejercicio a manos de la jurisprudencia. Se ha querido dar aquí, una muestra de la jurisprudencia más significativa a través las sentencias expuestas en el presente apartado, a sabiendas de la existencia de otras muchas resoluciones al respecto[599].

iv. Tribunal Constitucional

Mediante sentencia de 4 de junio de 2018[600], el Tribunal Constitucional se pronunció por primera vez sobre el derecho al olvido, revocando parcialmente la ya comentada STS 545/2015, de 15 de octubre.

Recordar que dicha sentencia del Supremo estimó parcialmente el recurso presentado por un periódico frente a la resolución de la Audiencia Provincial de Barcelona de 11 de octubre de 2013[601] -comentada en páginas anteriores- que accedió a las peticiones de los demandantes en el sentido de que dicho medio eliminase de su hemeroteca digital sus nombres y apellidos puesto que, a través de ella, se accedía a unas informaciones de más de veinte años sobre su detención por tráfico de drogas cuando en la actualidad los afectados ya habían cumplido condena y tenían cancelados sus antecedentes penales. El Alto Tribunal, reconoció el derecho al olvido de los interesados pero, rechazó que dicho medio digital debiese alterar su

[599] Asimismo, podría citarse, como resoluciones del Alto Tribunal concernientes al derecho al olvido, las siguientes: STS 1055/2016, de 11 de marzo, STS 1103/2016, de 15 de marzo, la STS 1381/2016, STS 1382/2016, STS 1383/2016, STS 1384/2016, STS 1385/2016, STS 1386/2016, STS 1387/2016, STS 1388/2016, todas ellas de 13 de junio; la STS 1454/2016, STS 1455/2016, STS 1456/2016, STS 1457/2016, STS 1458/2016, STS 1459/2016, STS 1460/2016, todas ellas de 20 de junio; la STS 1529/2016, STS 1531/2016, STS 1532/2016, STS 1533/2016, STS 1534/2016, STS 1535/2016, STS 1536/2016, todas ellas de 27 de junio; STS 1610/2016, STS 1611/2016, STS 1612/2016, STS 1613/2016, STS 1615/2016, STS 1618/2016, todas ellas de 4 de julio; STS 1689/2016, STS 1690/2016, STS 1693/2016, STS 1694/2016, STS 1695/2016, STS 1696/2016, STS 1697/2016, todas ellas de 11 de julio; STS 1797/2016, STS 1799/2016, STS 1800/2016, STS 1801/2016, STS 1802/2016, STS 1803/2016, STS 1805/2016, STS 1806/2016, STS 1807/2016, STS 1808/2016, STS 1809/2016, STS 1810/2016, todas ellas de 18 de julio; STS 1910/2016, STS 1911/2016, STS 1912/2016, STS 1913/2016, STS 1915/2016, STS 1916/2016, STS 1917/2016, STS 1918/2016, STS 1919/2016, STS 1920/2016, todas ellas de 21 de julio.

[600] STC 58/2018, de 4 de junio.

[601] SAP Barcelona 486/2013, de 11 de octubre, Sección 14.

hemeroteca digital para eliminar de ella la información de los nombres y apellidos de los afectados, constituyendo así, hasta ahora, un límite inherente al derecho al olvido.

Los afectados presentaron un recurso de amparo ante el Tribunal Constitucional que, sin embargo, entiende en su interpretación que debe prohibirse indexar los nombres y los apellidos de los recurrentes para su uso por el motor de búsqueda interno de la hemeroteca digital pues "*se trata de 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*" disponiendo que la función informativa de dicho periódico queda salvaguardada al seguir estando dicha información almacenada en soporte papel, al que poder acudir en caso de querer consultarla para fines de investigación (FJ 8º).

Así pues, mediante dicho pronunciamiento constitucional, se modifican los criterios que, siguiendo la jurisprudencia del Tribunal Supremo, configuraban hasta ahora el derecho al olvido, especialmente, al considerar que este derecho no viene limitado por las hemerotecas digitales que, a partir de ahora, deberán eliminar de sus buscadores internos la opción de búsqueda de informaciones acerca de una persona introduciendo su nombre y apellidos, por ser contrario al derecho al olvido.

Dispone así que, si bien "*la universalización de acceso a las hemerotecas, facilitado por su digitalización, es decir por su transformación en bases de datos de noticias, tiene un efecto expansivo sobre la capacidad de los medios de comunicación para garantizar la formación de una opinión pública libre*", también debe reconocerse que "*este efecto expansivo también supone un incremento del impacto sobre los derechos fundamentales de las personas que protagonizan las noticias incluidas en hemerotecas*" (FJ 6º).

Sin embargo, no debe confundirse la obligación de desindexar las informaciones por los buscadores de las hemerotecas digitales con la obligación de borrar dicha información de las

páginas web de origen, el TC considera que dichos nombres y apellidos no deben suprimirse de la fuente principal que contiene la noticia ni tampoco sustituir éstos por sus iniciales pues, "*una vez impedido el acceso a la noticia a través de la desindexación basada en el nombre propio de las personas recurrentes, la alteración de su contenido ya no resulta necesaria para satisfacer los derechos invocados por las personas recurrentes, pues la difusión de la noticia potencialmente vulneradora de éstos ha quedado reducida cuantitativa y cualitativamente, al desvincularla de las menciones de identidad de aquéllas. Esta limitación en la difusión de la noticia, que es lo que implica la protección de dichos derechos, se puede lograr sin necesidad de acordar su anonimización. Esta opción, que supondría una injerencia más intensa en la libertad de prensa que la simple limitación en la difusión, resulta por tanto innecesaria*" (FJ 8º).

El Tribunal, reconoce en su resolución la importancia del papel de la información pública en una sociedad democrática, en especial sobre la opinión y el debate público libre, sin embargo, en caso concreto rechaza la prevalencia del derecho a la información sobre la privacidad de los afectados, teniendo en cuenta el tiempo transcurrido -30 años-, la naturaleza privada de los sujetos, y la escasa notoriedad de los hechos delictivos. En cambio, considera que la publicidad de dichos hechos en la actualidad, ocasiona daños desproporcionados para el honor y la privacidad de los afectados.

Declara así el TC: "*Sin embargo, en el caso de autos el delito relatado en la noticia ni fue particularmente grave ni ocasionó especial impacto en la sociedad de la época. En consecuencia, el transcurso de tan amplio margen de tiempo ha provocado que el inicial interés que el asunto suscitó haya desaparecido por completo. A la inversa, el daño que la difusión actual de la noticia produce en los derechos al honor, intimidad y protección de datos personales de las personas recurrentes reviste particular gravedad, por el fuerte descrédito que en su vida personal y profesional origina la naturaleza de los datos difundidos (participación en un delito, drogadicción). Este daño, por consiguiente, se estima desproporcionado frente al escaso interés actual que la noticia suscita, y que se limita a su condición de archivo periodístico*" (FJ 8º).

Otra de las cuestiones relevantes de esta sentencia, y sobre la que se incidirá más adelante, es la relativa a su atribución al derecho al olvido de carácter fundamental y autónomo, sobre la base del derecho a la protección de datos personales, la intimidad y el honor "*a la hora de valorar el sacrificio requerido a la libertad de información [art. 20.1 d) CE], para asegurar el disfrute adecuado del derecho a la intimidad de las personas recurrentes en conexión con el derecho a la autodeterminación informativa (art. 18.1 y 4 CE), es necesario recordar la importancia de las hemerotecas digitales en el contexto de las actuales sociedades de la información. Esto significa que serán conducentes al restablecimiento del derecho al honor, a la intimidad y a la protección de los datos personales las medidas tecnológicas tendentes a limitar adecuadamente la difusión de la noticia, que garanticen, en lo que sea conciliable con dicha regla, la integridad de la hemeroteca y su accesibilidad en general*" (FJ 8º) y, en base a ello, dispone "este reconocimiento expreso del derecho al olvido*, como facultad inherente al derecho a la protección de datos personales, y por tanto como derecho fundamental, supone la automática aplicación al mismo de la jurisprudencia relativa a los límites de los derechos fundamentales*" (FJ 6º).

El derecho al olvido, pese a no encontrarse recogido expresamente en ninguna norma emanada del legislador español (se incluye, eso sí, en el Proyecto de Ley Orgánica de Protección de Datos Personales) forma parte de nuestro ordenamiento jurídico en tanto que resulta de la aplicación directa del GDPR que sí que lo contempla de forma expresa, así como de forma indirecta, de la necesidad del interpretar el derecho español conforme a las disposiciones internacionales en la materia (artículo 10.2 CE), e igualmente deriva de las resoluciones jurisdiccionales de tribunales supraestatales que resulten vinculantes, como ocurrió en el *caso Google* con el TJUE. En consecuencia, el Tribunal Constitucional, no podía obviar la realidad social del momento ni las demandas de amparo de los ciudadanos, teniendo en cuenta el nuevo marco regulador y la evolución imparable que ha presentado la protección de datos personales, como mandato inherente al ejercicio de sus funciones[602].

[602] Si bien ello podría comportar ciertas objeciones desde el punto de vista de la función de la judicatura y la creación de nuevos derechos a tenor de su labor de interpretación y los conflictos que pueden derivarse de la separación de poderes, afirma FRÍGOLS I BRINES "es absolutamente cierto que los jueces no se hallan legitimados para crear Derecho, puesto

Se produce así una relación de complementariedad, en la medida en que, si bien el derecho interpretado por los tribunales debe partir de la existencia misma de la ley, también es defendible la tesis de la subordinación de la propia ley al Derecho, como resultado de la consiguiente disociación de vigencia y validez, en términos de justicia, de las normas[603]. De este modo, parece claro que la seguridad jurídica y la propia hermenéutica jurídica de los tribunales, permiten desarrollar una interpretación crítica, ajustando los preceptos legales al contexto actual para una adecuada protección de los derechos fundamentales, sin que sea necesario en ningún caso que la aplicación de la norma y su tenor literal, sean del todo coincidentes[604].

2.3. Origen normativo

A raíz del clima de cambio descrito anteriormente, de las demandas de la ciudadanía para la protección de sus derechos fundamentales frente a las innovaciones tecnológicas y la afirmación por parte de la jurisprudencia de diversos órganos jurisdiccionales acerca de la existencia de un derecho al olvido, finalmente éste encontró su ratificación en el Reglamento UE 2016/679 de protección de datos personales[605] (GDPR), sobre el cual se incidirá más adelante.

---

que, como ya se dio, el Derecho en una sociedad democrática sólo puede ser fruto de la voluntad popular. Sin embargo, sí que se hallan legitimados para aplicarlo: esa es su función fundamental. El problema que subyace a la cuestión de si los jueces se hallan legitimados o no para crear, en alguna medida, Derecho, creo que radica en la distancia entre el concepto de aplicación y existencia del Derecho del que se parte para enjuiciar la actividad judicial […] la falta de autorización para crear Derecho no puede ser un escollo insalvable de la actividad jurisdiccional, porque la tarea del juez es inevitablemente creadora –aunque el grado en que dicha tarea sea creadora depende, al menos en parte, del margen que le confiera el legislador mediante la observancia o no del principio de taxatividad". Cfr. *Fundamentos de la Sucesión de Leyes en el Derecho penal español. Existencia y aplicabilidad temporal de las normas penales*, Bosch, Barcelona, 2004, p. 379.

[603] Cfr. ALEXY. *Teoría de la argumentación jurídica*, Centro de Estudios Políticos y Constitucionales, Madrid, 1989, pp. 22 y ss.

[604] Así lo dispone MÜLLER en su estudio sobre la integración interpretativa de la norma jurídica: "no aparecen en la práctica como juicios hipotéticos logificados, como órdenes idénticas a su tenor literal, sino como regulaciones que, además de los recursos metodológicos tradicionales, necesitan de numerosos elementos interpretativos procedentes de la realidad social normada, que no pueden extraerse mediante las reglas clásicas de la interpretación, ni del precepto y su génesis, ni del contexto sistemático de su significado". Cfr. "Tesis acerca de la estructura de las normas jurídicas" en *Revista Española de Derecho Constitucional*, nº 27, 1989, p. 114.

[605] *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 y por el que se deroga la Directiva 95/46/CE*.

Ante dichas circunstancias, y dada la función de adecuación del Derecho a la realidad social de cada momento, se dictó una nueva normativa europea en materia de datos personales mediante la cual se pretendía dotar de respuestas jurídicas a los problemas que estaba ocasionando la irrupción del *Big data* y la consolidación de una memoria virtual permanente en los derechos más fundamentales.

Así, el Reglamento europeo es el primer texto del ordenamiento jurídico en vigor que contempla expresamente el derecho al olvido, al cual denomina "derecho de supresión"[606], tal y como había reparado el TJUE en la famosa sentencia del *caso Google*, configurándolo sobre la base del derecho a la protección de datos personales, como una suerte de derivación del derecho a la intimidad y propia imagen, y como extensión del derecho al honor.

De este modo, trata de ponerse remedio a la situación preexistente en la que se había convertido en una tarea realmente ardua y, en ocasiones hasta imposible, el ejercicio de los derecho de acceso, rectificación, cancelación y oposición (comúnmente denominados ARCO), en un momento en el que el tratamiento de datos personales había – y ha- alcanzado sus cotas más altas. Además de la realización de dichos derechos, el GDPR permite a los interesados, obtener el borrado online de sus datos personales, y en ocasiones su cifrado, cuándo éstos resulten perjudiciales para sus derechos fundamentales.

[606] Artículo 17 GDPR: **1.** *"El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando 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 de otro modo; 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.* **2.** *Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, 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".*

En definitiva, la intención del derecho al olvido es proteger la privacidad de los individuos en los términos expuesto en esta tesis doctoral, y más allá de sus ligámenes inexorables con el derecho a la protección de datos personales, en última instancia el derecho de supresión se erige como garantía del derecho a la dignidad y el libre desarrollo de la personalidad. Así, como más tarde se verá, el derecho al olvido viene configurado heterogéneamente por diversos elementos que tienen en común dotar al titular de un control sobre sus propios datos personales, pudiendo suprimir digitalmente cualquier información que afecte a su privacidad, siempre que se den los presupuestos para ello.

Sin embargo, no se trata de dotar a los usuarios de un poder universal para construir un *currículum* digital a su antojo pues, el derecho al olvido no es absoluto, está sujeto a numerosas limitaciones como se deriva del propio articulado del GDPR, cuyo tercer párrafo del artículo 17 especifica, entre otras, el derecho a la libertad de expresión e información, razones de interés público, fines de investigación o estadístico, el cumplimiento de una obligación legal o el derecho de reclamación. Ello obligará a los órganos jurisdiccionales a llevar a cabo un ejercicio de ponderación cuando se produzca la colisión entre distintos bienes jurídicos protegidos que, como ya se ha visto, dadas las exigencias de adaptabilidad de los presupuestos jurídicos a la realidad actual, han ocasionado la evolución de la jurisprudencia constitucional en torno a la libertad de expresión e información.

Finalmente, en cuanto a su naturaleza jurídica, como se profundizará más adelante, si bien en origen, el legislador europeo parecía haber partido de los derechos ARCO para desarrollar el derecho de supresión, con el objetivo de adecuar sus presupuestos al nuevo contexto, la doctrina y la jurisprudencia más reciente le han dotado de un carácter fundamental autónomo, aunque sea a consecuencia de los anteriores.

3. Marco legal para el desarrollo evolutivo del derecho al olvido

3.1. Reglamento Europeo de Protección de Datos (GDPR)

Como se ha visto anteriormente, el derecho al olvido viene reconocido expresamente y por vez primera en el Reglamento europeo de protección de datos. De hecho, hasta la fecha,

éste es el único instrumento normativo vinculante y en vigor que recoge de forma expresa el derecho de supresión de toda persona sobre sus datos personales como potestad de autodeterminación informativa y como forma de garantía de su privacidad. No obstante, el actual Proyecto de Ley Orgánica de Protección de Datos Personales -en tramitación parlamentaria en el momento de redacción de este Capítulo- contempla, por primera vez en nuestro ordenamiento jurídico, el derecho al olvido en su artículo 15, bajo la denominación de "derecho de supresión"[607].

Este nuevo Reglamento supone un avance considerable en materia de protección de datos al tomar al fin conciencia de las amenazas que para los derechos fundamentales provocan las nuevas tecnologías, así como el uso masivo de datos derivado de éstas. En este sentido, afirma: "*el tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad*" (considerando cuarto) y, en consecuencia, apuesta notablemente por dotar a los ciudadanos de auténticos poderes de control sobre su información personal.

El GDPR ha dado así respuesta a las insistentes críticas recibidas por la Directiva 95/46 –la cual deroga- acerca de la fragmentación de la protección de datos que en nada favorecía a la seguridad jurídica, así como a la complejidad de la normativa anterior en materia de transferencias internacionales de datos personales -origen de múltiples conflictos para la economía global- y al problema de la "doble velocidad europea en materia sancionadora"[608]. En efecto, la Directiva derogada apenas imponía a los Estados la obligación de prever sanciones coercitivas para el cumplimiento de su normativa lo que originó grandes asimetrías en el seno de la UE donde, algunos países –entre ellos España- adoptaron un régimen económico

[607] "1. *El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.* 2. *Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa*".

[608] Cfr. LÓPEZ CALVO. *Comentarios al Reglamento Europeo de Protección de Datos*, Serpin, Madrid, 2017.

sancionador disuasorio y otros no. Ahora, el GDPR dispone un régimen de sanciones aplicable a todo el territorio de la Unión Europea mediante un sistema de multas proporcionadas, disuasorias y potencialmente millonarias[609].

Por otra parte, el Reglamento evidencia la irreversible europeización de la estrategia pública de protección de los derechos fundamentales frente al poder y el avance de la tecnología y la informática, que ya fue iniciada por la derogada Directiva 95/46/CE y que el artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea ya consiguió elevar a rango constitucional europeo un derecho fundamental autónomo a la protección de datos y que la jurisprudencia europea -principalmente el TJUE- ha reafirmado con sus numerosos pronunciamientos argumentando la prevalencia de los derechos fundamentales sobre la tecnología[610].

a) Principales novedades que presenta el Reglamento

Por primera vez en la historia, todos los países de la Unión Europea quedan sometidos a una misma regulación en materia de protección de datos personales, sin que sea necesaria su intervención legislativa para la aplicabilidad de los derechos que ésta conlleva. La nueva normativa asume como regla básica el hecho de que la información personal debe estar sometida al propio criterio del interesado, suponiendo un cambio radical en materia de protección de datos, en primer lugar, al dotar al titular de los datos de todo tipo de derechos para facilitar la gestión de su información personal en base a sus preferencias y, en segundo lugar, al someter la actuación de empresas privadas y administraciones públicas al interés del ciudadano, obligándoles a adoptar políticas activas de protección de datos y cambiando las reglas de juego existentes.

Asimismo, el Reglamento moderniza y unifica el derecho a la protección de los datos teniendo en cuenta el nuevo escenario tecnológico y tratando de acabar con las existentes

[609] RALLO LLOMBARTE. "De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018)", *Revista de Derecho Político*, nº 100, 2017, p. 660.

[610] Cfr. RUIZ MIGUEL, C. "El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico", en *Revista de Derecho Comunitario Europeo*, nº 14, pp. 7 ss.

discrepancias entre los Estados miembros a consecuencia, principalmente, de la gran cantidad de cláusulas abiertas que contenía (*open-ended-principles*), que dieron como resultado una trasposición divergente en las distintas normas europeas. Con una voluntad claramente integradora, se trata así de poner solución a los problemas existentes de regulación que en nada favorecía a la protección de los derechos fundamentales, dotando a las empresas operadoras de Internet de nuevas obligaciones así como reduciendo el margen de actuación de los Estados miembros.

Otra de las grandes novedades del GDPR es que trata de poner fin al problema de falta de territorialidad a través de la extensión de la aplicabilidad de su articulado hacia aquellos responsables que no estén establecidos en la UE cuando las actividades de tratamiento de datos personales estén relacionados con la oferta de bienes o servicios a interesados que residan en suelo europeo o que ejerzan su actividad en éste (artículo 3). De este modo, termina de una vez por todas con la disparidad de criterios entre los distintos órganos jurisdiccionales respecto de cuestiones tan importantes como la legitimidad pasiva de los intervinientes.

Con la extensión de su aplicación territorial se pretende subsanar los impedimentos existentes respecto de la actuación de los poderes legislativo y judicial, y poner fin a la práctica consolidada entre las corporaciones de Internet de establecer sus sedes en países cuyas legislaciones permiten sin demasiados problemas la mercantilización de la información personal, ignorando reiteradamente la legislación doméstica y europea en la materia e impidiendo el ejercicio eficaz de los derechos de los ciudadanos a quienes dejaba en una situación jurídica de indefensión. Así pues, el artículo 29 obliga a estas empresas a someterse al Derecho de la Unión y a los tribunales nacionales de los Estados miembros cuando ofrezcan sus servicios en suelo europeo, constriñendo la actuación de las mismas en el intento de cumplir con sus obligaciones.

Esta nueva normativa pretende hacer realidad el "habeas data" de los ciudadanos, permitiéndoles un mejor control de su información personal así como dotándolos de instrumentos efectivos para el cumplimiento de sus derechos, como se ha ejemplificado con la extensión de las obligaciones de su articulado más allá del territorio de la Unión.

Por otro lado, mediante la introducción del concepto de "responsabilidad activa", se obliga a unos y a otros a que adopten todas las medidas necesarias para cumplir con los principios, derechos y garantías que se recogen en el GDPR, responsabilizando a ambos de la gestión de la información personal (artículo 24), todo ello junto a numerosas obligaciones encaminadas hacia la protección de los derechos de los usuarios, entre otras, estableciendo códigos de buenas prácticas, realizando evaluaciones de impacto, introduciendo políticas de protección de datos por defecto o nombrando un Delegado de Protección de Datos.

Se recogen en cierto modo, los tradicionales derechos ARCO con significantes modificaciones. Así, por ejemplo, se simplifican las fórmulas para facilitar al interesado el ejercicio de sus derechos de rectificación (artículo 13), se dispone el derecho de todo interesado a obtener una copia de los datos personales objeto del tratamiento (artículo 15), se introduce el derecho de bloqueo de datos como variante o alternativa al derecho de cancelación (artículo 19), se prevé la posibilidad de limitar el tratamiento de los datos (artículo 18) y se refuerza el derecho de oposición introduciendo nuevos motivos como la elaboración de perfiles (artículo 21).

Para dotar de mayor virtualidad al control de los ciudadanos de su propia información personal se reconoce expresamente el derecho a la portabilidad de datos (artículo 20), permitiendo a todo usuario solicitar en cualquier momento la retirada de Internet de aquéllos datos personales que ya no sean necesarios para las finalidades iniciales por las que fueron recogidos, del mismo modo que si se trata de informaciones obsoletas o irrelevantes. Entre los derechos de nueva incorporación destaca preeminentemente, como ya se ha visto, el derecho de supresión, permitiendo a todo interesado obtener "sin dilación indebida" el borrado de sus datos personales (artículo 17).

Para facilitar el ejercicio de estas potestades se dispone que los responsables posibiliten la presentación de solicitudes por medios electrónicos, especialmente cuando el tratamiento se lleve a cabo por estos canales (artículo 15). De igual forma, el ejercicio de dichos derechos será

preeminentemente gratuito (artículo 12). Asimismo, el GDPR incorpora nuevas herramientas de control como el cifrado o la anonimización de los datos personales (artículo 32), evitando de forma irreversible la identificación de los sujetos; la seudonimización, consistente en reemplazar un atributo en un registro por otro de manera que la persona sólo puede ser identificada mediante otro mecanismo indirecto (artículo 25); la obligación de realizar una evaluación de impacto (*Privacy Impact Assessment*) cuando se lleve a cabo un tratamiento de datos que pueda conllevar un alto riesgo para los derechos y libertades de las personas físicas (artículo 35) o mediante la aplicación de otras medidas de seguridad (artículo 32)[611].

Se contemplan actuaciones preventivas encaminadas a cumplir con las disposiciones de su articulado, como se extrae de la inclusión de la protección de datos desde el diseño y por defecto como orientación de las políticas y decisiones empresariales que deben llevar a cabo los encargados de cualquier tratamiento de datos personales (artículo 25) como regla general y desde el origen. Junto a este extremo, se introduce el concepto de responsabilidad proactiva (*accountability*) que exige a los encargados la adopción de medidas suficientes para garantizar un tratamiento lícito (artículo 5.2) y exige transparencia en los procedimientos para salvaguardar el ejercicio de los derechos del interesado (artículo 12). De hecho, a lo largo de su articulado el GDPR insiste en la necesidad de transparencia e información al ciudadano sobre el conjunto de su información personal (contenido, situación, derechos…) y en base a tal principio vertebrador, ha introducido ciertas mejoras en los procesos de otorgamiento del consentimiento.

Por último, y desde una óptica procesal, destacar que, junto al anteriormente mencionado principio de extensión extraterritorial del artículo 3, se prevé como garantía adicional, que los recursos jurisdiccionales puedan ejercitarse en el Estado miembro en que el interesado tenga su residencia habitual (artículo 79). Asimismo, se reconoce a todo organismo, organización o asociación que tenga por objeto proteger los derechos e intereses de los usuarios y esté debidamente constituida conforme a la legislación doméstica, el derecho a presentar una

[611] El GDPR ya no distingue entre ficheros de nivel básico, medio o alto, sino que impone medidas de seguridad en base al estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y las libertades concretas de las personas físicas.

reclamación colectiva frente a la autoridad nacional de control por cuenta de uno o más interesados que consideren que se han vulnerado sus derechos (artículo 80).

b) Consideraciones críticas

Por lo que respecta a los aspectos formales, el marco legal comunitario plantea determinadas cuestiones respecto de su armonización a efectos materiales con las normativas nacionales en materia de protección de datos. En el caso del ordenamiento jurídico español, suscita dudas la articulación de los derechos de transparencia, información, acceso, rectificación, supresión, limitación del tratamiento, portabilidad de datos y oposición, todos ellos recogidos en el GDPR, con los tradicionales derechos ARCO (acceso, rectificación, cancelación y oposición) de la doctrina española. Asimismo, urge desarrollar una respuesta efectiva para determinadas cuestiones, como por ejemplo, qué ocurrirá a partir de ahora con el registro de ficheros, qué papel jugará la Agencia Española de Protección de Datos (AEPD) así como el valor de sus circulares, o los problemas que puedan surgir de la articulación del Reglamento con la LOPJ, dado que resulta menos garantista en comparación con la nueva normativa y, en consecuencia incompatible con el GDPR, mientras se dicta una nueva legislación doméstica que, en contra de lo dispuesto por el Reglamento, no ha llegado a tiempo para el 25 de mayo de 2018, fecha de entrada en vigor del GDPR.

En cuanto a los aspectos sustantivos del Reglamento, resulta llamativo cómo, pese a establecer ciertos principios programáticos en la norma que sugieren un cambio de modelo -proponiendo políticas de privacidad desde el diseño o facilitando el control por parte del ciudadano de sus propios datos- la normativa adolece de cierto continuismo, introduciendo medidas fragmentarias y dejando nuevamente mucho margen para la interpretación, debido al abuso de conceptos ambiguos y jurídicamente indeterminados[612]. Mención aparte merece la promoción que el GDPR realiza de la autorregulación, a través de las certificaciones y sellos

[612] El Reglamento abusa del empleo de términos jurídicos indeterminados así como de expresiones vagas o poco concisas, y asimismo, realiza remisiones constantes a la regulación posterior por los Estado miembro, a quienes delega la concreción de muchos aspectos jurídicos problemáticos, en contra del principio de armonización que se pretendió con la concepción de dicha normativa que, entre otras cosas se elaboró como Reglamento y no como Directiva para evitar la disparidad de criterios entre las legislaciones domésticas.

(artículos 42 y 43) y que parece incompatible con una intervención pública para la regulación del sector.

Esta falta de concreción, indirectamente, también acabará incidiendo sobre los órganos jurisdiccionales, quienes deberán de integrar las lagunas legales mediante su labor de interpretación, con la consiguiente lesión que ello conlleva para la separación entre poderes. La actuación del legislador que delega en los órganos jurisdiccionales la responsabilidad para la concreción de conceptos jurídicos indeterminados, es ciertamente criticable en tanto que estaría renunciando a su propia tarea de definición mediante la utilización de un concepto absolutamente general e indeterminado, pero aparentemente dotado de significación.

Esta complejidad terminológica lleva aparejada la introducción de la figura del Delegado de Protección de Datos, presentada como medida estrella para garantizar la seguridad, pero que en la práctica supondrá cierta arbitrariedad en las decisiones que éstos tomen, y que dependerá de los términos en que se lleve a cabo la interpretación de unos o de otros. Sin embargo, parece una obviedad que el alcance de un derecho fundamental deba delimitarse en términos objetivos y de un modo global y no en base a la opinión de ciertos expertos, dejando un peligroso margen para la autonomía privada.

En relación a lo anterior, el Reglamento asume como regla básica que la información personal debe estar sometida al control del interesado, a quien dota de un mayor dominio para que gestione sus datos conforme a su propio criterio. Sin embargo, estas medidas de autogobierno presuponen la existencia de una concienciación y responsabilidad ciudadana que, desgraciadamente, dista mucho de la realidad -sólo hay que ver cuántos usuarios leen las políticas de privacidad de las aplicaciones o servicios que usan a diario-, y a quién no se le puede exigir conocimientos jurídico-técnicos para ello.

Entendemos que, para que se trate de una medida ciertamente proteccionista, de ningún modo puede transferírsele a aquella persona que se vea expuesta en sus datos personales la responsabilidad de gestionar dicha situación, haciéndole dirigirse a una suerte de operadores y empresas de Internet. Todo lo contrario, deberían establecerse mecanismos que efectivamente

impongan medidas respetuosas con la privacidad desde el origen, cuyo tratamiento de datos se minimice y se constriña a fines específicos, y no recaiga en la responsabilidad individual, ni del interesado ni del Delegado de Protección de Datos. Así, por ejemplo, el derecho al olvido se debería de establecer automáticamente y como regla general cumplidos unos requisitos previos, y no limitar su operatividad bajo petición, dejando en manos y a instancia del interesado su ejecución.

Todo ello, junto con el relego del establecimiento de la mayoría de los procedimientos para el cumplimiento del articulado en manos de los legisladores domésticos, difiere notablemente de la voluntad homogeneizadora del legislador europeo.

En cuanto a su operatividad, el cumplimiento del Reglamento exige unos medios así como una preparación, dedicación y control constante por parte de las organizaciones que traten con datos personales, cuya aplicación efectiva parece en ocasiones imposible, pues incrementa exponencialmente sus esfuerzos burocráticos, lo que resultará especialmente gravoso para las PIMES y los autónomos. Así por ejemplo, el tenor literal de alguna de sus disposiciones exige contar con el consentimiento expreso del interesado para cada uno de los supuestos imaginables de tratamiento de sus datos personales.

Parece dudoso que este esfuerzo burocrático se traduzca efectivamente en un cambio sustancial para la privacidad de los ciudadanos pues, junto a las muchas cuestiones abiertas que no encuentran solución en la nueva normativa, ésta no parece contar con la connivencia de las grandes corporaciones del *Big data*. Así, por ejemplo, se plantean interrogantes acerca de cómo se aplica el GDPR en "la nube", muchas veces lejos del control de las empresas y objeto de duplicados. En teoría, a partir de ahora, deberá de tenerse pleno dominio sobre los datos vertidos en dicha plataforma para, por ejemplo, poder ejecutar derechos como el de supresión, con independencia de que se subcontrate a un tercero la responsabilidad del cumplimiento del GDPR.

En otro orden de cosas, resultaría ingenuo pensar que la finalidad última de esta nueva normativa es proteger a los ciudadanos y a sus datos personales frente a las amenazas del *Big*

data pues resulta bastante obvio que el propósito del GDPR es, asimismo, sentar las bases para lograr un mercado digital único y evitar que se continúen produciendo obstáculos para el mercado interior de la Unión Europea -que, en la práctica, está dificultando el ejercicio de actividades económicas a escala comunitaria- y acabar con el falseamiento de la competencia[613].

En cualquier caso y a pesar de las buenas intenciones del GDPR, no parece del todo realista el deseable cambio drástico en estas cuestiones pues, si bien es cierto que la nueva normativa introduce más obligaciones a los encargados y responsables del tratamiento de datos -bajo pena de sanción- así como reconoce más derechos para los interesados, no parece que cuente con el necesario respaldo de las empresas tecnológicas y las corporaciones del *Big data*, nada dispuestas a renunciar al filón de negocio que supone hoy en día la privacidad.

Si bien es cierto que no se puede negar el carácter renovador del GDPR, que apuesta por la privacidad de los ciudadanos y su empoderamiento para defenderse frente a las agresiones de las nuevas tecnologías, una auténtica transformación del modelo necesita forzosamente contar con la complicidad de aquellos que diseñan productos y ofrecen servicios relacionados en dicho contexto para que tomen consciencia de los retos actuales y actúen en consonancia para la protección de los derechos y libertades de los ciudadanos, a quienes se les ofrezca productos y servicios respetuosos con su privacidad y por defecto.

c) El nuevo marco europeo para la protección de datos personales

Por último y muy brevemente, debe hacerse referencia a la Directiva 2016/680 relativa al tratamiento de datos personales para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales[614] que, junto con el GDPR, han sido denominados como el "nuevo marco europeo de protección de datos".

---

[613] Esta ambivalencia, entre la protección de los derechos de los ciudadanos y del mercado digital único se observa en su considerando segundo, al afirmar "*El presente Reglamento pretende contribuir a la plena realización de un espacio de libertad, seguridad y justicia y de una unión económica, al progreso económico y social, al refuerzo y la convergencia de las economías dentro del mercado interior, así como al bienestar de las personas físicas*".

[614] Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de

Puesto que el GDPR no extiende sus actividades a aquellas materias que quedan fuera del alcance de la legislación europea por cuestiones de competencia, como por ejemplo en materia de seguridad nacional o el procesamiento de los datos personales con fines policiales y judiciales[615], ello se aborda en esta Directiva que, junto con el Reglamento europeo de protección de datos, tiene por objeto establecer los pilares para que el mercado único digital se consolide.

De este modo, la presente Directiva que entró en vigor el 5 de mayo de 2016 y debía trasponerse por los Estados miembros antes del 6 de mayo de 2018, tiene por objeto regular el tratamiento de los datos personales de todos aquellos que se vean inmersos en una investigación criminal con el objeto de que dicha información pueda ser compartida entre las autoridades policiales y judiciales de los distintos Estados europeos, y tratar así de combatir el crimen en Europa y el terrorismo internacional.

A tal fin se enumeran los principios que rigen el tratamiento de datos personales y por los que, necesariamente, éstos habrán de ser exactos, pertinentes y no excesivos, obligando a los Estados miembro a adoptar todos los mecanismos necesarios para garantizar un adecuado nivel de seguridad y confidencialidad así como fijar unos plazos apropiados para la supresión de los datos personales o para una revisión periódica de su necesidad de conservación (artículos 4 y 5), todo ello conforme a las líneas generales establecidas por el GDPR.

Aunque la Directiva se refiere exclusivamente al tratamiento de los datos que pueda tener alguna incidencia a nivel comunitario, encontramos varios conceptos jurídicos indeterminados en sus disposiciones. Por una parte no queda claro como las autoridades nacionales de cada país distinguirán entre aquellos datos que sean de interés exclusivamente a nivel doméstico y aquellos otros que puedan trascender las fronteras por lo que, en la práctica, es más que probable que haya un flujo innecesario de datos personales especialmente sensibles

---

prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

[615] Art. 2.2 GDPR: "*El presente Reglamento no se aplica al tratamiento de datos personales:* […] *d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención*".

entre los países europeos, lo que resulta contrario al principio de minimización de los datos del GDPR (y es que, más allá de las garantías que pueda ofrecer dicha Directiva, no hay nada tan seguro como el no compartir ningún dato).

Por otra parte, conviene también poner en duda la inocuidad del almacenamiento de los datos que se prevé por dicha Directiva, al menos en cuanto a su uso efectivo posterior pues, dada la abundancia de conceptos jurídicos indeterminados, no resulta difícil caer en teorías conspiratorias sobre la vigilancia masiva de los ciudadanos ni mucho menos sorprenderse de la paradoja que supone el principio de la protección de datos "por diseño y por defecto" que propugna (artículo 20).

3.2. La protección de datos personales como origen y fundamento del derecho al olvido. Breve recorrido por el reconocimiento del derecho a la protección de datos

Como se ha evidenciado anteriormente, el derecho al olvido tiene su origen y fundamento en el derecho a la protección de datos personales pues, por una parte, surge en el contexto de la revolución informática y tecnológica, por la necesidad de dotar a los ciudadanos de un mayor control sobre su información personal, como consecuencia de la exposición pública en Internet y el funcionamiento del modelo del *Big data*, lo que conlleva a facultarlos para suprimir aquellos datos que, por diversos motivos -como el transcurso del tiempo o el término de la finalidad para la que fueron recogidos-, sólo contribuyen a menoscabar su privacidad.

Por otra parte, como ya se ha analizado en páginas anteriores, la diversa jurisprudencia que ha dado origen al derecho de protección de datos y al olvido, así como contribuido a su configuración -desde el Tribunal de Justicia de la Unión Europea hasta nuestro Tribunal Constitucional-, así lo han señalado. No cabe duda pues, de que el derecho al olvido tiene sus raíces en el derecho a la protección de datos pese a que, como también ha sostenido la jurisprudencia, en la actualidad éste haya conseguido una virtualidad propia.

Como a continuación se profundizará, el derecho a la protección de datos -en origen "libertad informática" y, en la actualidad, también llamado *Habeas Data* o derecho a la

autodeterminación informativa[616]- tiene un reconocimiento amplio en distintos instrumentos supranacionales como la Carta de Derechos Fundamentales de la Unión Europea o el Convenio Europeo de Derechos Humanos, mientras que en nuestro ordenamiento jurídico no está expresamente positivizado en la Constitución española, sino que su reconocimiento se ha producido de la mano del legislador ordinario.

a) La protección de datos en la Constitución Española

Como ya se ha dicho, el derecho a la protección de datos es un derecho de configuración legal, pues resulta necesario acudir a la intervención del legislador para desvelar su contenido y, en consecuencia, dotarle de plena efectividad. Ello ocurre porque dicho derecho carece de una mención directa en el texto constitucional dado que, su artículo 18.4 cuando dispone "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*", no descifra el verdadero significado del derecho a la autodeterminación informativa, dejando una enorme apertura normativa para el legislador ordinario, así como para los Jueces y Tribunales.

Sin embargo, ello no supone negar el carácter fundamental del derecho a la protección de datos pues éste no presenta diferencias cualitativas con respecto a los restantes derechos fundamentales. Sin embargo, su naturaleza de configuración legal dota al legislador de unas mayores facultades a la hora de establecer el sistema de garantías[617]. Como señala DÍEZ-PICAZO GIMÉNEZ ello implica un desdoblamiento de las normas de referencia que, en este caso al no regir el respeto a la configuración constitucional del derecho fundamental como

[616] Algunos autores prefieren esta última denominación en cuanto que expresa la vertiente positiva del derecho, prescindiendo de la connotación negativa del "derecho a la protección de datos" y en tanto que parece que ésta fue su denominación original, pues fue la fórmula que empleada por el Tribunal Constitucional Federal de Alemania el 15 de diciembre de 1983, cuando interpretó en una sentencia ya famosa, la Ley del Censo. Entre estos autores encontramos a MURILLO DE LA CUEVA quien defiende dicha denominación pues "refleja el aspecto más característico de un derecho nuevo que ha ido cobrando cuerpo bajo distintas formas en los ordenamientos de los Estados democráticos: el control que ofrece a las personas sobre el uso por terceros de información sobre ellas mismas". Cfr. *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, 2009, p. 11.

[617] Cfr. DEL CASTILLO VÁZQUEZ. *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*, Civitas, Pamplona, 2007, pp. 319 ss.

criterio de referencia, éste vendrá dado por la unión entre la norma constitucional y las normas de desarrollo[618].

Debe en todo caso reconocerse a la Constitución española su valor indiscutible de ser uno de los textos constitucionales pioneros en el reconocimiento de la necesidad de proteger a las personas frente a las intromisiones de la informática pese a que su configuración le hizo valerse las críticas de la doctrina por entender que reiteraba innecesariamente la protección del derecho a la intimidad y el honor consagrados en su apartado primero[619].

Así, se ha llegado a afirmar por algunos autores que la tutela que otorga el artículo 18.4 CE no deja de ser residual o insatisfactoria en orden a la efectiva protección de la autodeterminación pues su referencia expresa a la "intimidad" no permite amparar conductas que siendo merecedoras de protección y perteneciendo a la esfera privada del sujeto, no pertenecen al ámbito estricto de la intimidad, lo que ha ocasionado, como a continuación se observará, una interpretación extensiva de dicho precepto para dar cabida al derecho fundamental de protección de datos personales[620].

Sin embargo, debemos recordar que la Constitución es una norma de mínimos, cuyo articulado pretende orientar la regulación de la vida en comunidad pero que no constituye un *numerus clausus* de derechos y libertades, sino que sus preceptos pueden y deben desarrollarse en ulteriores textos normativos más allá de su contenido esencial, al que deben respetar en todo caso. Por otra parte, la Constitución responde a la realidad sociopolítica del momento en que fue creada y, pese a que tiene una clara vocación de permanencia, ello no obsta que sus

[618] DÍEZ-PICAZO GIMÉNEZ. *Sistema de derechos Fundamentales*, Civitas, Madrid, 2013, p. 120.

[619] Por todos, MORALES PRATS critica, además, la ubicación del apartado en el texto constitucional de dicho precepto por convertirlo "una cláusula constitucional de oscura interpretación, en la que *a priori* no aparecen suficientemente aclarados sus fines, ni tan siquiera su alcance". Cfr. *La tutela penal de la intimidad: privacy e informática*, Destino, Barcelona, 1984.

[620] Por todos, MURILLO DE LA CUEVA. *Informática y protección de datos personales*, Centro de Estudios Políticos y Constitucionales, Madrid, 1993.

preceptos queden abiertos al propio dinamismo de la sociedad pues, para no perder virtualidad, sus contenido debe evolucionar para adaptarse a los nuevos contextos político sociales[621].

A este respecto, PÉREZ LUÑO reivindica un indudable reconocimiento para el artículo 18.4 CE en tanto que el legislador constitucional lleva a cabo un loable intento de actualización y adecuación de la normativa constitucional a las nuevas realidades sociales que ya incidían sobre el derecho a la dignidad del ser humano así como sobre el disfrute de sus derechos[622]. De hecho, al reconocer los riesgos de la informática y obligar al legislador a imponer una delimitación de su uso, la Constitución establece las bases para el reconocimiento posterior del derecho a la protección de datos gracias, en parte, a su apertura hermenéutica.

Así las cosas, el artículo 18.4 CE debe de considerarse en un doble sentido, por una parte como un precepto instrumental destinado al deber del legislador de controlar el uso de la informática a modo de refuerzo, en primera instancia, de la intimidad y al honor y, además, del resto de derechos y libertades que pudieran verse afectados por su uso indebido. En segundo lugar, y como tal ha quedado acreditado por la jurisprudencia constitucional, como el precepto que configura un derecho fundamental autónomo, el derecho a la protección de datos personales, como medio de protección de la información personal del individuo para preservar su dignidad y el pleno ejercicio de sus derechos.

Por último, junto al artículo 18.4 CE procede mencionar el artículo 105 b) CE que consagra el principio de transparencia administrativa y con el que existen ineludibles ligámenes. Este precepto supone un medio de control de la actuación administrativa en un doble aspecto: de un lado, el control por parte de todo ciudadano que se encuentre vinculado a

[621] Sobre esta cuestión, afirma GARCÍA DE ENTERRÍA "Lo que parece asegurarla una superioridad sobre las normas ordinarias carentes de una intención total tan relevante y limitada a objetivos mucho más concretos, todos singulares dentro del marco globalizador y estructural que la Constitución ha establecido". Cfr. *La constitución como norma y el Tribunal Constitucional*, Civitas, Madrid, 2001, p. 50.

[622] Cfr. "La protección de la intimidad frente a la informática en la Constitución española de 1978" en *Revista de Estudios Políticos*, nº 9, 1979, pp. 59 ss.

un procedimiento administrativo; de otro, el de todos los ciudadanos a estar informados del funcionamiento ordinario y cotidiano de las administraciones[623].

b) La protección de datos en la legislación ordinaria:

De acuerdo con lo anterior, la fórmula "*la ley limitará el uso de la informática*" del artículo 18.4 CE exigía una actividad legislativa directa para dotar de contenido material a esta nueva vertiente del derecho de privacidad y así, determinar y regular el contenido del derecho a la protección de datos personales, el legislador lo hizo a través de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (LORTAD) que se contextualiza en el momento en que aparecieron los primeros ordenadores personales y la introducción de la informática en los hogares[624]. ORTI VALLEJO explica dicho escenario de la siguiente manera: "la amenaza de esta tecnología para los derechos de la persona, se cifra hoy en la imbricación que, desde hace tiempo, viene produciéndose entre la informática y la transmisión y flujo de datos, de cuya unión, hasta semántica, surgió la telemática (telemetría, sistemas interactivos y correo electrónico)"[625].

Los avances tecnológicos desarrollados, que permitían la recopilación de datos, y el uso masivo de las tecnologías de la información, produjeron un cambio de escenario en el que el procesamiento automatizado se tornaba imprescindible en un entorno en el cual se extraían, agregaban, y se hacían públicos un enorme volumen de datos personales, con potenciales riesgos para los derechos y libertades más fundamentales. Así, cuando apenas había comenzado la Revolución Digital ya era patente el cambio sociocultural que se avecinaba y como éste

---

[623] GARRIGA DOMÍNGUEZ. "Nuevas tecnologías, derecho a la intimidad y protección de datos personales" en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. VI, Libro II, Dykinson, Madrid, 2013, p. 912.

[624] No obstante, es criticable la dejación del legislador que no cumplió el mandato constitucional del artículo 18.4 hasta más de una década después de su entrada en vigor y que propició remedios parciales e insuficientes como la Disposición Transitoria Primera de la Ley Orgánica 1/1982, de 5 de mayo sobre Protección civil del derecho al honor, intimidad personal y a la propia imagen, derogada posteriormente con la entrada en vigor de la LORTAD, que disponía "*En tanto no se promulgue la normativa prevista en el artículo dieciocho, apartado cuatro, de la Constitución, la protección civil del honor y la intimidad personal y familiar frente a las intromisiones ilegítimas derivadas del uso de la informática se regulará por la presente ley*".

[625] Cfr. *Derecho a la intimidad e informática (tutela de la persona por el uso de ficheros y tratamientos informáticos de datos personales. Particular atención a los ficheros de titularidad privada)*, Comares, Granada, 1994, p. 19.

requería de una concordancia del Derecho que se había quedado desfasado frente a las posibilidades lesivas de las nuevas tecnologías.

Así, dadas las posibilidades informáticas de interrelacionar datos personales, se hizo necesario para proteger la privacidad desarrollar una legislación capaz de poner freno al llamado "poder informático"[626] tal y como preveía el artículo 18.4 de la Constitución. Y en este contexto, y teniendo en cuenta la existencia de normas de protección de datos de carácter personal en otros países de nuestro entorno[627] así como la existencia de una Propuesta de Directiva del Consejo de la CE, de 24 de septiembre de 1990, relativa a la protección de los datos personales y la intimidad en relación con las redes públicas de telecomunicaciones y, en particular, la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas, se aprobó la LORTAD, cuyo artículo primero disponía "*La presente Ley Orgánica, en desarrollo de lo previsto en el apartado 4 del artículo 18 de la Constitución, tiene por objeto limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos*".

Brevemente procede destacar, tal y como señalaba en su Exposición de Motivos, que dicha norma se construyó sobre el principio del consentimiento que, junto con los principios de congruencia y racionalidad, pretendía permitir a las personas autodeterminar el nivel de protección de sus datos personales. Sin embargo, dicha aspiración no se llegó a materializar ciertamente pues, las previsiones concretas de su articulado nunca atribuyeron a los sujetos de un verdadero poder de control sobre su información personal. Aunque la LORTAD parecía estar enfocada a regular los ficheros de datos de carácter personal, en su vertiente más administrativa no obstante, reconocía a los sujetos una pluralidad de derechos en torno a la gestión de sus datos: impugnación de valoraciones basadas exclusivamente en datos

[626] Cfr. ROMEO CASABONA. *Poder informático y seguridad jurídica*, Fundesco, Madrid, 1987.

[627] Entre otras, la pionera *Data Lag* sueca de 1973, la alemana *Bundesdatenschutzgesetz* de 1977, la francesa *Loi relative à l'informatique, aux fichiers et aux libertés* de 1978 o la británica *Data Protection Act 1984*, sobre la que ya se ha incidido en Capítulos anteriores.

automatizados, derecho de información, derecho de acceso, derecho de rectificación y cancelación e incluso un derecho de indemnización (artículos 12 a 17).

No obstante, esta norma no sólo establecía derechos y facultades de las personas en relación con sus datos, también recogía derechos a favor de los que utilizaban ficheros, pues en la práctica no se contemplaba un derecho general a impedir el uso de los datos ni a determinar su destino. De hecho, incluso en aquellos casos en que el uso de los datos depende de la voluntad del sujeto, una vez otorgaba el consentimiento para el uso, sólo podría éste ser revocado por causas justificadas, por los que "la autodeterminación informativa" en este caso, era un tanto limitada.

Así, la LORTAD, con el objetivo de actualizar el derecho a la privacidad y combatir el abuso informático de los datos personales combinó, por un lado, la garantía del consentimiento con carácter excluyente y, por otro, sustrajo del consentimiento a un buen número de ficheros y tratamientos de datos personales por particulares y organismos públicos[628]. Además, junto al afectado y al responsable del fichero, se contemplaba un tercer sujeto interviniente: la Agencia Española de Protección de Datos (AEPD) -art. 17-, ente independiente, con presupuesto propio y plena autonomía funcional, creado *ex novo* para la vigilancia y el control del cumplimiento de la Ley y del ejercicio de los derechos de los interesados[629].

Por último, y como ya se ha abordado en capítulos anteriores[630], la LORTAD se construyó sobre la idea de "privacidad", alejándose conscientemente de la estricta intimidad del

---

[628] Artículo 2.2. "*El régimen de protección de los datos de carácter personal que se establece en la presente Ley no será de aplicación: a) A los ficheros automatizados de titularidad pública cuyo objeto, legalmente establecido, sea el almacenamiento de datos para su publicidad con carácter general; b) A los ficheros mantenidos por personas físicas con fines exclusivamente personales; c) A los ficheros de información tecnológica o comercial que reproduzcan datos ya publicados en boletines, diarios o repertorios oficiales; d) A los ficheros de informática jurídica accesibles al público en la medida en que se limiten a reproducir disposiciones o resoluciones judiciales publicadas en periódicos o repertorios oficiales; e) A los ficheros mantenidos por los partidos políticos, sindicatos e iglesias, confesiones y comunidades religiosas en cuanto los datos se refieran a sus asociados o miembros y ex miembros, sin perjuicio de la cesión de los datos que queda sometida a lo dispuesto en el artículo 11 de esta Ley, salvo que resultara de aplicación el artículo 7 por tratarse de los datos personales en él contenidos*".

[629] No obstante, fue mediante el Real Decreto 428/1993, de 26 de marzo, que se aprobó el Estatuto de la Agencia de Protección de Datos. Por ello, la AEPD, pese a ser creada en 1992 no empezó a funcionar hasta 1994.

[630] Vid. *supra* Cap. I. 4.1.

artículo 18 CE, como disponía su Exposición de Motivos: "*Nótese que se habla de la privacidad y no de la intimidad: Aquélla es más amplia que ésta* […] *Y si la intimidad, en sentido estricto, está suficientemente protegida por las previsiones de los tres primeros párrafos del artículo 18 de la Constitución y por las leyes que los desarrollan, la privacidad puede resultar menoscabada por la utilización de las tecnologías informáticas de tan reciente desarrollo* […] *En este caso, al desarrollar legislativamente el mandato constitucional de limitar el uso de la informática, se está estableciendo un nuevo y más consistente derecho a la privacidad de las personas*".

La LORTAD fue derogada por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD), actualmente vigente, que incorporó las exigencias derivadas de la ya derogada 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[631]. Quizás las prisas por la trasposición expliquen que dicha norma no tenga Exposición de Motivos alguna así como que sea menos concreta y acotada que su predecesora.

La LOPD que, como establece el artículo primero "*tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*", con tal propósito, extiende su tutela a todos los datos de carácter personal –esto es, a toda información relativa a personas físicas identificadas o identificables registrados en suporte físico –ampliándose su contenido a los ficheros manuales estructurados- que los haga susceptibles de tratamiento así como toda modalidad de uso posterior de los mismos, tanto por entidades privadas como por el sector público.

Entre las novedades a destacar, la LOPD incorpora el principio de finalidad exigiendo que ésta sea determinada, explícita y legítima, prohibiendo el empleo de los datos para otras

[631] Actualmente derogada por el Reglamento General de Protección de Datos, esto es, 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 datos y por el que se deroga la Directiva 95/46/CE.

finalidades incompatibles con aquellas para las que hayan sido recogidos. Este principio está intrínsecamente relacionado con la noción de "compatibilidad" en tanto que, *sensu contrario*, se ha entendido que se autoriza el tratamiento de datos para usos distintos de aquéllos para los que se hubiesen recogido, siempre y cuando su finalidad no sea incompatible.

En el proceso de tratamiento de datos de carácter personal aparece una nueva figura, el encargado del tratamiento –personas físicas, jurídicas o entidades públicas-, que diverge del responsable del tratamiento en tanto que tratará lo datos por cuenta de éste, actuando directamente sobre el tratamiento, motivo por el cual es susceptible de ser sujeto pasivo para la imposición de sanciones.

Entre los derechos de los interesados, dónde se refuerza el derecho de información mediante la ampliación de las obligaciones que debe de cumplir el responsable del fichero, se incluye un nuevo derecho de oposición que permite al interesado oponerse al tratamiento de sus datos en aquellos supuestos en que no sea preciso el consentimiento para proceder al tratamiento, aunque dicho derecho se desarrolla de forma insuficiente en la Ley.

Por último, señalar que la LOPD contempla la posibilidad de crear códigos tipos de carácter deontológico por parte de los titulares de ficheros públicos, facultad que en la normativa anterior quedaba limitada a los ficheros de titularidad privada.

En términos generales, puede decirse que la LOPD no está exenta de errores y deficiencias importantes[632], sin embargo, su Reglamento de desarrollo[633], sus posteriores modificaciones derivadas de las exigencias europeas así como su necesaria interpretación por la cuantiosa jurisprudencia sobre la materia y las instrucciones de la AEPD[634], han hecho de ella una legislación mejor, aunque mantiene ciertas carencias[635].

---

[632] Y eso que el texto original presentado por el Gobierno para la adopción de la LORTAD a la Directiva europea de datos, al recibir 140 enmiendas, ocasionó la redacción de un nuevo texto legal -la LOPD- desde cero.

[633] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD) vigente en la actualidad.

[634] Procede comentar brevemente que la AEPD es una autoridad de control encargada de velar por el cumplimiento y aplicación de la legislación sobre protección de datos y, a tal efecto, tiene facultades para instruir y divulgar la normativa de

Procede mencionar asimismo que, próximamente, la LOPD se verá derogada al dictarse una nueva norma de desarrollo del precepto constitucional – la tercera, sucesivamente- que consagra la garantía de los derechos frente al uso de la informática, esto es, el Proyecto de Ley Orgánica de Protección de Datos Personales - en tramitación parlamentaria en la actualidad-, para ajustar el derecho doméstico al contenido del GDPR y en la que, por primera vez en nuestro ordenamiento jurídico, se contempla el derecho al olvido (en el artículo 15, bajo la denominación de "derecho de supresión")[636].

c) El derecho a la protección de datos como Derecho Fundamental

El hecho de que la relación entre informática y derechos de las personas fuese recogida con el máximo rango normativo supuso, en efecto, un gran avance. Sin embargo, no cabe duda de que el artífice de la creación en el Derecho español del derecho fundamental a la protección de datos personales ha sido indiscutiblemente el Tribunal Constitucional[637].

El reconocimiento del derecho a la protección de datos como derecho fundamental es relativamente reciente, pues se derivó del pronunciamiento jurisprudencial del Tribunal Constitucional en la STC 292/2000, de 30 de noviembre, que lo incorpora al ordenamiento jurídico con *status* de fundamental, como un derecho de tercera generación (o cuarta, según se trate del autor[638]).

Ello se produce por la función del Derecho de dar respuestas jurídicas a la realidad existente, pues los avances tecnológicos hasta la fecha, hacían necesario la creación de herramientas jurídicas capaces de hacer frente a los desafíos presentados por la informática, la

---

protección de datos, investigar las posibles infracciones que contra ésta se cometan, así como imponer sanciones una vez determinada la existencia de incumplimientos.

[635] Cfr. NAVALPOTRO NAVALPOTRO. "Antecedentes de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal" en *Estudio práctico sobre la protección de datos de carácter personal* (Almuzara Almaida ed.), Lex Nova, Valladolid, 2007, pp. 33 ss.

[636] "1. *El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679.* 2. *Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa*".

[637] GARRIGA DOMÍNGUEZ. *Tratamiento de datos personales y derechos fundamentales*, Dykinson, Madrid, 2009, p. 33.

[638] Sobre esta cuestión se incide en apartados posteriores, Vid. *infra* Cap. III. 5.1.

técnica y la situación de las telecomunicaciones que permitían la captación, el almacenamiento, el tratamiento y la publicidad de enormes cantidades de información personal, con las consecuencias que ello podía comportar para la protección de los derechos fundamentales de los individuos.

La aparición de Internet redimensionó dicho fenómeno al permitir la interconectividad y el intercambio masivo de información de forma instantánea y universal, aumentando exponencialmente el movimiento de los datos personales. Añadiéndose ello a la perennidad de los datos, inherente a la propia lógica del funcionamiento de la red, así como al fácil acceso a éstos y su publicidad.

Así las cosas, resultó que la legislación ordinaria no era suficientemente garantista para la protección de la privacidad de los ciudadanos, pues para una verdadera efectividad del derecho a la protección de datos devenía necesario elevar su categoría a derecho fundamental. Así lo dispuso la STC 254/1993, de 20 de julio, en la que afirma el Tribunal Constitucional "*nuestra CE 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*" (FJ 6º).

Mediante esta sentencia pionera se reconoce una faceta positiva de control a los sujetos afectados, que se integra con la facultad de impedir el uso de ciertas informaciones a terceros, a la que se añade. En palabras del TC: "*La garantía de la intimidad adopta hoy un contenido positivo en forma de la 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)*" (FJ 7º).

Esta resolución resulta de vital importancia dado su reconocimiento de la "libertad informática" o el "habeas data", como actualmente se denomina al derecho de protección de datos y porque, mediante éste, el Tribunal Constitucional admite el Convenio 108 del Consejo de Europa como referencia interpretativa para determinar el contenido mínimo del derecho a la

protección de datos: "*la realidad de los problemas a los que se enfrontó la elaboración y la ratificación de dicho tratado internacional, así como la experiencia de los países del Consejo de Europa que ha sido condensada en su articulado, 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 cuales son esos datos personales en poder de las autoridades*" (FJ 8º).

Pese a su indiscutible alcance y su carácter precursor de otras resoluciones, dicha sentencia, sin embargo, no estuvo exenta de polémica pues, si bien afirma que de lo que se trata es de tutelar derechos fundamentales ya reconocidos y defiende la sustantividad propia de un nuevo derecho fundamental, el derecho a la protección de datos[639], limita el alcance protector del artículo 18.4 a su vinculación con los derechos al honor y a la intimidad "*En el presente caso estamos ante un instituto de garantía de otros derechos fundamentalmente el honor y la intimidad*" (FJ 6º) frente a las potenciales agresiones a la dignidad y a la libertad de la persona proveniente del uso ilegítimo del tratamiento mecanizado de datos[640].

Un segundo estadio en la configuración constitucional del derecho fundamental a la protección de datos se produjo a raíz de la STC 290/2000, de 30 de noviembre, que, partiendo del Fundamento Jurídico Sexto de la sentencia anterior, afirmó que el objeto del derecho a la protección de datos no es sólo la intimidad individual, protegida por el artículo 18.1 CE, sino que alcanza a todos los datos personales públicos que no escapan al poder de disposición del afectado por el sólo hecho de ser accesibles al conocimiento de cualquiera. Es decir, reconoce el derecho a la protección de datos como un derecho fundamental, desvinculándose parcialmente de la intimidad y el honor, atendiendo a la capacidad del individuo de hacer frente

---

[639] "*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 la 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'*", FJ 6º.

[640] Cfr. VILLAVERDE MENÉNDEZ. "Protección de Datos Personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 254/1993", en *Revista Española de Derecho Constitucional*, nº 41, 1994, pp. 187 ss.

a las potenciales agresiones a su dignidad y a su libertad frente a un uso ilegítimo de sus datos personales.

En dicha resolución el Tribunal Constitucional revalida el artículo 18.4 CE como un instituto de garantía del derecho a la protección de datos que, si bien está enraizado con el derecho al honor y a la intimidad, se manifiesta además como un derecho de libertad fundamental frente a las potenciales agresiones de la informática "*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 esa posesión y uso exigiendo a quien corresponda que ponga fin a la posesión y empleo de tales datos*" (FJ 7º).

Sin embargo la mayor relevancia de dicha resolución se encuentra en el voto particular suscrito por el Magistrado JIMÉNEZ DE PARGA (al que se adhirió el Magistrado MENDIZÁBAL ALLENDE) y que supone un punto de inflexión para la configuración del derecho a la protección de datos en tanto que se lleva a cabo desde un concepto autónomo del derecho a la libertad informativa, como un nuevo derecho fundamental hasta entonces no reconocido por la Constitución: "*A mi entender, 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* […] *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*" .

Sin embargo, mientras que en sentencias anteriores, el Tribunal Constitucional ya venía afirmando que el artículo 18.4 CE consagra un derecho fundamental autónomo y diferente del derecho a la intimidad, pues "*incorpora una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de las*

personas"[641] no fue hasta la STC 292/2000, de 30 de noviembre, que el derecho a la protección de datos personales se configuró como un derecho fundamental y específico que persigue garantizar "*un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir el tráfico ilícito y lesivo para la dignidad y derechos del afectado*" (FJ 6º)[642].

Esta resolución se dicta estando en vigor tanto la LOPD como la Directiva 95/46/CE de Protección de Datos –actualmente derogada por el GDPR-, de modo que la protección de los datos personales ya era una realidad tangible en nuestro ordenamiento jurídico. En este contexto, la STC 292/2000 perfila aún más el contenido de dicho derecho, constituyéndose en un pilar para su interpretación al disociar de forma definitiva la protección de datos del derecho a la intimidad, afirmando que la tutela del artículo 18.4 CE no se reduce sólo a los datos íntimos de la persona sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no éstos fundamentales[643].

En este sentido afirma el TC: "*Este derecho fundamental a la protección de datos, a diferencia del derecho a la intimidad del art. 18.1 CE, con quien comparte el objetivo de ofrecer una eficaz protección constitucional de la vida privada personal y familiar, atribuye a su titular un haz de facultades que consiste en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos cuya concreta regulación debe establecer la Ley, aquella que conforme al art. 18.4 CE debe limitar el uso de la informática, bien desarrollando el derecho fundamental a la protección de datos (art. 81.1*

[641] STC 254/1993, de 20 de julio, FJ 6º. En el mismo sentido, entre otras, STC 11/1998, de 13 de enero o STC 202/1999, de 8 de noviembre.

[642] Ello no obstante ha sido objeto de numerosas críticas por parte de la doctrina que entienden que se ha producido una interpretación extensiva del artículo 18.4 y discrepan que de su tenor litera pueda extraerse la creación de un nuevo derecho fundamental. Por todos, Cfr. MARTÍNEZ MARTÍNEZ. *Una aproximación crítica a la autodeterminación informativa*, CIVITAS, Madrid, 2004, p. 345. En dicha obra el autor se pregunta, "*Claro está que si a una norma cuyo tenor literal comienza con la expresión 'la ley limitará' se le asigna el papel de derecho fundamental ¿Qué valor constitucional debería atribuirse al artículo 53.1 CE?"*

[643] Cfr. DEL CASTILLO VÁZQUEZ. *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*, ob. cit., pp. 310 ss.

CE), bien regulando su ejercicio (art. 53.1 CE). La peculiaridad de este derecho fundamental a la protección de datos respecto de aquel derecho fundamental tan afín como es el de la intimidad radica, pues, en su distinta función, lo que apareja, por consiguiente, que también su objeto y contenido difieran" (FJ 5º).

Así, la STC 292/2000 invoca el artículo 18.4 CE para reconocer en él la existencia de un nuevo derecho fundamental extendiendo el ámbito de la intimidad del artículo 18.1 CE hacia la protección de la privacidad, dónde se insertaría el derecho a la protección de los datos personales[644], pese a qué en ocasiones ambas figuras pueden llegar a solaparse. De este modo, se configura el respeto a la vida privada como un límite al acceso y publicidad de la información personal del individuo.

Con ello, se cierra de este modo el proceso constitucional por el que se concede plena autonomía y reconocimiento al derecho de protección de datos con rango fundamental y se ejecuta finalmente, tanto el mandato constitucional al legislador contenido en el artículo 18.4 CE, como las aspiraciones de la ciudadanía de obtener medios eficaces de garantía de sus derechos fundamentales frente al desarrollo de las nuevas tecnologías y el creciente uso de la informática.

3.3. Regulación supraestatal del derecho a la protección de datos y a la privacidad

El derecho a la protección de datos personales está reconocido en numerosos instrumentos jurídicos supraestatales, de entre los cuales se pasará a continuación a comentar los más importantes. Ello ha sido primordial para que el legislador español haya podido encontrar los cauces apropiados para desarrollar el derecho de protección de datos, tomando como fundamento las regulaciones supranacionales de referencia[645].

---

[644] Ello viene a reforzar la línea argumental que se sostiene a lo largo de esta disertación en relación con el empleo del término "privacidad" como figura más idónea para designar el ámbito de interacción del derecho a la protección de datos así como del derecho al olvido, en contraposición con la más acotada "intimidad". Vid. *supra* Cap. I. 4.1.

[645] Y, partiendo de la base de que el derecho a la protección de datos, por las razones comentadas en páginas anteriores, deviene el fundamento del derecho al olvido, una comprensión global de este último requiere un examen, aunque sea en términos generales, de las normas que han dado lugar a su aparición y que, en cierto modo, lo cimientan.

Ello debe de ponerse en relación con la hermenéutica constitucional conjunta a la interpretación de conformidad con los Tratados internacionales, ratificados por España, a partir de las directrices establecidas por el artículo 10.2 de la Constitución "*Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España*".

Mediante dicho precepto, se impone tanto al legislador como a los intérpretes jurisdiccionales, la obligación de respetar el sentido y contenido de las normas supraestatales vinculantes en nuestro territorio para desarrollar el derecho del que se trate, asumiendo la fundamentación de su legitimidad, ya no sólo en su armonía con la Constitución y bajo los criterios interpretadores de los tratados y acuerdos internacionales, sino además, favoreciendo su máxima efectividad y, en suma, la de sus normas *iusfundamentales*[646].

En este sentido, señala RALLO LOMBARTE que la constitucionalización española del fenómeno informático en sede de garantía de derechos fundamentales, debe analizarse desde una perspectiva global y comparada, pues los desarrollos legislativos más importantes de nuestro ordenamiento jurídico en dicha materia no constituyen tanto iniciativa propia nacional como el inevitable resultado de la obligación de cumplir con los compromisos internacionales adquiridos por España en el orden internacional y europeo[647]. Por ello, a continuación, pasará a examinarse los instrumentos supranacionales más importantes en dicha materia y con mayor influencia en nuestro ordenamiento jurídico[648].

a) La Declaración Universal de Derechos Humanos de 1948

[646] BASTIDA FREIJEDO *et al*. *Teoría general de los derechos fundamentales en la Constitución española de 1978*, ob. cit., pp. 60 ss.

[647] Cfr. "De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018)", ob. cit., p. 643.

[648] Se prescinden en dicha enumeración, el Reglamento europeo de Protección de datos (*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 y por el que se deroga la Directiva 95/46/CE* –GDPR-) que ya ha sido comentado en las páginas iniciales del presente Capítulo, así como la Directiva 95/46/CE de Protección de Datos en tanto que dicho instrumento no se encuentra en la actualidad en vigor, por razones de extensión.

La Declaración Universal de Derechos Humanos, de 10 de diciembre de 1948, establece como fuente primigenia en la protección de la esfera de privacidad del sujeto el art. 12, donde si bien no queda recogida una protección específica de los datos personales, se cimienta el reconocimiento como derecho fundamental de una serie de prerrogativas asociadas a la vida privada del sujeto[649]:

> "*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques*".

Si bien ésta es una declaración genérica, no cabe duda de la importancia histórica que supone el reconocimiento en la Declaración Universal de Derechos Humanos de este precepto, fundamentado en la protección de la intimidad y la vida privada. Esto es así, en la medida en que su mención en el texto establece un precedente a seguir en el resto de textos internacionales de protección de los derechos humanos. La noción de derechos humanos elaborada en el texto de 1948 permite establecer una cultura jurídica, un estándar mínimo en materia de garantía y protección de los derechos humanos. No sólo eso, sino que la importancia misma de la Declaración Universal de Derechos Humanos radica en su labor destinada a la promoción de los derechos reconocidos en su articulado, dado que la fuerza, tanto en términos positivos como simbólicos, de su contenido serviría posteriormente como influencia a otros instrumentos internacionales de protección de derechos humanos, así como en el desarrollo de las propias Constituciones estatales. De acuerdo con lo expuesto, el reconocimiento de la esfera de privacidad del sujeto en su art. 12 fue un valioso precedente para avanzar en la protección jurídica de la intimidad y la vida privada, evolucionando ésta con el paso del tiempo a la protección de datos, o el propio derecho al olvido.

b) Convenio Europeo de Derechos Humanos de 1950

[649] Cfr. DEL CASTILLO VÁZQUEZ. *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*, ob. cit, p. 82.

La protección de la esfera de privacidad del sujeto en el ámbito europeo se consagra mediante el Convenio Europeo de Derechos Humanos (CEDH), de 4 de noviembre de 1950. Dispone en su art. 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, sino en tanto en cuanto 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 del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás".*

De igual modo que lo dispuesto respecto de la Declaración Universal de Derechos Humanos, no supone este precepto un reconocimiento de la protección de los datos personal como derecho fundamental. No obstante, el art. 8 CEDH ofrece un marco legal donde la protección de la intimidad y la vida privada puede llevar al posterior desarrollo por el *case law* del Tribunal Europeo de Derechos Humanos de derechos y libertades englobados dentro del núcleo constituido por este precepto. Sobre esta cuestión, puede destacarse la posición de *living instrument* (instrumento vivo) conferida al Convenio, en la Sentencia del Tribunal Europeo de Derechos Humanos (STEDH) *Tyrer v. United Kingdom*, de 25 de abril de 1978[650]. Considerar el CEDH como un *instrumento vivo* supone reforzar, no únicamente la vigencia del texto, sino la propia protección de los derechos humanos contenidos en su articulado. Efectivamente, cuando el Tribunal de Estrasburgo desarrolla una interpretación atendiendo al objeto y propósito del Convenio, lo hace de acuerdo con la realidad cambiante propia de las sociedades democráticas de los Estados parte. De acuerdo con QUERALT JIMÉNEZ: "el CEDH es un instrumento vivo lo que necesariamente implica que su interpretación venga marcada por su objeto y finalidad: esencialmente, la protección efectiva y real de los derechos de las personas.

[650] STEDH *Tyrer v. United Kingdom*, de 25 de abril de 1978, para. 31.

Y, como ha reiterado el TEDH, la efectividad del sistema como meta supone incorporar como criterio interpretativo el del efecto útil"[651].

Siguiendo con la doctrina del *living instrument*, el reconocimiento por el art. 8 CEDH de la protección de la intimidad y la vida privada propicia el marco de referencia normativo adecuado para el posterior desarrollo jurisprudencial por el *case law* de la esfera de privacidad del sujeto. En este sentido, puede observarse la interrelación construida por el Tribunal de Estrasburgo entre vida privada y protección de datos, en el *leading case* STEDH *S. and Marper v. United Kingdom*, de 4 de diciembre de 2008[652]:

> "*el mero almacenamiento de datos personales, relacionados con la vida privada de un sujeto equivale a una inferencia en el sentido del art. 8, que garantiza el derecho al respeto de la vida privada y familiar (...) el uso posterior de los datos almacenados no tiene relación con esa obtención. Sin embargo, al determinar si la información personal retenida por las autoridades abarca cualquier aspecto de la vida privada (...) el tribunal tendrá en cuenta el contexto específico en el que se ha registrado y conservado la información, la naturaleza de los registros y la forma en que éstos se utilizan y procesan, así como los resultados que se pueden obtener*".

Así las cosas, la STEDH *S. and Marper v. United Kingdom* supone un reconocimiento expreso del derecho a la protección de datos por parte del TEDH, en tanto que éste se deriva del reconocimiento en el art. 8 CEDH de la vida privada y la intimidad como bienes a proteger dentro del estándar de garantía desarrollado por el Convenio como sistema de protección de derechos y libertades en el ámbito europeo. Por lo que respecta al reconocimiento del derecho al olvido, si bien éste todavía no ha sido desarrollado dentro del *case law* del Tribunal de

---

[651] Cfr. "La recepción constitucional del estándar europeo sobre garantías en el proceso penal", en *Garantías constitucionales y Derecho penal europeo* (Mir Puig/Corcoy Bidasolo Dirs.), Marcial Pons, Barcelona, 2012, p. 227.

[652] STEDH *S. and Marper v. United Kingdom*, de 4 de diciembre de 2008, para. 67. No obstante, pueden mencionarse otros casos donde el Tribunal de Estrasburgo ha desarrollado el derecho a la protección de datos a partir de la garantía de la intimidad y la vida privada recogida en el art. 8 CEDH: STEDH *Gaskin v. United Kingdom*, de 7 de julio de 1989; STEDH *Z v. Finland*, de 25 de febrero de 1997; STEDH *Amann v. Switzerland*, de 16 de febrero de 2000; STEDH *Rotaru v. Romania*, de 4 de mayo de 2000; STEDH *L.L. v. France*, de 10 de octubre de 2006.

Estrasburgo, si puede traerse a colación un caso donde se ve indirectamente afectado, en concreto, la STEDH *Copland v. United Kingdom*, de 3 de abril de 2007, donde se reconoce en los siguientes términos de qué manera el almacenamiento masivo de datos puede ser contrario al art. 8 CEDH[653]:

> *"este Tribunal considera que la obtención y almacenamiento de datos personales obtenidos sin el conocimiento previo del sujeto, a partir de su teléfono móvil o su cuenta de correo electrónico, supone una interferencia en el disfrute de su esfera personal de privacidad".*

Esta interpretación del art. 8 CEDH supone entender incluido dentro del derecho a la vida privada el propio control de la información personal obtenida por terceros, pudiendo así limitarse de forma extensiva las posibles interferencias en la esfera de privacidad del sujeto dentro del contexto *Big data*. Partiendo de estos presupuestos, sería necesario que el Tribunal Europeo de Derechos Humanos avanzara en esta dirección para desarrollar en futuros pronunciamientos el derecho al olvido[654], partiendo en todo caso de los fundamentos establecidos en el art. 8, de forma que la posición del Convenio como *instrumento vivo* permitiera un desarrollo de su articulado que viniera a reconocer el derecho al olvido.

c) Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal

Como se ha dispuesto en el apartado anterior, el art. 8 CEDH no contiene un reconocimiento expreso del derecho a la protección de datos personales. Si bien es cierto que el posterior desarrollo jurisprudencial por el *case law* del Tribunal de Estrasburgo ha reconocido este derecho como parte integrante de la protección jurídica de la intimidad y la vida privada, el Consejo de Europa desarrolló previamente un instrumento normativo que de forma expresa estableciera unos mínimos de calidad respecto del tratamiento de los datos de carácter personal de sus ciudadanos, mediante el reconocimiento de los principios de tratamiento leal y legítimo,

[653] STEDH *Copland v. United Kingdom*, de 3 de abril de 2007, para. 44.

[654] Cfr. MARTÍNEZ LÓPEZ-SÁEZ. *Una revisión del derecho fundamental a la protección de datos de carácter personal. Un reto en clave de diálogo judicial y constitucionalismo multinivel en la Unión Europea*, Tirant lo Blanch, 2018, p. 145.

de veracidad, de seguridad y finalidad, así como garantizando la posibilidad de que dichos sujetos tuviesen conocimiento de la existencia de los ficheros en los que se contuviesen[655]. De este modo, la importancia del Convenio 108 radica, no sólo en su posición de preeminencia en la normativa supraestatal respecto del derecho a la protección de datos personales, sino también en la construcción de este derecho a partir de la protección jurídica de la intimidad y la vida privada, reconociendo de esta manera un concepto extensivo de privacidad donde se entienden comprendida la protección de los datos de carácter personal. Así las cosas, la adaptación del Convenio supuso un importante punto de partida para el desarrollo de un marco legal europeo en lo relativo al tratamiento de datos personales, además de para la cooperación entre Estados y la armonización de las distintas legislaciones nacionales.

El Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, fue ratificado por España el 27 de enero de 1984[656]. El Consejo de Europa desarrolló este texto motivado por la posición sustancial representada por la privacidad en el ejercicio de otros derechos, como por ejemplo la libertad de expresión. En su redacción estuvo también implicada la Unión Europea, de forma que se pretendía con este instrumento desarrollar una función armonizadora, siendo muestra palpable de ésta el hecho de que todos los Estados de la Unión Europea sean parte del Convenio[657]. En su art. 1, bajo la rúbrica "objeto y fin", se ofrece una síntesis de la finalidad y criterios orientadores del Convenio:

---

[655] Cfr. GUDÍN RODRÍGUEZ-MAGARIÑOS. *Nuevo reglamento europeo de protección de datos versus big data*, Tirant lo Blanch, Valencia, 2018, p. 62.

[656] De acuerdo con RALLO LOMBARTE: "no cuesta imaginar que el proceso de gestación del que acabaría siendo el primer instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos se inició suficiente tiempo atrás para ubicarse en el contexto temporal en el que los constituyentes españoles apostaron por constitucionalizar el artículo 18.4 CE. Una razón adicional para considerar razonable el anclaje en el artículo 18.4 CE del derecho a la protección de datos personales frente al uso de la informática". Cfr "De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018)" ob. cit., p. 648.

[657] Como señala MARTÍNEZ LÓPEZ-SÁEZ, respecto de las razones que motivan la elaboración del Convenio 108: "su elaboración y posterior adopción fue la manifestación de que la mayoría de los ordenamientos jurídicos nacionales en Europa compartían los mismos principios fundamentales en relación con la protección de datos, y, al mismo tiempo, existían disparidades impropias de los objetivos comunes de unidad y protección de los derechos humanos manifestados como unión". Cfr. *Una revisión del derecho fundamental a la protección de datos de carácter personal*, ob. cit., p. 65.

"El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o 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 (protección de datos)"

De acuerdo con el art. 2 del Convenio, relativo a las definiciones, se entiende como "datos de carácter personal" cualquier información relativa a una persona física identificada o identificable. Asimismo, la referencia a "fichero automatizado" significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado, entendiendo así las operaciones efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados. Dentro de éstas se comprenden el registro de datos, la aplicación a esos datos de operaciones lógicas aritméticas, así como su modificación, borrado, extracción o difusión. Finalmente, el Convenio 108 reconoce la figura de la "autoridad controladora del fichero", la cual viene referida a la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cual será la finalidad del fichero automatizado, así como las categorías de datos de carácter personal que deberán registrarse y las operaciones que a éstas se les aplicarán.

A partir de estos presupuestos estructurales, el Convenio refuerza la protección de datos mediante el desarrollo de una serie de principios fundamentales reconocidos universalmente, a la vez que establece normas jurídicamente vinculantes y procura la implementación de disposiciones que, atendiendo a un estándar mínimo en lo relativo al desarrollo tecnológico de los Estados parte, pueda ser adaptable a los distintos marcos legales internacionales, teniendo además una incidencia tanto en el ámbito público como privado[658]. En este sentido, puede destacarse lo dispuesto en el art. 5 del Convenio, relativo a la "calidad de los datos". Este precepto determina que los datos personales que sean objeto de tratamiento deben adecuarse a

[658] Cfr. QUESADA. *Protección de datos y telecomunicaciones convergentes*, Agencia Española de Protección de Datos, Madrid, 2015, p. 259. RALLO LOMBARTE señala de qué manera "los miedos originales sobre los registros públicos dieron paso a la necesidad de garantizar la protección de datos también frente a los tratamientos automatizados del sector privado". Cfr. "De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018)", ob. cit., p. 648.

los siguientes parámetros para garantizar su validez: se obtendrán y tratarán leal y legítimamente; se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; serán exactos y si fuera necesario puestos al día; se conservarán bajo una forma que permita la identificación de las personas concernidas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado. De este modo, el Convenio positiviza una serie de criterios que sirven como estándar para la protección de la privacidad en el proceso de tratamiento y análisis de los datos masivos.

No obstante, la protección que mediante el Convenio 108 pretende dispensarse a los datos personales debe ser complementaria con el respeto a la libertad de información sin fronteras, especialmente respecto de la extensión de ésta en el ámbito informático, a consecuencia del *Big data.* Como indica DEL CASTILLO VÁZQUEZ, esta protección será entendida en dos direcciones secantes: "de un lado, su tutela se dirige a preservar la vida privada de la persona concernida a través de lo que venimos llamando autodeterminación informativa o derecho a disponer de los datos propios, mediante el libre consentimiento del interesado para que terceros puedan proceder a su acopio, uso, tratamiento y cesión. El Derecho examinado implica, en consecuencia, la posibilidad de solicitar el acceso, la ratificación o cancelación de la información objeto de la tutela que obre en los ficheros (…) de otro lado el *habeas data* protege la llamada libertad informática, en su manifestación de la libertad personal a través de la cual se garantiza la igualdad y el trato no discriminatorio"[659].

Siguiendo con el tratamiento de los datos personales, resulta de interés en lo relativo al contexto del *Big data*, lo dispuesto en el art. 6 del Convenio, en tanto que establece un régimen más estricto respecto de los datos de carácter sensible:

> "*Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos*

[659] *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*, ob. cit., p. 88.

de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales".

Como puede apreciarse, se trata de datos personales que se encuentran especialmente vinculados a la esfera de privacidad del sujeto, siendo igualmente decisivos para el desarrollo de la libre personalidad de la persona, así como para el ejercicio de derechos y libertades públicas, como la libertad ideológica, sexual o religiosa. En caso de que las disposiciones del Convenio sean transgredidas, tanto en el tratamiento genérico de datos, como en el supuesto de los datos de carácter sensible recogidos en el art. 6, el art. 10 faculta a los Estados parte a la adopción de las sanciones convenientes atendiendo a su propio derecho interno.

Asimismo, en los arts. 18 y ss. del Convenio 108 se desarrolla la composición y funciones de un Comité Consultivo encargado, entre otras tareas, de presentar propuestas con el fin de facilitar o de mejorar la aplicación del Convenio, presentar propuestas de enmienda, formular su opinión respecto de cualquier otra propuesta de enmienda o, siempre a petición de los Estados parte, expresar su opinión acerca de cualquier cuestión relativa a la aplicación del Convenio (art. 19). Como dispone GUDÍN RODRÍGUEZ-MAGARIÑOS "la actividad del comité a lo largo de los más de treinta años de actividad se ha plasmado en la elaboración de numerosos informes, opiniones y estudios, así como en la preparación de Recomendaciones del Comité de Ministros del Consejo sobre cuestiones como la protección de datos en el entorno de las redes sociales, la elaboración de perfiles o el ámbito laboral"[660].

El Convenio ha sido posteriormente desarrollado mediante el Protocolo adicional al Convenio 108 del Consejo de Europa, del 8 de noviembre de 2001. Éste se centra en lo relativo a las autoridades de control y los flujos transfronterizos, procurando mejorar y readaptar la aplicación de los principios orientadores del Convenio, mediante la inclusión de provisiones

[660] Cfr. *Nuevo reglamento europeo de protección de datos versus big data*, ob. cit., p. 63.

vinculantes frente al incremento en el intercambio de datos personales causado por los mercados globalizados y el progreso tecnológico[661].

Por lo que respecta a las "autoridades de control" (art. 1), el Protocolo permite a los Estados parte determinar que una o más autoridades sean responsables de asegurar la conformidad de las medidas oportunas que den cumplimiento en el Derecho interno a los principios orientadores del Convenio, disponiendo dichas autoridades de poderes de investigación y de intervención, así como del poder de iniciar procedimientos legales o de dirigirse a las autoridades judiciales correspondientes en relación con violaciones de Derecho interno. Asimismo, la autoridad de control conocerá de las reclamaciones presentadas por parte de cualquier persona relativas a sus derechos y libertades fundamentales con respecto al tratamiento de datos personales y dentro de sus respectivas competencias. Pasando a la "transferencia de datos personales a destinatarios no sometidos a la competencia de las Partes del Convenio" (art. 2), el Protocolo determina que cada Estado parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es Parte del Convenio se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección, sin que sea necesario asegurar este estándar mínimo de protección si el derecho interno así lo establece a causa de los intereses concretos del afectado, intereses legítimos -especialmente los de carácter público- o de acuerdo con clausulas contractuales en las que se recogen las garantías suficientes por parte del responsable del tratamiento de la transferencia, siempre que dichas garantías sean estimadas adecuadas por las autoridades competentes de acuerdo con el derecho interno.

d) Ámbito comunitario: regulación en los Tratados de la Unión Europea

Si bien la normativa comunitaria en materia de protección de datos es especialmente rica dado el carácter transversal de ésta, nos limitaremos en este apartado a la presentación del marco genérico donde queda reconocido para el ámbito de la Unión Europea el derecho a la protección de datos de carácter personal. A partir de este marco legal se ha asentado el

[661] Cfr. QUESADA. *Protección de datos y telecomunicaciones convergentes*. ob. cit., pp. 260-261.

reconocimiento internacional y comunitario de la protección de datos y la esfera de privacidad del sujeto, derivándose indirectamente de esta atmosfera el desarrollo del derecho al olvido. No obstante, existen otros muchos instrumentos, principalmente en el ámbito europeo, que de forma directa o indirecta inciden en la configuración del derecho a la protección de datos y que, por razones de extensión, no resulta oportuno comentar[662].

Así las cosas, partiendo del art. 6 del Tratado de la Unión Europea, en la última versión posterior a la aprobación y ratificación del Tratado de Lisboa[663], queda establecido el siguiente sistema de protección de los derechos y libertades:

[662] Sólo en el ámbito de la Unión Europea, se encuentran actualmente en vigor más de medio centenar de normas relativas a la protección de datos, entre las cuales puede destacarse: Directiva 2016/681 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave; Directiva 2002/58/CE sobre privacidad y comunicaciones electrónicas; Reglamento 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos; Reglamento 767/2008 sobre el Sistema de Información de Visados (VIS) y el intercambio de datos sobre visados de corta duración entre los Estados miembros; Reglamento 603/2013 relativo a la creación del sistema «Eurodac» para la comparación de las impresiones dactilares para la aplicación efectiva del Reglamento 604/2013 y por el que se modifica el Reglamento 1077/2011, por el que se crea una Agencia europea para la gestión operativa de sistemas informáticos de gran magnitud en el espacio de libertad, seguridad y justicia; Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión; Directiva (UE) 2016/943 relativa a la protección de los secretos comerciales; Reglamento (UE) 2016/794 relativo a la Europol y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo; Reglamento 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE; Directiva 2013/40/UE relativa a los ataques contra los sistemas de información y por la que se sustituye la Decisión marco 2005/222/JAI del Consejo; Directiva 2010/40/UE por la que se establece el marco para la implantación de los sistemas de transporte inteligentes en el sector del transporte por carretera y para las interfaces con otros modos de transporte Texto pertinente a efectos del EEE; Reglamento 390/2009 por el que se modifica la Instrucción consular común dirigida a las misiones diplomáticas y oficinas consulares de carrera en relación con la introducción de identificadores biométricos y se incluyen disposiciones sobre la organización de la recepción y la tramitación de las solicitudes de visado; Reglamento 80/2009 por el que se establece un código de conducta para los sistemas informatizados de reserva y por el que se deroga el Reglamento (CEE) n o 2299/89 del Consejo; Reglamento 437/2003 relativo a las estadísticas de transporte aéreo de pasajeros, carga y correo; Directiva 2003/98/CE relativa a la reutilización de la información del sector público; Directiva 96/9/CE sobre la protección jurídica de las bases de datos.

[663] Tratado de Lisboa, por el que se modifican el Tratado de la Unión Europea y el Tratado Constitutivo de la Comunidad Europea (2007/C 306/01), firmado el 13 de diciembre de 2007. Conviene recordar que este Tratado, que entró en vigor a finales del 2009, surgió como reacción al fracasado intento de crear una Constitución Europea en 2004. En cuanto a sus características principales, mediante la modificación de los Tratados de Maastricht y Roma, se puso fin a la separación que venían conformando los tres pilares básicos de la Unión (las Comunidades Europeas, la política exterior y de seguridad común –PESC- y la cooperación en materia de justicia e interior –JAI-) confiriendo nuevas competencias legislativas al Parlamento Europeo para tratar de igualarlo al Consejo de Ministros, y dotó a la Unión Europea de personalidad jurídica propia para firmar acuerdos internacionales.

"1. La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados. Las disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados. Los derechos, libertades y principios enunciados en la Carta se interpretarán con arreglo a las disposiciones generales del título VII de la Carta por las que se rige su interpretación y aplicación y teniendo debidamente en cuenta las explicaciones a que se hace referencia en la Carta, que indican las fuentes de dichas disposiciones.

2. La Unión se adherirá al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Esta adhesión no modificará las competencias de la Unión que se definen en los Tratados.

3. Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales".

Este precepto estable el marco de referencia genérico para la protección de los derechos y libertades en el ámbito comunitario. En primer lugar, su apartado primero reconoce los derechos y libertades recogidos en la Carta de los Derechos Fundamentales de la Unión Europea, sobre la que se incidirá más adelante, ocupando ésta un lugar de preeminencia como declaración de derechos propia del ámbito comunitario. En segundo lugar, los apartados segundo y tercero suponen reconocer la adhesión de la Unión Europea al Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, siendo así reafirmada por el art. 6 TUE la competencia y legitimidad del sistema de protección de derechos y libertades propio del Consejo de Europa como muestra de una cultura jurídica europea basada en la protección de los derechos humanos. Asimismo, supone reconocer la

competencia del Tribunal de Estrasburgo para la interpretación-aplicación de las disposiciones del Convenio, como se ha expuesto respecto de la doctrina del *living instrument*[664], adaptando ésta a las necesidades evolutivas en el ámbito comunitario.

Una vez descrito el régimen general relativo al sistema de protección de los derechos y libertades propio del ámbito de la Unión Europea regulado en el art. 6 TUE, pueden considerarse otras disposiciones de naturaleza comunitaria que de forma específica recogen el derecho a la protección de los datos personales. Siguiendo con el TUE, puede citarse su art. 39:

> *"De conformidad con el artículo 16 del Tratado de Funcionamiento de la Unión Europea, y no obstante lo dispuesto en su apartado 2, el Consejo adoptará una decisión que fije las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del presente capítulo, y sobre la libre circulación de dichos datos. El respeto de dichas normas estará sometido al control de autoridades independientes".*

Para complementar este art. 39 TUE, procede mencionar el art. 16 del Tratado de Funcionamiento de la Unión Europea (TFUE):

> *"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*

[664] Vid. *supra* Cap. III. 3.3. b)

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".

Como puede observarse tras la lectura de ambos preceptos, el art. 39 TUE y 16 TFUE son fundamentales para garantizar un lugar de preeminencia a la protección de datos en el ámbito comunitario. Asimismo, resultan de especial importancia las referencias introducidas al Parlamento y Consejo Europeo, para que desarrollen los instrumentos normativos necesarios para garantizar el derecho a la protección de datos. En este sentido, puede reconocerse el punto de partida para normativo para la posterior aprobación del GDPR.

e) La Carta de Derechos Fundamentales de la Unión Europea

En Diciembre de 2000, los tres órganos europeos con funciones legislativas, esto es, la Comisión Europea, el Parlamento Europeo y el Consejo acordaron en Niza un documento llamado Carta de Derechos Fundamentales de la Unión Europea (CDFUE). La Carta tiene como objetivo reivindicar el carácter fundamental de los derechos que en ella se recogen, así como dotarlos de una mayor fuerza jurídica. Esta valor jurídico se alcanzó en el año 2009 cuando, mediante el Tratado de Lisboa, se otorgó fuerza vinculante a la Carta de Derechos Fundamentales, pasando ésta a formar parte del Derecho primario de la Unión.

La Carta de Derechos Fundamentales se ha convertido en un instrumento fundamental para el desarrollo de la protección en materia de datos personales. Por un lado, porque el art. 8 reconoce el derecho a la protección de datos personales de forma autónoma, independiente del derecho a la vida privada, recogido específicamente en el art. 7. De acuerdo con lo expuesto, los arts. 7 y 8 disponen lo siguiente:

Art. 7

"*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones*".

Art. 8

"1. Toda persona tiene derecho a la protección de los datos de carácter personal que le 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 le conciernan y a obtener su rectificación.

3. El respeto de estas normas estará sujeto al control de una autoridad independiente".

La importancia del reconocimiento autónomo de la protección de datos personales en el art. 8, además de su propia consagración en la declaración de derechos y libertades propia del ámbito comunitario, radica en que bajo el amparo de este precepto se ha desarrollado una abundante jurisprudencia que ha perfilado los límites y desarrollado sustancialmente su contenido.

Por lo tanto, cerrando en este punto la exposición sobre la normativa comunitaria reguladora del derecho a la protección de datos personales, puede seguirle lo dispuesto por RALLO LOMBARTE cuando considera de qué manera los artículos 6 TUE, 8 CDFUE y 16 TFUE "crearon una *nueva base jurídica* para la elaboración de una normativa global de la Unión Europea sobre protección de datos personales"[665]. A partir de dicho sostén jurídico, cabe la posibilidad de que la jurisprudencia comunitaria desarrolle el contenido del derecho al olvido, pudiendo de esta manera ampliar de forma sustancial el significado dado al derecho a la protección de datos personales en los instrumentos citados.

[665] Cfr. "De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018)", ob. cit., p. 660.

4. Concepto

A grandes rasgos, podemos decir que el derecho al olvido tiene como finalidad proteger la privacidad de las personas frente a los retos que han propiciado la aparición de las nuevas tecnologías en connivencia con el *Big data* e Internet. Es la respuesta que se ofrece desde el Derecho a los usuarios de la Red para que puedan suprimir cualquier información personal por la cual se vea afectada su privacidad, logrando una protección efectiva del derecho a la protección de datos lo que, a su vez, evita prácticas discriminatorias en torno a éstos.

Aunque, bien podría decirse que el derecho al olvido (*The right to be forgotten* en inglés, también conocido como *The right to oblivion*, el *Droit à l'oubli* en francés o el *Diritto al'oblio* en italiano) tiene ya un cierto recorrido histórico, aún adolece de carácter novedoso, por lo que todavía no nos encontramos ante un concepto jurídico "pacíficamente delimitado"[666] de hecho, podría decirse que es un concepto todavía en evolución, pues según se va sucediendo su positivización en las distintas normas así como se van dictando resoluciones jurisdiccionales al respecto –nacionales y supraestatales-, se concreta su objeto y añaden notas definitorias.

Es por ello que la doctrina ofrece múltiples soluciones, por ejemplo, DE TERWANGNE define el derecho al olvido como "el derecho de las personas físicas a hacer que se borre la información sobre ellas después de un periodo de tiempo"[667] otros autores menos acordes con el uso del término "derecho al olvido" hacen de su concepción una reivindicación, como ejemplo, el "derecho a retirarse del sistema y eliminar la información personal que la Red contiene"[668]. Existen también definiciones más creativas como la de SIMÓN CASTELLANO que define el derecho al olvido como el "derecho a equivocarse y volver a empezar", argumentando su necesaria contextualización en un Estado democrático de Derecho que permite a sus ciudadanos ser dueños de su futuro y reinventarse tantas veces como deseen, cuyo ordenamiento jurídico disocia y protege los datos personales que contienen las

[666] RALLO LLOMBARTE. *El derecho al olvido en Internet. Google versus España*, ob. cit, p. 17.

[667] Cfr. "Privacidad en Internet y el derecho a ser olvidado", *Revista de Internet, Derecho y Política*, nº 13, 2012, p. 54.

[668] PAZOS CASTRO. "El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, una relación imposible?", *InDret*, 2015, nº 1, p. 14.

resoluciones judiciales, apoya la reinserción social de los presos, reconoce las amnistías, y que tutela el derecho a la dignidad humana y el libre desarrollo de la personalidad[669].

En cuanto a sus orígenes, nos remiten al discurso pronunciado por la vicepresidenta de la Comisión Europea, VIVIANE REDDING, en el marco de la Conferencia sobre protección de datos y privacidad que presentaba el derecho al olvido del siguiente modo "*I want to introduce 'the right to be forgotten'. Social network sites are a great way to stay in touch with friends and share information. But if people no longer want to use a service, they should have no problem wiping out their profiles. The right to be forgotten is particularly relevant to personal data that is no longer needed for the purposes for which it was collected. This right should also apply when a storage period, which the user agreed to, has expired*"[670].

Sin embargo, la primera referencia al derecho al olvido la encontramos en la anteriormente citada STJUE del *caso Google*[671], que reconoció por vez primera el derecho al olvido, configurándolo como la potestad de todo interesado de solicitar que se bloqueen en las listas de resultados de los buscadores web los enlaces que conduzcan a informaciones que le afecten y que resulten obsoletas, incompletas, falsas o irrelevantes y no sean de interés público o incurran en otras circunstancias excepcionales. Sin embargo, esta denominación que vincula su definición a su contenido, es muy incipiente y, como se analizará en apartados posteriores del presente trabajo, en la actualidad el objeto y alcance del derecho al olvido ha sido ampliado notablemente.

El Grupo de Trabajo del Artículo 29 (GT29), con la intención de hacer las pertinentes aclaraciones respecto de la STJUE del *caso Google* y armonizar ciertos criterios sobre la aplicación del derecho al olvido dispuso acerca de éste, que se trata del "derecho a dificultar la localización de datos personales en Internet, con independencia de que su cancelación por el

---

[669] Cfr. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, ob. cit., p. 292.

[670] REDING, Viviane. "Privacy matters – Why the EU needs new personal data protection rules", *The European Data Protection and Privacy Conference*, 2010.

[671] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

editor de los mismos no haya podido ser instado con éxito por su titular, por lo que dichos datos pueden seguir estando disponibles para toda persona que vaya a la fuente sin intermediación de un motor de búsqueda"[672], contenido hoy ampliado considerablemente.

El artículo 17 del GDPR, texto normativo que recoge de forma pionera dicho derecho, lo define como el "derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales" siempre y cuando concurran ciertas circunstancias. No obstante, la denominación del derecho al olvido fue asimismo un punto de constante debate durante la tramitación de la Propuesta de Reglamento, que fue variando a lo largo del tiempo hasta dar con una solución definitiva.

Originalmente, en la redacción de la Propuesta de Reglamento presentada por la Comisión Europea el 25 de enero de 2012, el artículo17 se titulaba "derecho al olvido y la supresión", seguidamente, el Parlamento Europeo, en resolución de 12 de marzo de 2014, rechazó esta denominación dejándola sólo en "derecho de supresión". En el curso de las negociaciones, el Consejo de la UE, por su parte, mediante documento de 15 de junio de 2015, abogó por mantener la denominación de derecho al olvido y a la supresión, y este último texto fue el que mantuvo un mayor peso en la redacción final del GDPR.

La solución a la que se llegó finalmente, como es sobradamente conocida, fue de carácter mixto, denominando esta nueva prerrogativa como "derecho de supresión" e incorporando entre paréntesis su denominación más popular de "derecho al olvido", quizás para reforzar la idea de que este nuevo derecho expresamente reconocido deriva de la evolución de los clásicos derechos de protección de datos, de oposición y cancelación, al compás de la propia evolución de las nuevas tecnologías[673]. Ciertamente, el empleo de la expresión "derecho al olvido", aunque más coloquial, parece más oportuna en tanto que ilustra la motivación

[672] *Guidelines on the implementation of the court of justice of the european unión judgement on "Google Spain and Inc. v. AEPD and Mario Costeja González*", de 26 de noviembre de 2014. Documento disponible online: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

[673] ÁLVAREZ CARO. "El derecho de supresión o al olvido", en *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (Piñar Mañas dir.), Reus, Madrid, 2016, pp. 243-245.

principal que ha dado lugar a su origen, esto es, combatir la perennidad de los datos personales en Internet, cuya memoria *a priori* es ilimitada.

Así, podríamos definir el derecho al olvido como el derecho al borrado digital de hechos pasados que tiene toda persona que se haya sentido vulnerada en su derecho a la privacidad, debido a causas justificadas o porque con el paso del tiempo sus datos personales han perdido su virtualidad. No debe confundirse el derecho al olvido como el derecho a configurar un pasado a medida, obligando a los editores de páginas web o a los motores de búsqueda a suprimir aquellos resultados o contenidos digitales que no quieran verse asociados a una persona, pero sí que supone un límite a la memoria eterna de Internet, dónde el tiempo es lineal y no se distingue entre pasado y presente lo que provoca en muchos casos, bien por el transcurso del tiempo, bien por la descontextualización, una vulneración de los derechos fundamentales del afectado, pudiendo perjudicar seriamente el libre desarrollo de su personalidad y hasta su dignidad personal.

Se trata pues de un interés jurídicamente protegido consistente en lograr que los datos personales de un individuo no sean accesibles al resto de personas en la Red, con independencia del perjuicio efectivamente causado o de si éstos son exactos o ciertos, sino porque no existe ningún fin lícito que legitime la disponibilidad de dichos datos por parte de terceras personas. El significante de "olvido", asimismo, alude al transcurso del tiempo como factor inherente a su ejercicio, como así se ha establecido por la jurisprudencia.

En definitiva, el derecho al olvido representa, en última instancia, una reacción frente al hecho de que información de nuestro pasado pueda ser utilizada y conocida en el presente para una finalidad diferente de aquélla para la que inicialmente fue recogida, con independencia de que mediare o no el consentimiento del interesado[674].

[674] ARENAS RAMIRO. "Reforzando el ejercicio del derecho a la protección de datos" en *Hacia un nuevo Derecho europeo de Protección de Datos* (Rallo Lombarte/García Mahamut eds.), Tirant lo Blanch, València, 2015, p. 335.

5. Naturaleza jurídica

A la hora de definir la naturaleza del derecho al olvido, y pese a las diversas y numerosas teorías en torno a la categorización de los derechos, nos decantamos por su configuración conforme a las esencias que a continuación se pasarán a examinar y que de ningún modo son excluyentes, sino que determinan facetas distintas del mismo derecho al olvido de mayor a menor concreción. Así, desgranando el derecho al olvido, podemos decir que se trata de un derecho humano, un derecho fundamental, un derecho subjetivo y un derecho de la personalidad[675].

Sin embargo, esta clasificación obedece a un criterio puramente académico, metodológico si se quiere, pero que en ningún caso puede abordarse por separado ya que su tratamiento moderno requiere de cierta unidad. Como señaló MONTÉS PENADÉS, la tutela de la personalidad se perfila como un problema unitario pues se trata de fenómenos jurídicos que ontológicamente sólo tienen una respuesta, al constituir las prerrogativas más elementales de la persona humana en las sociedades civilizadas[676].

5.1. Derecho Humano

El término "derecho humano" tiene diversas acepciones en función de la teoría filosófico-jurídica que se acoja para la fundamentación de los mismos. Así, mientras que muchos autores emplean el término "derecho humano" como sinónimo de "derecho fundamental"[677], otra parte de la doctrina, con la que nos identificamos, entiende que la diferencia entre ambas categorías estriba en que los derechos humanos son aquellos que así se

[675] Existen múltiples tipologías de clasificación de los derechos humanos, la mayoría de ellas con un valor meramente académico, sin embargo, en el presente trabajo se ha procedido a una catalogación en base a categorías concretas cuya inserción en las mismas lleva aparejadas importantes consecuencias jurídicas que permiten tratar aspectos clave en la configuración y comprensión del derecho al olvido.

[676] "No existen diferencias conceptuales entre los términos derechos humanos, fundamentales y de la personalidad […] el tema terminológico es un producto histórico". Cfr. *Derecho civil*, Tirant lo Blanch, València, 1992, pp. 34-36.

[677] Cfr. FERRAJOLI. *Derechos y garantías. La ley del más débil*, Trotta, Madrid, 2004.

declaran en Tratados internacionales mientras que los derechos fundamentales son aquéllos derechos humanos recogidos en el ordenamiento jurídico interno[678].

Con la formulación de derecho humano, nos referimos al ámbito de garantía -un mínimo denominador común- necesario para la realización del ser humano en su plenitud, comprendiendo aquí aquellas necesidades o intereses inherentes a todo ser humano para poder emanciparse, realizarse a si mismo en condiciones de libertad, igualdad y dignidad, teniendo en cuenta que el ser humano convive en sociedad y es interdependiente, lo que impide dotar a los derechos humanos de un valor absoluto. Dichos intereses son consustanciales a la condición de persona, lo que los convierten en derechos universales, cuya aspiración resulta generalizable y libre de todo subjetivismo, se convierten por tanto en objetivos jurídicamente protegidos para todos los seres humanos, con independencia de las concretas características del ordenamiento jurídico al que cada persona esté sometido.

Los derechos humanos nacen tras la Segunda Guerra Mundial y encontramos su contenido en distintos tratados internacionales como la Declaración Universal de los Derechos Humanos de 1948 o incluso regionales, como el Convenio Europeo de Derechos Humanos de 1950. Estos instrumentos jurídicos consagran unos acuerdos de mínimos sobre lo que se consideran unos valores comunes y básicos, un estándar digno de protección de toda persona, universalmente propugnado y en todo caso.

Si en el inicio de los derechos humanos, éstos encontraron su fundamento en la libertad individual como medio para limitar la acción del poder, consistiendo la *primera generación* de derechos humanos en libertades civiles y políticas (derecho a la vida, a la seguridad, al voto, a la huelga…), en la *segunda generación* se consolidaron los derechos económicos, sociales y culturales (derecho a la salud, a la educación, al trabajo…) cuyo objetivo principal era garantizar unas condiciones de vida dignas para todos los ciudadanos, todo ello sobre la idea de igualdad.

[678] Sin embargo no se trata de compartimentos estancos sino de unos mismos derechos, con igual contenido y finalidad, protegidos en distintas normas jurídicas. Muestra de ello es el artículo 10.2 CE que obliga a interpretar los derechos fundamentales "*de conformidad con la Declaración Universal de los Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España*".

En la actualidad se puede sostener la creencia de que nos hallamos ante una *tercera generación* de derechos humanos complementadora de las fases anteriores, referidas a las libertades de signo individual y a los derechos económicos, sociales y culturales. Este tercer estadio de protección se construye sobre la consideración de las necesidades e intereses del ser humano como un todo[679], y adaptadas al contexto actual, lo que conlleva la reconstrucción de las libertades, que dejan de ser ideas abstractas que se agotan "en y para sí mismas", para devenir derechos humanos que se realizan "con" los demás y "en" un contexto social e histórico determinado[680].

Esta nueva generación, aglutina derechos y libertades que se presentan como una respuesta al fenómeno de la "contaminación de las libertades" (*liberties pollution*), término con el que algunos sectores de la teoría social anglosajona aluden a la erosión y degradación que aqueja a los derechos fundamentales ante determinados usos de las nuevas tecnologías[681].

Partiendo de esta concepción, el derecho al olvido, en concreto, podría encasillarse dentro de lo que se ha venido denominando "derechos de tercera generación" pues en este contexto, debido al desarrollo informático y tecnológico, se ha vuelto necesario dotar al individuo de un control sobre sus datos personales así como de preservarlo de un ámbito de privacidad libre de injerencias ajenas, pues derechos como la dignidad personal, la libertad, la intimidad, el honor o la propia imagen, estaban resultando lesionados como consecuencia del nuevo entorno socio-tecnológico y de su incidencia en los derechos reconocidos por las anteriores generaciones.

Por ello, la proclamación de los derechos de la "tercera generación" de ningún modo sustituye a los derechos clásicos ni tampoco puede afirmarse que esta categoría de derechos, consista en un *numerus clausus*, pues todavía hoy, dada la permanente evolución del contexto

---

[679] Para la tercera generación de derechos el carácter universal de los derechos humanos ha dejado de ser postulado ideal para devenir una necesidad práctica. Se trata pues de dar cumplimiento al proyecto emancipatorio cosmopolita de la modernidad, de aquella herencia cultural de la ilustración que no se llegó a desarrollar. Cfr. HABERMAS. *El discurso filosófico de la modernidad*, Taurus, Madrid, 1991.

[680] ARA PINILLA. *Las transformaciones de los derechos humanos*, Tecnos, Madrid, 1990, p. 112.

[681] PÉREZ LUÑO. "Las generaciones de derechos humanos", en *Historia de los Derechos Fundamentales* ob. cit., p. 368.

económico, social y cultural, hace necesario crear nuevas categorías jurídicas o reformular las ya existentes para proteger los bienes jurídicos contra nuevas formas de lesión.

Otros autores, van más allá y defienden la existencia de una *cuarta generación* de derechos humanos que vendría integrada por las nuevas formas que cobran los derechos de las tres anteriores generaciones en el entorno del ciberespacio y que pasan por la apropiación social de las nuevas tecnologías.

Se sostiene así la existencia de una "ciudadanía digital", coexistente con el status tradicional de ciudadano, que ha dado lugar a la aparición de nuevos valores, derechos y estructuras sociales aún en periodo de incubación, cuyos rasgos definitorios giran en torno a la defensa del acceso universal a la tecnología, a los derechos y libertades en el entorno digital y a la libertad informativa en Internet[682].

Con independencia de que se defienda la existencia de tres o cuatro generaciones, lo importante es la idea subyacente de que los derechos humanos responden a los cambios generacionales de paradigmas, por lo que el catálogo de derechos y libertades siempre estará en continua evolución y es susceptible de ser ampliado. Así, surge una nueva generación en tanto que la generación precedente se revela insuficiente –pero no ineficaz- para atender a las necesidades imperantes de la realidad, por lo que las generaciones posteriores de derechos humanos complementan –no suplen- las anteriores.

Sin embargo, esta última idea no parece estar del todo asentada, por lo que todavía la categorización de determinados derechos como de "tercera o cuarta generación" supone cierto estigma, aún hoy parte de la doctrina dota a estos derechos de cierto simbolismo e inocuidad cuando, si se toman en serio, comportan verdaderas limitaciones a la acción del Estado y de los propios particulares. La presentación de los derechos humanos en categorías cronológicas supone un problema desde el momento en que puede entenderse erróneamente que una generación sucede a otra, pues los derechos que se atribuyen a las distintas categorías

[682] Vid. por todos, BUSTAMANTE DONAS. "Hacia la cuarta generación de Derechos Humanos. Repensando la condición humana en la sociedad tecnológica" en *CTS+I: Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación*, nº 1, 2001.

confluyen y se solapan[683]. Debe rechazarse pues, toda connotación de prioridad de unos derechos respectos de otros.

La posibilidad de clasificar los derechos humanos en distintas generaciones, no resta ni un ápice a su entidad, que no se ve debilitada por las divergencias que las distintas características históricas de su aparición han proyectado sobre éstos. Compartimos pues, la visión de PÉREZ LUÑO sobre los derechos humanos los cuales define como "un conjunto de facultades e instituciones que, en cada momento histórico, concretan las exigencias de la dignidad, la libertad y la igualdad humanas"[684], y que ayuda a entender los derechos humanos como una conquista progresiva según las necesidades concurrentes.

Como se venía diciendo, esta clasificación de los derechos humanos, que sólo obedece a criterios históricos de ordenación, sin embargo, ha supuesto ciertos obstáculos para su operatividad en el sistema jurídico –cuyos primeros damnificados han sido los derechos sociales- que debe partir en todo momento de una igualdad semántica de los derechos. Así, a dicha categorización por generaciones no debe otorgársele ninguna otra explicación que no sea su carácter didáctico, como método para explicar su aparición, que favorece una visión mecanicista de la evolución de los derechos humanos cuya conquista ha sido lineal y cronológica en el tiempo.

Por ello tampoco debe abusarse de la denominación de "nuevos derechos" en tanto que, derechos como la protección de datos o el derecho al olvido, son una concreción de otros derechos más clásicos –viejos, si se quiere- de los que se derivan indirectamente pese a su autonomía, pero no forman una categoría de derechos distinta ni son el relevo de los anteriores. La aparición de nuevos derechos se explica por la nueva realidad social que, en este caso el paradigma del *Big data*, ha originado nuevas formas de amenaza para los mismos bienes jurídicos, por lo que se ha convenido oportuno crear nuevas categorías jurídicas capaces de

[683] PECES-BARBA MARTÍNEZ. *Curso de derechos fundamentales. Teoría general*, Universidad Carlos III-Boletín Oficial del Estado, Madrid, 1999, p. 70.

[684] Cfr. *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 2010, p. 50.

responder a los nuevos riesgos planteados para los valores de la persona humana y a su concreción en derechos.

Debe partirse pues de una concepción unitaria de los derechos humanos, capaz de superar el separatismo de las tesis liberales y el negativismo del socialismo utópico.

5.2. Derecho fundamental

Los derechos fundamentales son aquellos derechos humanos que han sido sancionados positivamente en un determinado ordenamiento jurídico, son derechos "que no son alienables o negociables, sino que corresponden, por decirlo de algún modo, a prerrogativas no contingentes e inalterables de sus titulares y a otros tantos límites y vínculos insalvables para todos los poderes, tanto públicos como privados"[685].

Desde una óptica formal, a diferencia de los derechos humanos, los derechos fundamentales no son inherentes a la condición de persona, sino que se reconocen exclusivamente a aquellos sujetos a quienes el legislador ha concedido su titularidad[686]. Ahora bien, respecto de sus titulares, se trata de derechos irrenunciables, inalienables, indisponibles, intrasmisibles, inviolables y exigibles jurídicamente.

Siguiendo esta concepción formal, el carácter fundamental de los derechos depende del rango de la norma que los reconoce, que debe ser de carácter constitucional o de alcance supralegal. Ello se debe a que, para preservar intacto el contenido de los derechos fundamentales, se han de prever mecanismos constitucionales de control capaces de protegerlos frente a cualquier alteración o injerencia, así como que su garantía permita invocar dichos derechos frente a todos, incluyendo el propio legislador.

---

[685] FERRAJOLI. *Derechos y garantías. La ley del más débil*, ob. cit., p. 37.

[686] Frente a esta perspectiva, compartida por los principales textos normativos (Constitución Española, Carta de Derechos Fundamentales de la Unión Europea, Convenio Europeo de Derechos Humanos…), existe una concepción material de los derechos fundamentales, en base a la cual los derechos fundamentales son aquéllos que, en un ordenamiento dado, se reconocen a todas las personas por el mero hecho de serlo. Estas posturas doctrinales, se centran exclusivamente en el contenido de los derechos, no en su significado, y defienden los derechos fundamentales como derechos inherentes a las personas. Vid. por todos, FERRAJOLI. *Derechos y garantías. La ley del más débil*, ob. cit.

Del mismo modo, ni siquiera todos los derechos comprendidos en la Constitución son derechos fundamentales. Se ha convenido en situar a los derechos fundamentales en aquéllos que quedan incluidos entre los artículos 14 a 29 de la Constitución, insertándose en el Título I de la Carta Magna[687]. En el ordenamiento jurídico español, el carácter fundamental de un derecho tiene notables connotaciones, principalmente relacionadas con los mecanismos para su garantía pues, como es sabido, aquéllos derechos que son derechos fundamentales en la Constitución española, gozan de un estatus jurídico superior y, en consecuencia, su protección frente a una eventual vulneración es mucho mayor[688].

Así, en virtud del artículo 53 CE, los derechos fundamentales son los únicos susceptibles de ser defendidos frente a su vulneración mediante la figura del recurso de amparo con un procedimiento preferente y sumario de protección, de manera autónoma, motivo por el cual se les reconoce una "invocabilidad directa". Además de este privilegio, la protección constitucional reforzada que se les otorga tiene otras importantes implicaciones pues, por ejemplo, requieren de una ley orgánica para el desarrollo de su contenido (art. 81 CE) y, en caso de su modificación, exigen un procedimiento agravado de reforma constitucional (art. 168 CE).

En el caso del derecho al olvido se trata, sin duda, de un derecho fundamental por varias razones. En primer lugar, dada su relación íntima con otros derechos fundamentales, como vertiente -o proyección, si se prefiere- del derecho al honor y a la intimidad (art. 18.1 CE) y a la protección de datos de carácter personal (art. 18.4 CE).

---

[687] Algunos autores discrepan enormemente de la categorización de derechos y libertades llevada a cabo en el ordenamiento jurídico español que otorga un carácter preponderante a unos derechos frente a otros, con negativas consecuencias para algunos de ellos, como los derechos sociales, que de facto no tienen mecanismos de garantía frente a su vulneración. Así, señala AÑÓN ROIG, "Han quedado patentes, tras el esfuerzo argumentativo de autores de muy distinto signo y perspectiva, sus debilidades, su excesiva simplicidad, sus dependencias de construcciones dogmático-jurídicas superadas y sus presupuestos ideológicos implícitos". AÑÓN ROIG: "Derechos sociales: cuestiones de legalidad y de legitimidad", en *Anales de la Cátedra Francisco Suárez*, Vol. 44, 2010, p. 23.

[688] Así, por ejemplo, no es lo mismo vulnerar el derecho a la libertad de cátedra, derecho fundamental situado en el artículo 20.1 CE, que el derecho al medio ambiente que, por situarse en el artículo 45 CE, no goza de la misma protección jurídica en la práctica.

El vínculo entre estos derechos ya ha sido expresamente declarado por la jurisprudencia constitucional[689] pues, recordemos, por una parte, el honor -íntimamente vinculado a la dignidad de la persona- la protege "*frente a expresiones o mensajes que la hagan desmerecer en la consideración ajena al ir en su descrédito o menosprecio o que sean tenidas en el concepto público por afrentosas*"[690]; y por otra parte, la intimidad tiene por objeto garantizar al individuo "*un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona, frente a la acción y el conocimiento de los demás, sean éstos poderes públicos o simples particulares. De suerte que el derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado, no sólo personal sino también familiar, frente a la divulgación del mismo por terceros y una publicidad no querida*"[691].

Y, frente a ellos, el derecho a la protección de datos personales del artículo 18.4 CE desarrolla un instituto de garantía de los derechos comprendidos en el apartado primero del precepto, "*como forma de respuesta a una nueva forma de amenazada concreta a la dignidad*[692] *y a los derechos de la persona*" [693], que no aporta por sí solo una protección suficiente. Se erige así como una suerte de "libertad informática" consistente, en sí misma, en un derecho o libertad fundamental[694].

Así, el derecho al olvido, subyace como un mecanismo jurídico necesario para garantizar los derechos y libertades comprendidas en los apartados primero y cuarto del artículo

---

[689] STC 290/2000, de 30 de noviembre.

[690] STC 14/2003, de 28 de enero, FJ 12º.

[691] STC 176/2013, de 21 de octubre, FJ 4º.

[692] Se comparte aquí la visión expresada por el Magistrado Manuel Jiménez de Parga en el voto particular de la STC 290/2000, de 30 de noviembre, por la que se reconoció la autonomía del derecho a la protección de datos. Frente a la inexistencia de una cláusula abierta en la Constitución española que permita reconocer directamente derechos fundamentales no expresamente enumerados, el Magistrado propuso, como criterio general, que el Tribunal Constitucional debía tutelar los nuevos derechos fundamentales a partir del art. 10.1 de la Constitución por ser, "la libertad informática" en dicho caso, un derecho inherente a la dignidad humana. Así, para la fundamentación y origen del nuevo derecho fundamental, relegaba a carácter accesorio los artículos 18.1 CE (derecho a la intimidad), el 20.1 (libertad de expresión e información) y los tratados internacionales sobre derechos humanos y sobre el tratamiento automatizado de datos de carácter personal, así como otros principios constitucionales pues entendía que la dignidad personal del artículo 10.1 CE operaba como una cláusula general para el reconocimiento de nuevos derechos fundamentales.

[693] STC 254/1993, de 20 de julio, FJ 6º.

[694] *Ibid*, FJ 5º.

18 CE -comprendidos bajo el paraguas de la privacidad que se ha venido defendiendo a lo largo de este trabajo- que, dado el avance de la informática y el desarrollo de las nuevas tecnologías, no son capaces de poner fin a sus vulneraciones por sí mismas. Así las cosas, el derecho al olvido se constituye como "*una vertiente del derecho a la protección de datos personales frente al uso de la informática y es también mecanismo de garantía para la preservación de los derechos a la intimidad y al honor, con los que está íntimamente relacionado*"[695].

Desde una perspectiva más profunda, el derecho fundamental al olvido está íntimamente relacionado con la dignidad de la persona -como puntal principal de todos los derechos fundamentales[696] así como cláusula general interpretativa- y con el libre desarrollo de la personalidad (art. 10.1 CE), pues su máxima aspiración consiste en dotar de autonomía a todo individuo, permitiéndole tutelar sus propios intereses y asegurando para ello una parcela libre de injerencias[697]. Entendiéndose ambas nociones como presupuestos que pretenden establecer una cláusula general de libertad que presida el conjunto del ordenamiento jurídico[698].

De hecho, la dignidad humana y el libre desarrollo de la personalidad constituyen los fines últimos de toda democracia constitucional. Estas aspiraciones, deben orientar el conjunto del ordenamiento jurídico e incluso la acción del Estado democrático de Derecho, junto con el respeto a los derechos de los demás y a la Ley[699].

---

[695] STC 58/2018, de 4 de junio, FJ 5º.

[696] Siguiendo la idea de ARENDT del "derecho a tener derechos". Cfr. ARENDT. *Los orígenes del totalitarismo*, Alianza, Madrid, 2006.

[697] La dignidad de la persona y su libre desarrollo es donde tienen su raíz, y fundamento lógico y ontológico todos los derechos fundamentales, configurándose de esta manera el artículo 10 como "*el germen o núcleo de los derechos que les son inherentes*" a la persona. STC 53/1985, de 11 de abril, FJ 1º y 3º.

[698] "Los derechos fundamentales del artículo 18 CE, al igual que el derecho a la integridad física y moral del artículo 15 CE, son una prolongación de la propia identidad que a su vez es inseparable de la dignidad personal y el libre desarrollo de la personalidad como valores supremos y fundamento último de la libertad radical de la persona". GARCÍA LOPEZ. *El impacto de Internet en el libre desarrollo de la personalidad*, Wolters Kluwer, Madrid, 2018, p. 74.

[699] En este sentido, señala GÓMEZ MONTORO que "Nuestro art. 10.1, aun sin contener derechos fundamentales, constituye la base común a todos ellos; en él, dignidad de la persona, derechos fundamentales y libre desarrollo de la personalidad aparecen como valores entrelazados que constituyen (junto al respeto a la Ley y a los derechos de los demás) 'el fundamento del orden político y de la paz social', sin que parezca posible delimitar dónde acaba uno de esos valores y empieza otro". GÓMEZ MONTORO. "La titularidad de derechos fundamentales por personas jurídicas: un intento de fundamentación", en *Revista Española de Derecho Constitucional*, año nº22, nº65, 2002, p. 96.

En segundo lugar, el derecho al olvido es un derecho fundamental porque, al configurarse como garantía de la privacidad, protege en última instancia el libre desarrollo de la personalidad y, tomando en consideración el hecho de que toda violación a la privacidad supone en último término una vulneración de la libertad, nuestro ordenamiento jurídico exige que los presupuestos legales inherentes a la libertad sean desarrollados por la vía de los derechos fundamentales, como parte de su garantía.

En tercer y último lugar, porque así lo ha declarado recientemente el propio Tribunal Constitucional, siguiendo la argumentación llevada a cabo en su día para otorgar carácter fundamental al derecho a la protección de datos personales: "*si las libertades informáticas pueden definirse como derecho fundamental, también lo es, porque se integra entre ellas, el derecho al olvido*"[700]. Mediante su elaboración jurisprudencia el Tribunal Constitucional, además, dispone que el "derecho al olvido digital" constituye un derecho fundamental con carácter autónomo: "*el derecho al olvido es una vertiente del derecho a la protección de datos personales frente al uso de la informática, 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*"[701]. Esta autonomía que se le confiere al derecho al olvido, lo dota de contenido propio y faculta a su titular para llevar a cabo su ejercicio sin necesidad de alegar la infracción de ningún otro derecho o libertad por conexión, confiriéndole una sustancialidad propia que, sin duda, le otorga una situación privilegiada para reaccionar ante una eventual vulneración de su contenido.

Así, una vez concluido que el derecho al olvido es un derecho fundamental, ello comporta numerosas consecuencias. En primer lugar, el derecho al olvido vincula de forma inmediata a los poderes públicos, sin necesidad de intermediación legislativa alguna.

En segundo lugar, el derecho al olvido despliega efectos vinculatorios no sólo en las relaciones con los poderes públicos y entre particulares, sino también entre los propios poderes

[700] STC 58/2018, de 4 de junio, FJ 5º.

[701] STC 58/2018, de 4 de junio, FJ 5º.

públicos, quienes deben respetar su contenido en todo caso, incluso cuando se sucedan "relaciones de sujeción especial".

Por último, el derecho al olvido como derecho fundamental, opera incluso frente al legislador -a quien corresponde crear todos los demás derechos y deberes, limitando su libertad de configuración en el ordenamiento jurídico- pues éste tiene la fuerza propia de la norma que lo proclama[702].

5.3. Derecho subjetivo

A un derecho se le conceden propiedades subjetivas[703] cuando al sujeto de una norma se le dota de un estatus jurídico en virtud del cual ostenta la idoneidad para ser titular de situaciones jurídicas y/o autor de los actos que son ejercicio de éstas[704]. Los derechos subjetivos pues, se configuran como una suerte de expectativas positivas, cuando gozan de un contenido prestacional o, por el contrario, pueden dotar a sus titulares de una expectativa negativa, consistente en no sufrir injerencia alguna.

PECES-BARBA MARTÍNEZ parece compartir la visión según la cual los derechos subjetivos podrían considerarse como derechos de resistencia[705], pues dotan al individuo de herramientas jurídicas para poder reaccionar frente a los poderes públicos y preservar así su dignidad y libertad personal y, en relación a ello, el autor distingue tres dimensiones de los derechos subjetivos: la dimensión garantizadora, la participativa y la promocional[706].

---

[702] DÍEZ-PICAZO GIMÉNEZ. *Sistema de derechos Fundamentales*, ob. cit., pp. 59-60.

[703] Por el contrario, la dimensión objetiva de un derecho estriba en su valor como fundamento del orden político y la paz social (art. 10.1 CE), lo que se traduce en un deber general de protección y promoción de los derechos fundamentales por parte de los poderes públicos, dada la función de vertebración del orden constitucional de los derechos fundamentales. La faceta objetiva de los derechos fundamentales no sólo supone que éstos se erigen como límites negativos que condicionan la validez del conjunto del ordenamiento jurídico, sino que también se configuran como un mandato de acción y un deber de protección general a los poderes públicos. Es por ello que el Tribunal Constitucional ha reconocido la existencia de una "doble dimensión" de los derechos fundamentales (Vid. STC 64/1988, de 12 de abril, por todas).

[704] FERRAJOLI. *Derechos y garantías. La ley del más débil*, ob. cit., p. 39.

[705] Sobre la idea de resistencia, cfr. PRIETO SANCHÍS. *Estudio sobre derechos fundamentales*, Debate, Madrid, 1990.

[706] Cfr. *Curso de derechos fundamentales. Teoría general*, ob. cit., 423.

En base a esta categorización, los derechos civiles, entre los cuales se insertaría el derecho al olvido, desarrollan una función garantizadora, en el sentido más clásico de la idea de límite como abstención, en tanto que disponen una barrera en torno al individuo para que éste pueda construir libremente un ámbito privado, sin interferencias de otros sujetos ni de los poderes del Estado.

En segundo lugar, siguiendo la teoría jurídica de ALEXY, sabemos que una disposición jurídica confiere derechos subjetivos cuando una norma *N* es aplicable al caso de *a* bajo las situaciones dadas y ésta, no sólo le confiere a *a* un determinado derecho o libertad sino que, además, frente a su eventual vulneración, *a* tiene frente a *b* un derecho a *G*[707].

Así, el derecho al olvido confiere a su titular un derecho subjetivo pues no sólo le reconoce un ámbito de privacidad frente a la intromisión ajena así como un derecho al *habeas data* sino que, frente a una situación en la que su esfera legal de libertad haya sido lastimada, le concede la posibilidad de obtener del responsable la supresión de los datos que le conciernan, sin dilación indebida y, en caso de incumplimiento de dicho deber por el obligado, podrá acceder a una indemnización por daños y perjuicios.

a) El debate sobre la eficacia horizontal de los derechos

Tradicionalmente, los derechos subjetivos se han instrumentalizado para dotar al individuo de una herramienta de actuación frente al Estado o cualquier poder público para la protección de sus derechos, motivo por el cual encuentran su fundamentación contextualizados en el Estado de Derecho. Sin embargo, ello lleva a la cuestión de si los derechos fundamentales rigen en las relaciones entre particulares pues, en origen éstos no se pensaron para reglamentar relaciones jurídico-privadas.

El reconocimiento de la eficacia horizontal de los derechos fundamentales deriva directamente de la doctrina *vis expansiva de los derechos*[708] en base a la cual los derechos

[707] ALEXY. *Teoría de los Derechos Fundamentales*, Centro de Estudios Políticos y Constitucionales, Madrid, 2001, pp. 175-178.

[708] Sobre la doctrina *vis expansiva de los derechos*, cfr. PÉREZ TREMPS. "La interpretación de los derechos fundamentales", en *Interpretación constitucional* (Ferrer Mac-Gregor coord.), Tomo II, Porrúa, México, 2005.

fundamentales ya han superado su función original como ámbitos de libertad individual frente a la actuación de los poderes públicos para transformarse en instrumentos jurídicos que protegen la libertad frente al poder y frente a otros particulares, como consecuencia lógica de la capacidad expansiva de las esferas garantistas de los derechos en tanto en que constituyen una pieza esencial para defender los valores democráticos.

La libertad de un individuo, así como sus derechos fundamentales, pueden ser también vulnerados por personas no investidas de potestad pública alguna, ello no queda limitado al poder público, por lo que debe de dotarse a los ciudadanos de garantías legales suficientes para proteger sus derechos y libertades frente a cualquiera. De hecho, muchas de las conductas típicas de lesión o amenaza de los derechos fundamentales, se suceden más frecuentemente por parte de personas individuales, como sucede con el derecho al honor.

Los derechos fundamentales, en cuanto parte integrante de la Constitución, son predicables frente a los poderes públicos y frente a los particulares, ello se deriva del artículo 9.1 CE que establece como la Constitución vincula a "*los ciudadanos y a los poderes públicos*". Otra cosa es si la vinculación de los derechos fundamentales es igual en ambos casos, frente a lo cual PÉREZ TREMPS distingue entre la vinculación directa o inmediata que tiene lugar respecto de los poderes públicos y, por el contrario, la vinculación indirecta de los derechos fundamentales en las relaciones entre particulares, en la medida en que éstos quedan determinados por el alcance definido por los poderes públicos pese a que, en la práctica, la eficacia de los derechos en ambas situaciones es muy similar[709].

En el contexto de Internet, dada su peculiar naturaleza y las posibilidades de interacción entre distintos agentes, la idea de la eficacia horizontal de los derechos cobra aún más sentido pues, lo relevante para los derechos humanos en este ámbito, es que deben adaptarse al nuevo medio, caracterizado por romper con el modelo tradicional de relación de poder -de arriba abajo- que propiciaban los medios tradicionales, y establecer un sistema descentralizado de comunicación, caracterizado por su eficacia horizontal –opuesta a la comunicación vertical

[709] Cfr. *Derecho constitucional. El ordenamiento constitucional. Derechos y deberes de los ciudadanos*, Tirant lo Blanch, València, 2016, p. 136.

ofrecida por la radio y la televisión- pues los individuos pueden recibir información –datos personales, incluidos- pero también emitirla.

Ello convierte a la tecnología en un medio aparentemente democrático –al menos para los que ya intervienen en él- pero, al mismo tiempo, se presenta como potencial vulneradora de los derechos fundamentales pues, por ejemplo, su carácter bidireccional puede ocasionar la emisión de información no controlada por parte del individuo, afectando negativamente a su privacidad, o la desinformación por exceso de información –que, además, no siempre es verdadera-, y que incide en su autonomía individual y política[710].

Dicho contexto conlleva necesariamente reformular la concepción clásica y reafirmar el carácter horizontal de los derechos fundamentales pues, su función objetiva–a la que se ha aludido anteriormente- permite justificar su extensión al ámbito privado. Los derechos fundamentales no se presentan únicamente como condicionantes de la actuación de los poderes estatales -debe superarse este reduccionismo propio de la concepción liberal clásica- sino que, además, se articulan como normas con "la vocación de regular cualquier aspecto de la vida social, incluidas, por ejemplo, las relaciones entre particulares"[711].

b) La situación de oligopolio como argumento para afirmar la eficacia horizontal del derecho al olvido

En la lógica profunda de los derechos fundamentales está la convicción de que entre gobernantes y gobernados existe, por definición, una situación de desequilibrio a favor de los primeros, por lo que los segundos han de ser compensados con especiales garantías capaces de compensar las múltiples potestades y privilegios de los primeros[712]. Esta situación de desequilibrio se da también en las relaciones entre los ciudadanos –usuarios, si se prefiere en este contexto- y los propietarios y administradores de los dominios y buscadores web y, en general, frente alas corporaciones de *Big data* que, posicionados en una clara situación de

[710] IGLESIAS GARZÓN. "Tecnología, comunicación y política en el siglo XX", en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. I, Libro I, Dykinson, Madrid, 2013, pp. 315 y 316.

[711] PRIETO SANCHÍS. *El constitucionalismo de los derechos. Ensayos de filosofía jurídica*, Trotta, Madrid, 2013, p. 28

[712] DÍEZ-PICAZO GIMÉNEZ. *Sistema de derechos Fundamentales*, ob. cit., p. 135.

oligopolio[713], tienen un poder absoluto en el Mercado y condicionan a los usuarios a quienes imponen sus condiciones contractuales, por lo general abusivas[714].

Como se ha mencionado anteriormente, esto está íntimamente relacionado con la llamada "fuerza expansiva de los derechos fundamentales" pues éstos deben orientar el desarrollo de toda la legislación así como impregnar al conjunto del ordenamiento jurídico lo que, sin duda, tiene implicaciones, no sólo para los operados privados, sino también para el conjunto de los poderes públicos y para el propio sistema democrático.

Dice ALEXY que el efecto horizontal de los derechos fundamentales está íntimamente relacionado con los deberes del Estado democrático de Derecho pues, las normas iusfundamentales, en tanto principios objetivos aplicables a todos los ámbitos del Derecho, implica que el Estado está obligado a tenerlas en cuenta también en la legislación civil, e incluso en la jurisprudencia civil pues, por mandato constitucional, todas las normas, prescripciones y cláusulas de Derecho privado deben estar influenciadas iusfundamentalmente[715].

No puede obviarse que existen determinados supuestos en los que, aun tratándose de un sujeto privado, éste ostenta algún tipo de privilegio concedido o tolerado por el Estado del que carecen el resto de particulares y que lo sitúa en una posición de superioridad. Este es el caso de ciertos motores de búsqueda como *Google* o *Internet Explorer* así como de determinados software, portales web u otros operadores de Internet que, dada la naturaleza del medio en el

---

[713] Respecto de los buscadores web, el último informe del reputado grupo estadista *Statcounter* en agosto de 2018, revela que sólo seis buscadores se reparten la cuota de mercado global. *Chrome*, en el primer puesto con un 90,46% de cupo, seguido por *Bing*, *Yahoo!*, *Baidu*, *Yandex RU* e *Shenma*. http://gs.statcounter.com/search-engine-market-share#monthly-201807-201808 En España, sin embargo, *Google Chrome* ostenta el 95, 23% de cuota de mercado a fecha de redacción de estas líneas. http://gs.statcounter.com/search-engine-market-share/all/spain/#monthly-201807-201808

[714] Sobre esta cuestión, ORDUÑA MORENO dispone la necesidad de extender el principio jurídico de la transparencia a todo contratante, ya sea consumidor o no, que, como adherente, tenga que recurrir a este modo de contratar bajo condiciones generales, sin posibilidad real de negociación y con una clara posición de inferioridad y asimetría en dicha relación jurídica. El autor defiende la existencia de un nuevo valor constitucional, esto es la transparencia, promovido desde los postulados de la justicia contractual que proyectan, asimismo, los principios de igualdad y no discriminación del artículo 14 CE y los artículos 20 y 21 de la Carta de los Derechos Fundamentales de la Unión Europea. Cfr. ORDUÑA MORENO/SANCHEZ MARTÍN. *La transparencia como valor del cambio social: su alcance constitucional y normativo. Concreción técnica de la figura y doctrina jurisprudencial aplicable en el ámbito de la contratación*, Aranzadi, Navarra, 2018, pp. 73-74.

[715] ALEXY. *Teoría de los Derechos Fundamentales*, ob. cit., pp. 515-517.

que desarrollan su actividad, basado fundamentalmente en las leyes del libre mercado y la autorregulación, tienen una capacidad de influencia y condicionamiento en las personas individuales sin precedentes, todo ello en connivencia con los Estados, que mayoritariamente han optado por abstenerse de cualquier política intervencionista.

Teniendo esto en cuenta, así como la situación de preeminencia que ostentan muchos de los operadores de Internet, prácticamente en posiciones de oligopolio y, pese a que las relaciones con sus usuarios y consumidores no dejan de ser individuales, éstas están plagadas de ventajas exorbitantes, dándose ciertos paralelismos con la posición clásica de los individuos frente al Estado. Esta conexión con los poderes públicos, justifica el despliegue de la eficacia de los derechos fundamentales pues los individuos, ven atacados sus derechos y libertades por la posición preeminente de estos operadores jurídicos particulares, por lo que debe concedérseles garantías suficientes para preservar sus derechos fundamentales.

Dadas las razones expuestas anteriormente, procede afirmar el efecto horizontal de los derechos fundamentales[716] y, en consecuencia, no se observan obstáculos para dotar de dicha eficacia al derecho al olvido digital, más bien lo contrario pues, al tener éste lugar en el contexto de Internet –hábitat parcelado por entidades particulares-, el único modo de hacerlo efectivo es reconocerle la capacidad para accionarlo ante dichos poderes privados[717]. Los valores subyacentes a determinados derechos fundamentales, entre ellos el derecho al olvido, están expuestos en igual medida a agresiones públicas y privadas por lo que el ordenamiento jurídico tiene el deber de proporcionar una garantía adecuada en ambas situaciones.

[716] No obstante, y como señala DÍEZ-PICAZO GIMÉNEZ, negar la eficacia horizontal a los derechos fundamentales no implica negar, asimismo, la absoluta irrelevancia de éstos para la regulación de las conductas de los particulares sino sólo que los derechos fundamentales no pueden ser invocados directamente *ex constitutione* frente a particulares. En efecto, el legislador puede extender la esfera de aplicación de esos derechos a las relaciones entre particulares mediante derechos de rango legal, dictando legislación civil o penal a dicho efecto pues, "que la Constitución no otorgue un derecho directamente invocable no implica que no imponga un deber de protección legal". Cfr. *Sistema de derechos Fundamentales*, ob. cit., p. 145.

[717] Así lo ha entendido el Tribunal Constitucional en distintas ocasiones en las que ha otorgado genuina eficacia horizontal a los derechos fundamentales, sin que haya sujeto público en relación privada, intervención pública relevante o intermediación legislativa, como, por ejemplo, en el ámbito de las relaciones laborales (Vid. por todas, STC 1/1998, de 12 de enero) donde las relaciones entre particulares se caracterizan por una cierta supremacía del empleador sobre el empleado.

5.4. Derecho de la personalidad

La expresión "derecho de la personalidad" se ha acuñado tradicionalmente por parte de la doctrina civilista y se emplea para designar un conjunto un tanto heterogéneo de derechos subjetivos dirigidos a proteger la integridad personal del ser humano tanto en su vertiente física (vida, integridad física) como en su faceta más espiritual (honor, intimidad, imagen…)[718]. Así, éstos se caracterizan, desde un punto de vista negativo, por su naturaleza no patrimonial y, desde una óptica positiva, por proteger determinados atributos de la personalidad misma.

Se trata pues de derechos de ejercicio personalísimo (artículo 162 CC) o, si se prefiere, de atributos de la personalidad susceptibles de apropiación jurídica (art. 333 CC) cuyo contenido último consiste en la posibilidad de exigir que el resto de las personas no se entrometan en el ámbito propio de la persona. Son derechos absolutos o *erga omnes* que, en la medida en que forman parte del orden público, constituyen un límite a la autonomía de la voluntad (artículo 1255 CC) y cuya infracción ha de repararse por vía de la indemnización[719]. En cuanto a nuestro objeto de estudio, cabe destacar que entre los derechos de la personalidad, se encuentran el derecho al honor, intimidad e imagen y a la protección de datos de carácter personal, todos ellos reconocidos en el artículo 18 CE y que están vinculados directamente con el derecho al olvido.

En cuanto a las características de los derechos de la personalidad, tradicionalmente se han considerado derechos innatos, inherentes al concepto de persona y de ejercicio personalísimo, así como derechos irrenunciables, indisponibles, intransmisibles e imprescriptibles. Sin embargo estos atributos hoy en día aceptan matices y no se predican con

[718] La cuestión de establecer con nitidez las relaciones que existen entre los derechos de la personalidad y los derechos fundamentales es ciertamente complicada y depende del concepto que de estos últimos se tenga. Sin embargo, siguiendo la fundamentación mantenida a lo largo de este Capítulo, si situamos el debate dentro de la esfera constitucional, podría afirmarse que, mientras que los derechos de la personalidad son derechos subjetivos, no todos ellos son derechos fundamentales sino que, sólo tendrán un carácter fundamental cuando así lo recoja la norma constitucional. Un claro ejemplo de ello es el derecho de autor que, pese a ser un derecho de la personalidad, no goza de un rango legal constitucional. Así pues, se produce una doble caracterización de algunos derechos, como derechos fundamentales y como derechos de la personalidad, pero ello no implica que estemos ante dos derechos diferentes, sino que se trata de un mismo derecho visto desde perspectivas distintas.

[719] DÍEZ-PICAZO GIMÉNEZ. *Sistema de derechos Fundamentales*, ob. cit., p. 34.

la misma intensidad. De hecho, en cuanto a su carácter indisponible e irrenunciable, y pese a que ha sido tradicionalmente una característica ligada intrínsecamente con los derechos de la personalidad, esta concepción ha sido superada por las circunstancias actuales y ya no se puede defender con valor absoluto.

Si bien puede sostenerse que el titular de un derecho de la personalidad no puede disponer por completo del mismo, ni puede transmitirlo definitivamente, ni extinguirlo por medio de renuncia, ello no implica que el titular de este derecho carezca, en todo caso, de toda facultad jurídica de disposición en relación con ese derecho[720]. En efecto, y siempre dentro de los márgenes establecidos por la Ley, el titular tiene cierto poder de transacción respecto de algunas facetas de sus derechos de la personalidad, como es el caso del derecho a la intimidad o a la imagen, donde los particulares, por ejemplo, pueden celebrar contratos mediante los cuales se preste su imagen a una determinada campaña publicitaria o bien pueden acordar un publirreportaje en el interior de su domicilio, a cambio o no de una contraprestación dineraria. Así, una persona no puede renunciar en términos absolutos, por ejemplo, a su derecho a la intimidad pero sin embargo, puede disponer de él parcialmente, consintiendo la intromisión ajena en su esfera más privada, e incluso, patrimonializando así un derecho de la personalidad.

Partiendo de esta idea, y situando el foco del debate en el derecho al olvido, eso lleva a preguntarse si es posible negociar con los datos personales que integran el mismo. Una vez más, las semejanzas entre la configuración del derecho al olvido y otros derechos de la personalidad como el honor o la intimidad, son evidentes y, teniendo en cuenta el hilo argumentativo anterior, podría no parecer razonable responder negativamente a dicha cuestión.

Sin embargo, este asunto es mucho más complejo de lo que a simple vista aparenta, y deben hacerse varias puntualizaciones al respecto. Por una parte, no parece coherente configurar el derecho al olvido sobre la base del derecho a la propiedad privada de una manera

[720] MARTÍNEZ DE AGUIRRE ALDAZ, C. "Los derechos de la personalidad", en *Curso de Derecho Civil (I). Derecho de la Persona*, (De Pablo Contreras, coord.), Edisofer, Tomo I, Vol. 2, Madrid, 2016, p. 266.

absoluta, como planteó la doctrina anglosajona del "*right to privacy*" en un primer momento[721] porque, aunque sin duda ambas nociones protegen una esfera privada de las personas, lo hacen de distinta manera y englobar ambas bajo la perspectiva unitaria del derecho a la propiedad, conllevaría innumerables consecuencias jurídicas y económicas.

El derecho al olvido, como tantas veces se ha repetido, encuentra su fundamento en el derecho a la protección de datos, lo que arroja consecuencias jurídicas especiales, dada la naturaleza propia de los mismos así como del funcionamiento concreto de la economía de los datos. Hay que tener en cuenta, en primer lugar, que los datos comprendidos bajo el paraguas del derecho al olvido son de diversa índole así, si bien podría tratarse de una fotografía, también podría referirse a una dirección de correo electrónico, por lo que su heterogeneidad dificulta enormemente la posibilidad de subsumir todos ellos en una misma categoría.

En segundo lugar, además de la diversidad de los datos que circulan por Internet, hay que añadirle el hecho de que, frecuentemente, estos datos suelen estar interrelacionados (así, por ejemplo, una dirección de correo electrónico puede ir aparejada a una fotografía), lo que añade complicaciones en este sentido.

En tercer lugar, se requiere un análisis pormenorizado del caso concreto ya que el transcurso del tiempo tiene una gran incidencia en el derecho al olvido y, resulta además que, muchos de esos datos son divulgados voluntariamente por los propios interesados, por lo que la expectativa razonable de privacidad no se aplica de igual modo.

Así, siguiendo la terminología anglosajona, debemos diferenciar entre el "*right of privacy*" del "*right of publicity*", atribuido a las personas públicas que explotan comercialmente su imagen, voz u otras características personales aparejadas a su identidad, al que sí que se le admite la categoría de "*property right*" a diferencia del primero, el cual queda limitado por su

[721] WARREN y BRANDEIS, cuando propusieron el "*right to be let alone*", lo reivindicaron como una consecuencia lógica del derecho a la privacidad, mucho más amplio, y, para la elaboración de su postura doctrinal, reexaminaron el concepto del "*right to privacy*" en base al derecho de propiedad. Cfr. "The Right to Privacy", ob. cit.

pertenencia a la categoría de los derechos de la personalidad, a quienes no se les reconoce transmisibilidad alguna[722].

Todo este conglomerado de circunstancias hacen realmente difícil ponderar el derecho al olvido en términos generales, en base a la teoría de la responsabilidad extracontractual, pues como se verá más adelante, se debe analizar el caso concreto para determinar las eventuales vulneraciones ante una expectativa razonable de privacidad, lo cual no está exento de polémica pues, dicha concepción varia drásticamente en función de los distintos grupos sociales, económicos y culturales. Frente a ello, hay quienes defienden la aplicación del régimen de propiedad en oposición al régimen de responsabilidad extracontractual, aduciendo que el enfoque de agravios no presenta un mecanismo consistente y factible para la aplicación de los derechos de privacidad, mientras que la teoría general de la propiedad privada, serviría mejor a los intereses de las partes individuales y la sociedad en general[723].

Ciertamente resulta difícil encontrar argumentos que nieguen rotundamente la posibilidad de transmitir los datos personales para su explotación económica pues, siguiendo la doctrina de derechos como la intimidad o al honor así como la autonomía privada que rige el derecho de contratos, pocas trabas pueden darse a la cesión contractual del uso de datos personales, siempre y cuando se respeten las normas de protección de datos personales así como el resto de garantías legales[724]. Sin embargo, algunos autores como MUÑOZ SORO y OLIVER-LALANA, rechazan dicha posibilidad en base a la necesidad de establecer límites al consentimiento como expediente legitimador pues, si bien reconocen cierto paternalismo en su

[722] Cfr. MARTÍNEZ VELENCOSO. "El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?", en *InDret*, nº 1, 2018, pp. 7-11.

[723] Así lo señalaron ya WARREN y BRANDEIS: "El derecho a la propiedad en su más amplio sentido, al incluir toda posesión, al incluir todos los derechos y privilegios, y al abarcar por tanto el derecho a la inviolabilidad de la persona, es el único que ofrece esta amplia base sobre la que sustentar la tutela que el individuo reclama". Cfr. *El derecho a la intimidad*, Civitas, Madrid, 1995, p. 55.

[724] A este respecto, la STC 292/2000, de 30 de noviembre: "*Privada la persona de las facultades de disposición y control sobre sus datos personales, lo estará también de su derecho fundamental a la protección de datos, puesto que […] se rebasa o se desconoce el contenido esencial cuando el derecho queda sometido a limitaciones que lo hacen impracticable, lo dificultan más allá de lo razonable o lo despojan de la necesaria protección*" (FJ 10º).

postura, argumentan la inviabilidad de considerar un derecho fundamental como un bien libremente disponible dentro del modelo jurídico europeo[725].

No cabe duda de que la información personal se ha convertido en un bien valioso, cuyos beneficios económicos no redundan en la persona interesada, la que ha generado el contenido en cuestión y ante la cual se derivan las principales consecuencias. Así pues, ¿por qué no reconocer derechos de propiedad sobre la información personal, como parte de una serie de derechos positivos entre los que se incluiría la libertad de enajenarlos? Sin duda ello ofrecería a toda persona un mayor control sobre su información privada pues, en función de un mayor o menor beneficio económico, decidiría lo que está dispuesta a compartir con el resto[726]. Sin embargo, la información personal como ya se ha señalado, tiene unas características propias que la hacen difícilmente asimilable a la propiedad clásica[727]. Puede poseerse por más de una persona y no se destruye mediante su consumo ni pierde valor cuando más veces se ha usado, todo lo contrario, pierde valor cuanto menos se usa y se queda obsoleta.

Ocurre también, que la mayoría de los datos comprendidos en la Red pueden estar recogidos en una base de datos (una página web o una red social) cuya elaboración y titularidad pertenece a una tercera persona[728]. Ello sugiere más similaridades con la doctrina de la propiedad intelectual, aunque tampoco en un sentido estricto pues ello podría abrir la puerta al

---

[725] "Sucede así en otras áreas de relevancia colectiva, como el consumo o el trabajo, donde ni siquiera la voluntad libre del consumidor o del trabajador constituye un mecanismo legitimador absoluto". Cfr. *Derecho y cultura de protección de datos. Un estudio sobre la privacidad en Aragón*, Dykinson, Madrid, 2012, pp. 67-68.

[726] "It is preferable from the viewpoint of individual fairness and collective benefit, as well as logic and intellectual consistency, to regulate personal information through the property rule, which affords the individual maximum control over personal information and allows all interested parties to enter into mutually acceptable transactions without tying up valuable societal resources. Privacy torts may still play an important role under specific circumstances defining those torts – as a separate claim or an additional theory for recovery. However, property should serve as a general paradigm for new legislation regulating issues relating to personal information". BERGELSON. "It's Personal but Is It Mine? Toward Property Rights in Personal Information" en *UC Davis Law Review*, Vol. 37, nº 379, 2003.

[727] PÉREZ LUÑO rechaza vincular la *privacy* con la *property* pues, señala que ello supondría limitar el disfrute de la intimidad a grupos selectos que puedan permitirse acceder a la propiedad privada, mientras que la intimidad es un valor predicable de todos los estratos sociales, como una exigencia imprescindible para asegurar a los ciudadanos su capacidad de participación en la sociedad democrática. Cfr. *Derechos Humanos, Estado de Derecho y Constitución*, ob. cit., p. 369.

[728] Se encuentran semejanzas insospechadas entre la doctrina seguida hasta ahora con los datos personales y la teoría jurídica de los animales salvajes –que, en base al artículo 610 CC son susceptibles de ocupación- pues parecen no pertenecer a nadie hasta que éstos no se recogen por un individuo o entidad.

tratamiento de la información personal como un material protegido por los derechos de autor, lo que podría conllevar a la creación de un monopolio de la información[729]. Algunos detractores de esta postura señalan que, de adoptarse un derecho de propiedad sobre los datos, las empresas encargadas de almacenarlos se verían obligadas a negociar con los individuales la venta de información personal lo que incrementaría los costes de transacción y el alcance de la información personal disponible para diversas empresas disminuiría[730], sin embargo esa parece ser precisamente la idea de quienes defienden la postura que aboga por la patrimonialización de los datos.

Otro autores como PÉREZ LUÑO son más enérgicos al mostrar su rechazo a dicha posibilidad, señalando la paradoja existente "fruto de la ideología latente en la dogmática iusprivatista burguesa"[731] en querer defender los derechos de la personalidad considerándolos objeto de propiedad privada, extendiendo en ellos los instrumentos pensados para la tutela externa del derecho de propiedad. Parece, no obstante, que los problemas de otorgar un derecho de propiedad sobre los datos personales son otros, empezando por la duración pues, a diferencia de la propiedad privada, la de los datos podría expirar por el transcurso del tiempo o de la finalidad para la que fueron empleados. También, en cuanto al contenido de los datos que se ofreciesen en propiedad, son muchos los interrogantes que se plantean y que por razones de extensión no pueden desarrollarse en este trabajo[732].

Así, de dar por válida la teoría de la propiedad sobre la información personal, debido a la naturaleza particular de lo que aquí se está tratando, parecería más idónea su configuración

[729] SOLOVE. "Conceptualizing Privacy" en *California Law Review*, Vol. 90, nº 1087, 2002, p. 1112.

[730] MERGES. "Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations", en *Southern California Law Review* Vol. 8, nº 1293, 1996, p. 1304.

[731] Cfr. "El derecho al honor y a la intimidad", en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. VI, Libro II, Dykinson, Madrid, 2013.

[732] Entre ellos, ¿debería imponerse algún límite?, ¿Podría enajenarse el usufructo exclusivamente, con independencia de la nuda propiedad?, ¿Podrían venderse los mismos datos a distintas personas? Pues parece evidente que más de una persona o entidad puede tener interés legítimo respecto de una misma información personal.

como una categoría mixta entre la propiedad privada clásica y los derechos de propiedad intelectual, lo que limita sin duda el alcance de los derechos de propiedad sobre los datos[733].

Sin embargo, y hasta la elaboración de una posición doctrinal clara al respecto, parece prematuro configurar el derecho al olvido sobre la base del derecho de propiedad, por lo que debe fundamentarse en la categoría tradicional de los derechos de la personalidad, como hasta ahora se ha venido haciendo y, en su caso, bajo la teoría de la responsabilidad extracontractual. Por lo que, hablar de posesión o de titularidad de los datos personales parece más apropiado que de propiedad[734].

Así las cosas, haciendo un resumen de la exposición y elaboración doctrinal anterior, y dada la naturaleza jurídica del derecho al olvido y la posición en la Carta Magna del artículo 18 -precepto en cual se inserta-, las facultades que otorga a sus titulares y sus vínculos con la vida privada, el honor y la dignidad personal no podemos sino concluir que se trata, respectivamente, de un derecho fundamental, relativo a la personalidad, con carácter subjetivo y, en consecuencia, un derecho humano.

6. Sujeto

Siguiendo con la estructura de los derechos fundamentales desde el punto de vista de la doctrina clásica civilista, procede distinguir ahora entre los diversos sujetos intervinientes en el derecho al olvido, no sin antes remarcar la peculiaridad que se produce cuando se aplica la categoría de derecho subjetivo a un derecho de la personalidad, pues en numerosas ocasiones se producen dificultades para distinguir entre el objeto y el sujeto del derecho. Como señalan

[733] Esta postura intermedia parece desprenderse, en alguna ocasión, de los escritos de WARREN y BRANDEIS: "La protección otorgada a los pensamientos, sentimientos y emociones manifestadas por escrito o en forma artística, en tanto en cuanto consista en impedir la publicación, no es más que un ejemplo de la aplicación del derecho más general del individuo a no ser molestado […] la cualidad de ser propiedad o posesión es inherente a cada uno de estos derechos como lo es de cualesquiera otros que el derecho reconoce, y, dado que es éste el atributo que distingue a la propiedad, podría considerarse apropiado referirse a estos derecho como una propiedad. Pero, obviamente, se parecen poco a lo que, por regla general, se entiende por dicho término. El principio que ampara los escritos personales, y toda obra personal […] no es en realidad el principio de la propiedad privada, sino el de la inviolabilidad de la persona". Cfr. *El derecho a la intimidad*, ob. cit., pp. 44-45.

[734] De hecho el GDPR trata de evitar toda terminología relacionada con la propiedad y la posesión, empleando en su lugar otras denominaciones más neutras como "interesado", "datos comprendidos" u "objeto de tratamiento", (artículo 86 GDPR).

DÍEZ-PICAZO y GULLÓN "Ciertamente, se observa que la independencia entre el sujeto y el objeto del derecho subjetivo es indudable. Pero, si se aplica la categoría de derecho subjetivo a los derechos de la personalidad, la oscuridad se presenta de inmediato por varias razones, que se pueden resumir en la heterogeneidad y en lo inseguro y arbitrario que es en muchas ocasiones distinguir el objeto del sujeto del derecho"[735].

6.1. Titularidad activa

En cuanto a la titularidad activa de los derechos fundamentales, respecto de las personas individuales esto no plantea demasiados problemas pues aquéllos fueron primariamente concebidos como derechos de los ciudadanos, constituyendo su estatuto jurídico básico. No obstante, como se verá a continuación, en algunas situaciones la protección de los derechos fundamentales se ha hecho extensible a las personas jurídicas, ampliando su razón de ser.

Partiendo de esta premisa, parece obvio que las personas individuales son titulares del derecho al olvido, otra cuestión es si todas ellas lo son en igual medida, con independencia de su carácter público o privado. Respecto de esta cuestión, y pese a que se examinará más detalladamente en el apartado relativo a los límites del derecho al olvido[736], sólo señalar en términos generales que no debe confundirse la titularidad de un derecho con las condiciones para su ejercicio. Así, todas las personas individuales gozan del derecho al olvido en toda su extensión pese a que, según las características propias del individuo en cuestión así como del caso en concreto del que se trate y de los derechos fundamentales con los que eventualmente colisione, las condiciones para su ejercicio serán unas u otras[737].

Así, afirmando la titularidad del derecho al olvido por parte de las personas físicas y dejando aparte -por razones de extensión y por no desviarse del objeto de estudio- aspectos accesorios acerca de la aplicabilidad de los derechos fundamentales, con respecto a los menores

[735] Cfr. *Sistema de Derecho Civil*, ob. cit., p. 337.

[736] Vid. *infra* Cap. III.9.

[737] En efecto, no parece razonable aplicar igual régimen jurídico a las personas públicas, que participan en la gestión de los asuntos públicos, para lo que han sido elegidos y por lo que responden ante la opinión pública, y las personas particulares; del mismo modo en que hay que diferenciar entre la intromisión en la privacidad de una persona producida en su faceta privada o en el transcurso de una actividad pública.

o extranjeros, por ejemplo, resta examinar la cuestión relativa a la posibilidad de conceder a las persona jurídicas la titularidad del derecho al olvido.

a) Personas jurídicas

Tradicionalmente se ha negado la eficacia horizontal de los derechos humanos al entender que su ligamen con la dignidad humana hacen que su titularidad sea exclusivamente individual[738]. Esta argumentación se ha acogido por parte de un sector doctrinal para negar la titularidad del derecho al olvido por parte de las personas jurídicas[739].

Sin embargo, en la actualidad debe superarse esta construcción dogmática de los derechos fundamentales cuyo significado debe contextualizarse en la concepción individualista de los derechos fundamentales -en base a la cual los derechos fundamentales son los derechos del hombre en cuanto tal, derivados de su dignidad de persona- que adolece de una importante carga ideológica liberal que impregnó las Constituciones europeas posteriores a la II Guerra Mundial[740].

El contexto actual, por el contrario, obliga a plantearse la cuestión desde otro punto de vista y es que, el Estado social y democrático de Derecho no sólo se articula desde la variable incuestionable del individuo como sujeto de derechos y libertades, sino que también se expresa a través de los grupos de diversa naturaleza en los que el individuo decide organizarse[741].

Ciertamente, la clásica concepción doctrinal ya ha sido superada incluso por el propio Tribunal Constitucional que, en base a la propia sistemática constitucional, rechaza dicha

---

[738] Así lo entendió también el Tribunal Constitucional en sus decisiones iniciales en las que negó la titularidad del derecho al honor a las personas jurídicas: "*el derecho al honor tiene en nuestra Constitución un significado personalista, en el sentido de que el honor es un valor referible a personas individualmente consideradas, lo cual hace inadecuado hablar del honor de las instituciones públicas o de clases determinadas del Estado*" (STC 107/1988, de 8 de junio, FJ 2º).

[739] Por todos, SIMÓN CASTELLANO, quien afirma: "el derecho al olvido se podría configurar como un derecho individua, subjetivo, de autonomía, de libertad, vinculado necesariamente a la dignidad humana, luego las personas jurídicas no serían titulares del derecho al olvido digital". Cfr. *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, València, 2011, p. 127.

[740] VIDAL MARÍN. "Derecho al honor, personas jurídicas y tribunal constitucional", en *InDret*, nº 1, 2007, p. 3.

[741] CARRILLO LÓPEZ. "Libertad de expresión, personas jurídicas y derecho al honor", en *Derecho Privado y Constitución*, nº 10, 1996, p. 91.

postura[742]. De hecho, la jurisprudencia constitucional se ha pronunciado acerca de esta cuestión en varios asuntos relacionados con el derecho al honor[743], con lo que resulta fácilmente extrapolable al derecho al olvido, dados los ligámenes existentes entre ambas figuras.

Si bien es cierto que existen determinados derechos fundamentales que, debido a su naturaleza, no resultan atribuibles a las entidades (como el derecho a la vida o a la integridad física), afirmar que las personas jurídicas[744] pueden ser titulares de derechos fundamentales no es, sin embargo, desproporcionado. En primer lugar porque, siguiendo una concepción institucional de los derechos, no parece descabellado defender que algunos derechos fundamentales sean predicables también respecto de las personas jurídicas pues los bienes o valores jurídicos que tutelan no les resultan ajenos y constituyen la base del propio Estado social y democrático de Derecho, dado el doble carácter de los derechos fundamentales, en tanto que derechos subjetivos y valores objetivos del orden constitucional[745].

En segundo lugar, porque las personas jurídicas están constituidas por un grupo de personas físicas que emplean instrumentalmente a dicha entidad como medio para llevar a cabo determinados fines que de otra forma no sería posible conseguir y, en virtud del artículo 9.2 CE, los valores de libertad e igualdad se reconocen no sólo al individuo sino también a "*los grupos en que se integra*".

En tercer lugar, y como ya se ha hecho mención anteriormente, porque debe superarse la concepción doctrinal clásica en virtud de la cual, la vinculación entre cualquier derecho

---

[742] STC 214/1991, de 11 de noviembre.

[743] Por todas, STC 139/1995, de 26 de septiembre. En dicha resolución, el Tribunal Constitucional afirma: "*aunque el honor es un valor es un valor referible a personas individualmente consideradas, el derecho a la propia estimación o al buen nombre o reputación en que consiste no es patrimonio exclusivo de las mismas* […] *el significado del derecho al honor ni puede ni debe excluir de su ámbito de protección a las personas jurídicas*".

[744] Suscribimos la definición de DÍEZ-PICAZO y GULLÓN en base a la cual las personas jurídicas se constituyen por aquellas realidades sociales a las que el Estado reconoce o atribuye individualidad propia, distinta de sus elementos componentes, sujetos de derechos y deberes y con una capacidad de obrar en el tráfico por medio de sus órganos o representantes. Cfr. *Sistema de Derecho Civil*, ob. cit., p. 618.

[745] Los derechos fundamentales son "*elementos esenciales de un ordenamiento objetivo de la comunidad nacional, en cuanto ésta se configura como marco de una convivencia humana justa y pacífica, plasmada históricamente en el Estado de Derecho y, más tarde, en el Estado Social y Democrático de Derecho, según la fórmula de nuestra Constitución*", STC 25/1981, de 14 de julio.

fundamental y la dignidad humana es motivo suficiente para que dicho derecho no sea susceptible de ser ejercido por personas jurídicas.

La Constitución española, por su parte, no proporciona una respuesta expresa a la cuestión de si las personas jurídicas pueden ostentar derechos fundamentales[746], pese a que así parece reconocerlo en algunos preceptos como el artículo 16 respecto a la libertad ideológica y religiosa de los "*individuos y las comunidades*" o el artículo 27.6 CE en cuanto a la libertad de creación de centros docentes[747]. Por otro lado, la jurisprudencia se ha pronunciado sobre ello en numerosas ocasiones y, a rasgos generales, ha tendido a recocer a las personas jurídicas aquellos derechos fundamentales que, habida cuenta de su objeto y finalidad, pueden serles de utilidad. Así, sostiene que: "*en nuestro ordenamiento constitucional, aún cuando no se explicite en los términos con que se proclama en los textos constitucionales de otros Estados, los derechos fundamentales rigen también para las personas jurídico nacionales en la medida en que, por su naturaleza, resulten aplicables a ellas*"[748].

Si bien es cierto que la descripción del derecho al olvido como un derecho de la personalidad puede precipitar a una conclusión apriorística y errónea en base a la cual se niegue a las personas jurídicas la capacidad para ser titulares de derechos fundamentales, un examen detallado de la cuestión nos conduce a afirmar, cuando hablamos de personas jurídico-privadas, justo lo contrario.

En primer lugar, porque resulta difícil sostener que la privacidad, la memoria o la reputación comercial de una sociedad anónima o de una fundación cultural no han de ser objeto de tutela pues, de lo contrario, ello podría fácilmente causar un perjuicio injustificado a dicha

[746] Sin embargo, SALVADOR CODERCH entiende que no es necesario: "La Ley española calla, pero es que no hace falta que hable para reconocer ese limitado derecho a la reputación: basta con que lo haga con carácter general el artículo 38 del Código Civil ("Las personas jurídicas pueden…ejercitar acciones civiles… conforme a las leyes y reglas de su constitución")". Cfr. *¿Qué es difamar? Libelo contra la Ley del Libelo*, ob. cit., p. 40.

[747] Otros instrumentos jurídicos sí que reconocen expresamente la titularidad de derechos de las personas jurídicas, entre ellos, el Convenio Europeo de Derechos Humanos de 1950 que, en su artículo 34, establece la posibilidad de presentar una demanda a "*cualquier persona física, organización no gubernamental o grupo de particulares que se considere víctima de una violación*", excluyendo así por otra parte, a las personas jurídico-públicas.

[748] STC 23/1989, de 2 de febrero.

entidad así como obstaculizar gravemente su funcionamiento, sin que cupiera posibilidad alguna de reacción por parte de la persona jurídica. En el ámbito y finalidad para los que ha sido creada, la persona jurídica tiene naturalmente una reputación que defender y, en consecuencia, hay un objeto a tutelar por el derecho que debe de dotarle de herramientas jurídicas para defenderse frente a una eventual vulneración, conforme a las finalidades legalmente permitidas[749].

En segundo lugar, debido a su conexión con otros derechos como el derecho al honor[750]. Si bien el alcance y contenido del derecho al olvido está aún por determinar, la jurisprudencia acerca de la extensión de la titularidad del derecho al honor a las personas jurídicas es muy abundante[751]. Así, igual que el Tribunal Constitucional ha admitido que el derecho fundamental al honor no es patrimonio único de las personas físicas puesto que habida cuenta de su significado "*ni puede ni debe excluir de su ámbito de protección*" a las personas jurídicas de Derecho privado[752], nada impide que lo mismo ocurra con el derecho de supresión.

Recordemos que el derecho al olvido, junto con otras particularidades como la privacidad o el dominio de los datos personales, dota asimismo a sus titulares de un cierto control sobre su reputación, en el contexto de las nuevas tecnologías y el uso de la informática. Así, en una sociedad en la que los individuos ponen en común sus intereses con otras personas para la consecución de determinados objetivos, no parece lógico concebir el derecho al olvido como una prerrogativa exclusivamente individual, pues resulta esencial para el desarrollo libre de una persona jurídica, fuertemente vinculado a su identidad, en tanto que garantiza un amplio margen de libertad de actuación.

Así lo entendió el TC, que reconoce a las personas jurídicas aquéllos derechos fundamentales que sirvan como medio o instrumento necesario para la consecución de la

---

[749] SALVADOR CODERCH. *¿Qué es difamar? Libelo contra la Ley del Libelo*, ob. cit., p. 39.

[750] STC 58/2018, de 4 de junio.

[751] En el caso del derecho al honor, además, su extensión a las personas jurídicas encuentra sustento legal en la Ley Orgánica 2/1984, de 12 de marzo, reguladora del derecho de rectificación cuyo artículo 1 así lo recoge expresamente.

[752] STC 139/1995, de 26 de septiembre.

finalidad para la cual fueron constituidas así como para la protección de su objeto entendida en dos vertientes, para proteger su identidad cuando desarrolla sus fines, así como para garantizar las condiciones de ejercicio de su entidad. Es en este entorno donde el derecho al olvido puede servir a una entidad privada como una herramienta para actuar frente al desmerecimiento ajeno así como para desarrollar libremente su actividad pues, siguiendo la argumentación constitucional esto "*supondría ampliar el círculo de la eficacia de los mismos más allá del ámbito privado y de lo subjetivo para ocupar un ámbito colectivo y social*"[753].

Estos pronunciamientos jurisprudenciales pueden -y seguro que el futuro inmediato así será- hacerse extensibles al derecho al olvido dadas las analogías existentes entre ambas figuras pues, el derecho a controlar la privacidad y la reputación personal así como a la autodeterminación informativa, superan claramente el reducto individual de la persona e inciden sobre grupos sociales de naturaleza heterogénea, que son también sensibles a la consideración que el entorno social tenga de ellos así como la actividad que realizan y la coherencia de sus presupuestos fundacionales con la práctica cotidiana[754].

No obstante, los derechos fundamentales reconocidos a las personas jurídicas no gozan de la misma la extensión y contenido que respecto de los sujetos individuales pues, su peculiar naturaleza, circunscribe los mismos a una forma jurídica concreta así como a un determinado fin según el caso particular, siendo susceptibles de sufrir variaciones en función de las particularidades de la entidad concreta[755].

Ahora bien, lo dicho anteriormente no rige para las personas jurídico-públicas que merecen un tratamiento distinto en esta cuestión atendiendo a su peculiar naturaleza jurídica. Pese a que, por motivos de extensión y para acotar debidamente el objeto de estudio de la presente disertación no se incidirá en dicha cuestión, parece obvio señalar que la especial naturaleza de los poderes públicos, en base a la cual gozan de un estatus privilegiado así como

---

[753] *Ibid*.

[754] Interpretando extensivamente a CARRILLO LÓPEZ, M. "Libertad de expresión, personas jurídicas y derecho al honor", ob. cit., p. 99.

[755] BASTIDA FREIJEDO/VILLAVERDE MENÉNDEZ et al. *Teoría general de los derechos fundamentales en la Constitución española de 1978*, Tecnos, Madrid, 2001, p. 89.

de potestades especiales y otras prerrogativas de actuación, hacen muy difícil trasladar aquí la teoría de la eficacia horizontal de los derechos fundamentales anteriormente expuesta.

Así lo ha dispuesto el Tribunal Constitucional cuya jurisprudencia ha sostenido que, aunque las instituciones públicas merecen cierta protección de su honor, prestigio y autoridad[756], esto no puede producirse en la misma consideración y protección que respecto de las personas individuales, pues de ningún modo ello está encarnado en un derecho fundamental por lo que, concluye, éstas no ostentan un derecho al honor. Así se entendió respecto del derecho al honor, sobre el cual el TC ha negado expresamente que las personas jurídico-públicas gocen del mismo por entender que es un valor predicable, exclusivamente, respecto de las personas individualmente consideradas[757]. Es más, sólo en casos muy excepcionales se han reconocido derechos fundamentales a personas jurídico-públicas (por ejemplo, el derecho a la tutela judicial efectiva del artículo 24 CE en su vertiente procesal[758] o el derecho a la libertad de información[759], en ciertas ocasiones)[760].

Y es que, a diferencia de las entidades de Derecho Privado, las personas jurídico-públicas no se crean como consecuencia del ejercicio de un derecho fundamental -la libertad de asociación del artículo 22 CE-, sino que el origen de estas entidades reside únicamente en un acto de un poder público[761], no existiendo así el presupuesto anterior para justificar la titularidad de otros derechos fundamentales.

[756] Por todas, STC 214/1991, de 11 de noviembre.

[757] STC 107/1988, de 8 de junio.

[758] STC 64/1988, de 12 de abril.

[759] STC 190/1996, de 25 de noviembre.

[760] VIDAL MARÍN. "Derecho al honor, personas jurídicas y tribunal constitucional", ob. cit., p. 10.

[761] Cfr. GÓMEZ MONTORO. "La titularidad de derechos fundamentales por personas jurídicas: un intento de fundamentación", ob. cit.

b) Personas fallecidas

Resuelto el problema acerca de la titularidad de las personas jurídicas del derecho al olvido, otra cuestión que suscita dudas es si éste puede accionarse sobre una persona ya fallecida.

En primer lugar, conviene recordar que el nacimiento determina la personalidad y, del mismo modo ésta se extingue con el fallecimiento[762] (o la ausencia declarada y equiparada al fallecimiento por presunción legal -art. 34 y 193 CC-). Así, únicamente dentro del período temporal marcado por el cumplimiento de los requisitos de nacimiento y no fallecimiento se posee personalidad jurídica y, por tanto, cabe ser considerado titular de derechos fundamentales.

Siguiendo lo dispuesto en el Código civil, se configura como principio general que las personas susceptibles de ser titulares de derechos sean aquellos individuos vivos (art. 29 CC), sin embargo ello no impide la posibilidad de tutela mediante el reconocimiento legal de ciertos derechos en casos concretos, respecto de una persona fallecida, ejercitables por sus causahabientes, que pueden integrar el contenido meramente legal de derechos fundamentales como el honor o la intimidad. Así ocurre en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen que, pese a reconocer el principio civilista por el cual, la muerte del sujeto de derecho extingue los derechos de la personalidad, dispone excepcionalmente la posibilidad de que el Derecho tutele la memoria del fallecido, en tanto que la considera como una prolongación de la personalidad (artículo 4)[763].

Y es que, a veces ocurre que las personas que nos precedieron han dejado en nosotros una memoria, un recuerdo o una imagen por lo que el ordenamiento jurídico español, a diferencia de otros, ha decidido tutelar la buena reputación de las personas más allá de su

[762] Artículos 30 y 32 del Código Civil.

[763] Ahora bien, esta facultad, puesto que es una medida excepcional, está sometida a ciertas condiciones –así, por ejemplo, esta acción no se podrá ejercitar cuando el fallecido, en vida, no hubiese ejercitado acción alguna pudiendo haberlo hecho – y a ciertos límites –como el plazo de ochenta años desde el fallecimiento del afectado, para el supuesto de que sea el Ministerio Fiscal el que interponga la acción-.

vida[764]. En el caso del derecho al olvido, precisamente lo que se pretende es salvaguardar la identidad del titular, lo que incluye asimismo tanto el reducto de una parcela de su privacidad como su reputación o estima social, en un ejercicio de autodeterminación o gestión de su información personal.

Así lo estima el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal –en tramitación parlamentaria en el momento de redacción de la presente disertación- que, tras excluir del ámbito de aplicación de la Ley su tratamiento, prevé expresamente que los herederos (o el albacea o la persona o institución designada a tal efecto por el fallecido) puedan solicitar el acceso a los datos de su causahabiente así como solicitar su rectificación o supresión[765], bajo pena de infracción leve en caso de incumplimiento[766] y sin más limitaciones que las establecidas por ley o cuando la persona fallecida así lo hubiese prohibido expresamente.

La idea rectora es que el interesado en la tutela es quien trae causa del afectado, motivo por el cual se le indemniza en la medida en que se estime que ha sido lesionado. Así, el guardián de la memoria del causante -sus herederos o la persona natural o jurídica designada por éste en vida- actúa como fiduciario que no puede reclamar en interés propio, pero sí puede

[764] SALVADOR CODERCH. *¿Qué es difamar? Libelo contra la Ley del Libelo*, ob. cit., p. 36.

[765] Artículo 3 del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal: "*Datos de las personas fallecidas. 1. Los herederos de una persona fallecida que acrediten tal condición mediante cualquier medio válido conforme a Derecho, podrán dirigirse al responsable o encargado del tratamiento al objeto de solicitar el acceso a los datos personales de aquella y, en su caso, su rectificación o supresión. Como excepción, los herederos no podrán acceder a los datos del causante, ni solicitar su rectificación o supresión, cuando la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley. 2. El albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello también podrá solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de éste y, en su caso su rectificación o supresión. Mediante real decreto se establecerán los requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones y, en su caso, el registro de los mismos. 3. En caso de fallecimiento de menores, estas facultades podrán ejercerse también por sus representantes legales o, en el marco de sus competencias, por el Ministerio Fiscal, que podrá actuar de oficio o a instancia de cualquier persona física o jurídica interesada. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse, además de por quienes señala el párrafo anterior, por quienes hubiesen sido designados para el ejercicio de funciones de apoyo*".

[766] Artículo 74 del Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal.

solicitar el cumplimiento del derecho al olvido y, en caso de vulneración del mismo, una indemnización razonable para deshacer dicho agravio[767].

6.2. Titularidad pasiva

En cuanto al sujeto pasivo frente a quién se ostenta el derecho al olvido conviene, en el caso del derecho al olvido, hacer algunas matizaciones. En primer lugar porque, si bien es cierto que tradicionalmente los derechos fundamentales fueron pensados como derechos frente al Estado -los poderes públicos[768]-, como ya se ha comentado en páginas anteriores, paulatinamente se les ha venido reconociendo un "efecto horizontal", por lo que pueden resultar también vinculantes en las relaciones jurídicas entre particulares[769].

Además, como también se ha comentado anteriormente, el derecho al olvido se enmarca en un contexto muy específico –Internet- en el que, los motores de búsqueda juegan un papel esencial a la hora de dotar de publicidad un determinado contenido que pueda ser digno de tutela por el Derecho para exigir su supresión[770]. Así, el interrogante que suscita es si, junto a los propietarios y administradores de una determinada App o de un dominio web, los motores de búsqueda pueden ser responsables pasivos frente a una pretensión de supresión.

Si bien anteriormente ya se ha hecho referencia a la situación de oligopolio en la que se encuentran determinados buscadores de Internet –situación que se ha visto agravada por los

---

[767] SALVADOR CODERCH. *¿Qué es difamar? Libelo contra la Ley del Libelo*, ob. cit., p. 37.

[768] Sobre los derechos fundamentales como límites al poder, cfr. ASÍS ROIG. *Las paradojas de los derechos fundamentales como límites al poder*, Dykinson, Madrid, 2000.

[769] En cuanto al efecto horizontal de los derechos fundamentales y las normas iusfundamentales en el sistema jurídico, dice ALEXY: "Esta influencia es especialmente clara en el caso de los derechos frente a la justicia civil. Entre los derechos frente a la justicia civil se encuentran derechos a que sus fallos no lesionen con su contenido derechos fundamentales. Esto implica un efecto, cualquiera que sea su construcción, de las normas iusfundamentales en las normas del derecho civil y, con ello, en la relación ciudadano/ciudadano". ALEXY. *Teoría de los Derechos Fundamentales*, ob. cit., p. 507.

[770] Sobre una cuestión accesoria a ésta se pronunció el TJUE en la STJUE (Gran Sala), de 23 de marzo de 2010, *Google France SARL y Google Inc. v. Louis Vuitton Malletier SA,* Asuntos acumulados C-236/08 y C-238/08, en relación a sus "servicios neutros de referenciación" comercial. Para el TJUE el motor de búsqueda es responsable cuando desempeña un papel activo que pueda darle al usuario conocimiento o control de los datos almacenados, mientras que quedarían exentos de responsabilidad cuando su función fuese de naturaleza "técnica, automática y pasiva", es decir, cuando se tratase de una actividad neutra. Así, dispuso el Tribunal, la responsabilidad del motor de búsqueda no deriva ni del carácter remunerado del servicio, ni de la concordancia de la palabra clave seleccionada, ni del término de búsqueda introducido por un usuario, sino de la redacción del mensaje comercial que acompañaba el enlace promocional o de la selección de la palabra clave.

acuerdos comerciales de éstos con las principales empresas tecnológicas para vincular sus buscadores con los dispositivos inteligentes de conexión a Internet, como configuración de fábrica- ello provoca que, entre los usuarios y los buscadores web (como con otras corporaciones del *Big data*), se produzca una relación de sujeción y poder análoga a la que se da entre los ciudadanos y los poderes públicos y que motivaron el establecimiento de garantías constitucionales para la salvaguarda de los derechos y las libertades fundamentales pues, entre ellos, se produce claramente una situación de desequilibrio en perjuicio de los primeros.

Resulta interesante detenerse un momento en el examen de la legitimación procesal de los motores de búsqueda a la hora de ejercitar el derecho al olvido, materia sobre la cual ya se pronunció el TJUE en su famosa sentencia del *caso Google*[771], contestado positivamente a esta cuestión. Brevemente, para contextualizar esta materia, conviene hacer referencia a la praxis habitual de muchas corporaciones transnacionales que, para evadirse del cumplimiento de los derechos de los que gozan los ciudadanos europeos en su legislación nacional y europea, alegan no estar sometidos al Derecho de la UE ni a la legislación doméstica en cuestión por tener la sede social de su empresa en un tercer país. Frente a esta actitud, llevada a cabo reiteradamente por el buscador *Google* -que, por tener su sede en Estados Unidos ha venido negando tener legitimación procesal en este caso de litigios, bajo el argumento de que el responsable del tratamiento de los datos es el titular del sitio web donde se publican los datos originalmente-, los tribunales nacionales, ante las peticiones de amparo de sus ciudadanos, se han visto forzados a resolver una cuestión fundamental respecto del tratamiento de los datos, esto es, ante quién debe ejercitarse el derecho de acceso, rectificación, cancelación u oposición ante la webmaster que edita originalmente los datos o ante el motor de búsqueda que, con su indexación, favorece su difusión.

El TJUE, como bien se ha visto anteriormente, se pronunció sobre esta cuestión y resolvió que *Google Spain* se dedica al ejercicio efectivo y real de una actividad mediante una instalación estable en España que, al estar dotada de personalidad jurídica propia, es una filial

[771] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

de *Google Inc.* en territorio español y, por tanto, un "establecimiento" a efectos de la Directiva 1995/46/CE de protección de datos[772] –en vigor en dicho momento-. El Tribunal afirmó que dicha Directiva no exigía, para ser aplicable el derecho nacional, que el tratamiento de los datos personales sea efectuado "por" el propio establecimiento en cuestión, sino que se halle "en el marco de las actividades" de éste, afirmación que en ningún caso puede ser objeto de una interpretación restrictiva.

La sentencia europea concluyó que *Google Search* es un buscador a nivel mundial gestionado por la entidad *Google Inc*., domiciliada en Estados Unidos, que presta sus servicios en España a través de *www.google.es* mientras que la filial *Google Spain*, con personalidad jurídica y domiciliada en España, gestiona la venta de espacios publicitarios, actuando como su agente comercial en territorio español, sin que esta última realice una actividad directamente vinculada al tratamiento de información en Internet.

La ya derogada Directiva 95/94/CE disponía que el establecimiento en el territorio de un estado miembro implicaba el ejercicio efectivo de una actividad mediante un establecimiento estable, con independencia de que se tratase de una simple sucursal o una filial ya que el objetivo de la norma era evitar, en última instancia, la desprotección de los ciudadanos. Por ello, consideró el TJUE que la actividad de dicho buscador en Internet y su establecimiento permanente en España –el cual se dedica a rentabilizar dicha actividad mediante la venta de espacios publicitarios- están indisolublemente unidos y se predicaba de ambas la responsabilidad por el tratamiento de datos de carácter personal[773], permitiendo a los interesados dirigirse indistintamente contra cualquiera de ellos y, en consecuencia, reafirmando la legitimación procesal pasiva de los motores de búsqueda.

En relación a esta cuestión, y como se ha mencionado en páginas anteriores, se ha producido un fenómeno ciertamente peculiar en nuestra jurisdicción doméstica pues, pese a haber transcurrido un tiempo considerable desde la sentencia TJUE en el *caso Google* –cuya

[772] Directiva 1995/46/CE, de 24 de octubre, del Parlamento Europeo y del Consejo de la Unión Europea de protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[773] FJ 56º.

doctrina es harto conocida-, el Tribunal Supremo dictó dos sentencias resolviendo, precisamente, sobre la legitimación procesal de un motor de búsqueda –*Google Spain*, de nuevo- cuando el tratamiento de los datos personales se lleva a cabo por sociedades mercantiles con establecimiento principal y filiales; y que, en cuestión de pocos días de diferencia, dieron lugar a pronunciamientos contradictorios por parte de la Sala Civil y la Sala Contencioso-Administrativo del mismo[774].

Así, la Sala de lo Contencioso-Administrativo del Alto Tribunal dispuso en su STS 574/2016, de 14 de marzo, que *Google Spain* carecía de legitimación pasiva para ser parte en los procedimientos ante la Agencia Española de Protección de Datos[775] al no apreciar interdependencia entre la actividad publicitaria de *Google Spain* y la del motor de búsqueda *Google Inc.* El Tribunal Supremo, rechazó que ambas sociedades, matriz y filial, constituyan una "unidad material" y refutó que *Google Spain* sea responsable de un tratamiento de datos indebido cuya acción sancionadora debía haberse dirigido, según su parece, a *Google Inc.,* cuyo domicilio social se encuentra en Estados Unidos.

En consecuencia, respecto de la eventual corresponsabilidad de la filial española, la argumentación de la sentencia gira en torno a la imposibilidad de identificar alguna actividad de *Google Spain* en la actividad del motor de búsqueda de *Google Inc.*, rechazando que la vinculación mercantil o empresarial existente entre ambas pudiera ser argumento suficiente para defender la coparticipación como responsable del tratamiento pese a ser una actividad vinculada económicamente, dada la distinta naturaleza de los fines de tratamiento, no siendo la unidad de mercado o negocio motivo suficiente[776].

---

[774] Nos encontramos ante un caso verdaderamente insólito pues, en el transcurso de pocos días, el Tribunal Supremo interpretó en resoluciones divergentes el concepto de "tratamiento de datos de carácter personal" sin plantear una cuestión prejudicial al TJUE sino interpretando de forma dispar su jurisprudencia en el *caso Google*. No se recuerda un precedente similar en el que un tribunal supremo de un Estado miembro, con días de diferencia, interprete de manera expresamente contradictoria un concepto tan relevante del Derecho comunitario sin, ni siquiera, plantear una cuestión prejudicial ante el TJUE.

[775] STS 574/2016, de 14 de marzo, Sala de lo Contencioso-Administrativo.

[776] Es más, la Sala afirmó "*No debe confundirse la determinación de los fines y medios del tratamiento, que es lo que caracteriza la condición de responsable, con una actividad de colaboración en la consecución de sus objetivos e, incluso en el caso en los que existiera corresponsabilidad en el tratamiento de datos, no es de apreciar solidaridad en el cumplimiento de las obligaciones, de manera que cada responsable lo es de aquellas que se derivan de su actividad*" (FJ 9º).

Frente a ello, casi un mes después, la Sala de lo Civil del Tribunal Supremo entendió en su STS 1280/2016, de 5 de abril, que *Google Spain* podía ser demandada en un proceso civil de protección de derechos fundamentales por tener, a estos efectos, la consideración de responsable en España del tratamiento de datos realizado por el buscador *Google*[777].

La Sala, en el marco de un proceso civil de protección de derechos fundamentales, cambió de parecer y consideró que *Google Spain* sí que es responsable del tratamiento de los datos personales que indexa el buscador *Google Inc.,* no siendo un factor determinante la forma jurídica que *Google Inc*. haya adoptado en territorio español, y que, por tanto y al contrario que en su anterior sentencia, la filial española puede ser demandada en un procedimiento de tutela del derecho al honor y a la intimidad[778].

Ante la evidente disparidad de criterios, la Sala de lo Civil matiza que ambas resoluciones aparentemente contrapuestas no tienen efecto prejudicial sobre el recurso que resuelven puesto que rigen principios dispares en ambas jurisdicciones[779]. De hecho, la primera sentencia dictada por la Sala de lo Contencioso-Administrativo, motivó la difusión de una nota informativa por la AEPD mediante la cual se aclaraba que, pese al pronunciamiento de dicha Sala, el ejercicio del derecho al olvido podía llevarse a cabo por los interesados ante la jurisdicción española dado que *Google Inc.* disponía de oficinas en España (*Google Spain*) para la promoción de sus productos y servicios, lo que le somete a las leyes europeas y nacionales de los países miembros en materia de protección de datos[780].

---

[777] STS 1280/2016, de 5 de abril, Sala de lo Civil.

[778] Entiende la Sala que, *Google Inc.* no sería posible sin *Google Spain* que le aporta los recursos económicos, no siendo un factor determinante la forma jurídica que *Google Inc.* haya decidido que adopten sus establecimientos en Estados distintos de aquél en que está situado su domicilio social. Los argumentos jurisprudenciales de la Sala se basan asimismo, en la existe8ncia de anteriores litigios en España en los que se demandó a *Google Spain* por la actividad del buscador *Google* y en los que *Google Spain* asumió la legitimación pasiva, lo que considera constitutivo de actos propios.

[779] "*Debe recordarse la existencia de distintos criterios rectores en las distintas jurisdicciones, por la diversidad de las normativas que con carácter principal se aplican a unas y a otras*" (FJ 3º).

[780] Mediante dicha nota informativa, de 15 de marzo de 2016, la AEPD quiso aclarar que dicha sentencia no modificaba los criterios establecidos por el TJUE en su sentencia del caso Google sino que se limitaba a disponer quien debía ser el destinatario de las solicitudes, por lo que los interesados podían seguir acudiendo a la AEPD para tramitar las solicitudes o, en su caso, frente a Google Inc.

Así, se observa la disparidad de criterios acerca de una cuestión accesoria si se quiere -por su naturaleza procesal-, pero francamente importante para la aplicabilidad del derecho al olvido pues, una y otra, resuelven aspectos procesales fundamentales a la hora de ejercitar la tutela de dicho derecho, en especial respecto de los sujetos responsables del tratamiento de los datos personales cuando éste se lleva a cabo por sociedades mercantiles con establecimientos principal y filiales.

Esta disparidad de criterios, fruto quizás de la reciente gestación o de la novedad del derecho del que se trata, se ha visto hoy en día superada pues, el GDPR, a través de la extensión de su alcance territorial[781], no deja lugar a dudas y, en la actualidad, cualquier empresa que lleve a cabo un tratamiento de datos contrario a la Ley -incluidos los motores de búsqueda- es perfectamente susceptible de ser demandada ante los órganos jurisdiccionales españoles cuando sus actividades tengan incidencia en territorio español, con independencia de que ésta se encuentre sita o no en él.

7. Objeto

Como se ha venido defendiendo, el derecho al olvido tiene un carácter poliédrico que viene integrado por un conglomerado de derechos fundamentales que interaccionan entre sí, a veces incluso colisionando entre ellos, y que forman parte de un todo mucho más amplio. La existencia y configuración del derecho al olvido obedece al contexto social y tecnológico en el que se inserta, y en las múltiples amenazas que genera Internet, medio que se caracteriza precisamente, por integrar en él los tradicionales medios de comunicación a los que no

[781] Artículo 3 GDPR:

1. "*El presente Reglamento se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento del responsable o del encargado en la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.*

2. El presente Reglamento se aplica al tratamiento de datos personales de interesados que residan en la Unión por parte de un responsable o encargado no establecido en la Unión, cuando las actividades de tratamiento estén relacionadas con: a) la oferta de bienes o servicios a dichos interesados en la Unión, independientemente de si a estos se les requiere su pago, o b) el control de su comportamiento, en la medida en que este tenga lugar en la Unión.

3. El presente Reglamento se aplica al tratamiento de datos personales por parte de un responsable que no esté establecido en la Unión sino en un lugar en que el Derecho de los Estados miembros sea de aplicación en virtud del Derecho internacional público".

substituye, sino que integra y magnifica, con el consecuente incremento de las posibilidades de lesión que ello conlleva para los derechos fundamentales más clásicos.

Así, podemos hablar de la interacción del derecho a la privacidad -un término escogido a conciencia, como ya se ha explicado en páginas anteriores, por abarcar parámetros más amplios que la intimidad estricta reconocida constitucionalmente- con el derecho al honor, a la propia imagen, a la dignidad personal y al libre desarrollo de la personalidad, la libertad de expresión y de comunicación -que operan fundamentalmente como límite al derecho de supresión- y, por último, el derecho a la protección de los datos personales.

La pluralidad de manifestaciones en las que la privacidad se explicita, no implican la disolución de su concepto sino su ampliación y adaptación a las exigencias cambiantes de la realidad. Como señala PÉREZ LUÑO, la metamorfosis del derecho de privacidad no ha significado la pérdida de su función tutelar de los valores de la personalidad, sino la posibilidad de preservar las garantías de autodeterminación del sujeto que ejerce su privacidad en el seno de sus relaciones con los demás ciudadanos, frente a poderes públicos y privados[782].

Todo ello permite defender una perspectiva unitaria del derecho al olvido, conformado por diversos bienes jurídicos protegidos interrelacionados entre sí pese que, a su vez, están tutelados por diversas figuras jurídicas. Sostenemos una concepción global, dinámica y proyectiva del derecho al olvido pese a que, sin embargo, su objeto pueda analizarse desde sus fuentes individuales como se procederá a continuación en aras de lograr una mejor comprensión del derecho de supresión, partiendo de una óptica más tradicional. Así pues, brevemente y centrándose exclusivamente en los bienes jurídicos que protegen (sin entrar en la titularidad de los derechos, las condiciones de ejercicio o sus procedimientos de protección), se examina a continuación las figuras clásicas aparejadas a la protección de la privacidad, con cierta incidencia en el contenido del derecho al olvido.

[782] PÉREZ LUÑO. "El derecho al honor y a la intimidad", ob. cit., pp. 1083-1084.

7.1. El derecho al honor

El artículo 18 CE dispone que "*se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen*", lo que evidencia el indiscutible ligamen entre ambos derechos, que constituyen el núcleo de los derechos de la personalidad en la esfera espiritual, al versar todos ellos sobre la protección de un ámbito privado reservado para la propia persona, destinando su garantía a la protección de un mismo bien jurídico, la vida privada. El desarrollo de este precepto constitucional se llevó a cabo por la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, la intimidad personal y familiar y la propia imagen (LOPDH)[783]que constituye el instrumento jurídico fundamental para la protección civil de dichos derechos.

En cuanto al honor, es habitual en la jurisprudencia del Tribunal Supremo distinguir entre su aspecto subjetivo, esto es, la estima de la persona hacia sí misma, y su faceta objetiva, estima de los demás hacia esa persona; como manifestaciones intrínsecas del derecho a la dignidad personal, lo que constituye la "fama o reputación"[784]. En relación a este último aspecto, se encuentra el prestigio profesional que, según su alcance y sus circunstancias, un ataque al mismos puede constituir asimismo una lesión al derecho al honor[785].

Un reflejo de dicha distinción puede apreciarse en el artículo 7.7 LOPDH que considera intromisión ilegítima "*la imputación de hechos o la manifestación de juicios de valor a través de las acciones o expresiones que de cualquier modo lesionen la dignidad de otra persona,*

[783] Junto a ella, conviene también mencionar la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal (LOPD) y la Ley Orgánica 2/1984, de 26 de marzo, sobre el derecho de rectificación (LODR) y el Código Penal (delitos contra la intimidad y el derecho a la propia imagen –artículos 197 y siguientes- y calumnias e injurias, como delitos contra el honor –artículos 205 y siguientes-).

[784] Por todas, STS 511/2012, de 24 de julio.

[785] La protección del art. 18.1 CE sólo alcanza "*a aquellas críticas que, pese a estar formalmente dirigidas a la actividad profesional de un individuo, constituyen en el fondo una descalificación personal, al repercutir directamente en su consideración y dignidad individuales, poseyendo un especial relieve aquellas infamias que pongan en duda o menosprecien su probidad o su ética en el desempeño de aquella actividad; lo que, obviamente, dependerá de las circunstancias del caso, de quién, cómo, cuándo y de qué forma se ha cuestionado la valía profesional del ofendido*", STC 180/1999, de 11 de octubre (FJ 5º).

menoscabando su fama –aspecto objetivo- *o atentando contra su propia estimación*" –aspecto subjetivo-.

Así, puede decirse que el bien jurídico protegido por el derecho al honor es el aprecio social, la buena fama o la reputación, en definitiva "el derecho a que otros no condicionen negativamente la opinión que los demás hayan de formarse de nosotros"[786], aunque, sin lugar a dudas, el derecho al honor tiene una íntima conexión con la dignidad de la persona (artículo 10.1 CE).

Aunque conceptualmente es distinto del derecho a la intimidad, hay una evidente conexión entre ambas figuras en tanto que "el honor es la fachada exterior del edificio en cuyo interior se resguarda la esfera privada de la vida de las personas", esto es, honor e intimidad son, respectivamente, la cara interna y externa de la protección de la esfera privada de las personas[787]. Se trata pues de un derecho inherente a la esfera de privacidad de los individuos que, en consecuencia, puede estar o no relacionado, en función del caso en concreto, con la protección de los datos personales en tanto que una inutilización indebida de éstos podría lesionar la reputación de una persona.

Hay que tener en cuenta, como ha advertido la jurisprudencia constitucional, que el contenido del derecho al honor viene determinado por las normas, valores e ideas sociales vigentes en cada momento[788], por lo que puede experimentar variaciones por razón del tiempo y el espacio. Así, la determinación de su contenido resulta un tanto problemático pues la lesión al aprecio social, la buena fama o la reputación varia en función de las pautas sociales de cada momento, así como del margen de apreciación subjetiva de la persona de que se trate.

Procede señalar que, pese a su significado personalista, se permite el ejercicio del derecho al honor, tanto por los herederos de un difunto, cuando se entienda que una

[786] STC 49/2001, de 26 de febrero, FJ 5º.

[787] DÍEZ-PICAZO GIMÉNEZ. *Sistema de derechos Fundamentales*, ob. cit., p. 293.

[788] Por todas, STC 49/2001, de 26 de febrero.

determinada afrenta afecta extensivamente a la reputación de su familia[789], como por parte de las personas jurídicas[790].

En ocasiones este derecho entra en colisión con la libertad de expresión e información pues el derecho al honor se encuentra restringido, especialmente, por los derechos a informar y a expresarse libremente, por lo que en dichas ocasiones procede llevar a cabo un juicio de ponderación entre dichos bienes jurídicos. Para llevar a cabo dicho examen hermenéutico, debe tomarse en consideración la relevancia pública del asunto, el carácter público o privado de la persona sobre la que se emite dicha crítica u opinión, el contexto en el que se producen las manifestación enjuiciables y, por encima de todo, si éstas contribuyen o no a la formación de la opinión pública libre[791].

Ahora bien, el derecho al honor encuentra su límite en el insulto, así, éste opera como un límite insoslayable a la libertad de expresión del artículo 20.1 CE, quedando prohibido que ninguna persona se refiera a otra de forma insultante o injuriosa o atentando injustificadamente contra su reputación, haciéndola desmerecer ante la opinión ajena[792].

7.2. El derecho a la intimidad personal y familiar

La intimidad personal y familiar protege el reducto más privado de la vida del individuo, aquéllos aspectos más personales de su coexistencia y de su entorno familiar, cuyo conocimiento queda restringido a los integrantes del núcleo familiar, este derecho se encuentra reconocido expresamente tanto por la Constitución española como por LOPDH.

Los derechos a la intimidad personal y familiar, reconocidos en el artículo 18 CE, aparecen como derechos fundamentales y personalísimos estrictamente vinculados a la propia personalidad, derivados de la dignidad personal del artículo 10 CE, puesto que son inherentes a la propia existencia del individuo. Es por ello que puede afirmarse que, el derecho a la

[789] STC 190/1996, de 25 de enero.

[790] STC 139/1995, de 26 de septiembre.

[791] Por todas, STC 15/1993, de 18 de enero.

[792] Por todas, STC 297/2000, de 11 de diciembre, FJ 7º.

intimidad personal y familiar encarna un lugar preeminente y el aspecto general central de los derechos recogidos en el artículo 18 CE, mientras que el resto de derechos serían concreciones respecto de aspectos específicos de la vida privada.

Cabe señalar aquí la diferente manera en que operan la intimidad respecto del honor anteriormente analizado, pese a que ambos actúan como potenciales restricciones de las libertades de información y expresión, la intromisión en la intimidad no tiene por que conllevar necesariamente una vulneración del derecho al honor. Se trata de dos bienes jurídicos distintos que se encuentran vinculados a su vez con valores y principios no exactamente idénticos: mientras que con el primero se intenta proteger a la persona de posibles atentados contra su imagen y consideración social, la intimidad se proyecta sobre la esfera general de la vida privada que se quiere excluir del dominio público[793]. Del mismo modo y en relación con una consideración más actual del derecho a la intimidad, parece evidente la relación de la intimidad con el derecho a la protección de datos que, si bien la lesión a este último no tiene porqué conllevar una vulneración de la intimidad personal, si supone una intromisión de su privacidad.

En concreto, el derecho a la intimidad "*implica la existencia de un ámbito propio y reservado frente a la acción y conocimiento de los demás, necesario, según las pautas de nuestra cultura, para mantener una calidad mínima de vida humana*"[794]. Esta definición del Tribunal Constitucional contempla el aspecto negativo y más tradicional del derecho a la intimidad, consistente en la facultad de todo sujeto de excluir todo lo relativo a su propia persona de la acción y conocimiento ajenas; existiendo asimismo una faceta positiva, relativa a la capacidad de todo sujeto de gestionar su reducto más privado, inherente a su propia persona.

El bien jurídico a proteger no se limita exclusivamente al ámbito estricto de su propia persona, sino que la expresión "vida familiar" extiende su garantía a ciertos eventos que puedan ocurrirle a los padres, cónyuges, hijos… de un sujeto en tanto que éstos normalmente, y dentro

[793] RUIZ-RICO RUIZ. "Una exploración necesariamente sintética sobre el concepto y los límites de las libertades de expresión e información" en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. VI, Libro II, Dykinson, Madrid, 2013, p. 1239.

[794] STC 231/1988, de 2 de diciembre , FJ 3º.

de las pautas culturales de nuestra sociedad, trascienden al individuo, por lo que su indebida publicidad o difusión le repercutirá igualmente de forma negativa[795]. En relación a ello, el derecho a la intimidad comprende, en principio, el derecho a conocer la propia filiación, en cuanto a la identidad personal[796].

Del mismo modo la intimidad incluye tanto su faceta "moral" como corporal, "*frente a toda indagación o pesquisa que sobre el cuerpo quisiera imponerse contra la voluntad de la persona, cuyo sentimiento de pudor queda así protegido por el ordenamiento, en tanto que responda a estimaciones y criterios arraigados en la cultura de la comunidad*"[797]. Del mismo modo, se extiende la protección las informaciones relativas a la salud, preferencias y conductas sexuales, a los datos económicos o bancarios de una persona -aunque no de forma absoluta[798]-, y hasta la protección del individuo frente a molestias o ruidos externos que, por su extraordinaria intensidad, hacen imposible la habitabilidad al sujeto afectado[799].

Sin embargo, determinar el alcance exacto de la esfera íntima, elemento esencial para discernir cuándo se produce una intromisión en la misma, es harto complicado, en tanto que su ámbito puede ser susceptible a consideraciones subjetivas de cada individuo y, además, el legislador no ha proporcionado criterios suficientes para su determinación –sólo algunas referencias al uso de aparatos de escucha para acceder a la vida privada de otras personas, o la revelación de datos obtenidos en virtud de una relación profesional-, por lo que ello ha sido hasta ahora tarea de la jurisprudencia.

El Tribunal constitucional, en su tarea interpretativa ha negado la posibilidad de que cada cual determine su propia esfera íntima, siguiendo un criterio material a la hora de delimitar la esfera privada "*íntimo es aquello que ha de poder mantenerse oculto para disfrutar*

[795] STC 197/1991, de 17 de octubre.

[796] Cfr. *STEDH Odièvre v. Francia*, de 13 de febrero de 2003, TEDH 2003/8.

[797]STC 37/1989, de 15 de febrero.

[798] STC 76/1999, de 26 de abril.

[799] STC 119/2001, de 24 de mayo.

de una vida digna y con un mínimo de calidad"[800] pese que, en algunos supuestos como ocurre con los personajes famosos, la previa actitud del interesado puede tener cierta influencia para decidir si una determinada intromisión es ilícita o no[801].

7.3. El derecho a la propia imagen

El derecho a la propia imagen consiste en la facultad de toda persona de decidir respecto al empleo de su imagen, como medio para garantizar la capacidad del individuo de controlar, en la medida de lo posible, la difusión de un elemento tan personal como la propia efigie, de tal forma que no pueda emplearse ésta, con o sin finalidad de lucro, sin su propio consentimiento[802].

Éste ha sido definido por la jurisprudencia constitucional como el derecho a determinar la información gráfica generada por los rasgos físicos personales de su titular que puede tener difusión pública, cuyo objetivo es salvaguardar un ámbito propio y reservado, aunque no íntimo, frente a la acción y conocimiento de los demás[803].

Su protección se encuentra recogida en el artículo 18.1 CE, configurándose como un derecho de la personalidad, derivado de la dignidad humana y dirigido a proteger la dimensión moral del individuo, atribuyéndole a su titular la facultad de determinar la publicidad o no de toda la información gráfica generada por sus rasgos físicos personales. Se trata así de un derecho fundamental, consistente en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, cualquiera que sea su finalidad.

Se garantiza un ámbito de libertad para el sujeto "*respecto de sus atributos más característicos, propios e inmediatos como son la imagen física, la voz o el nombre, cualidades definitorias del ser propio y atribuidas como posesión inherente e irreductible a toda*

---

[800] STC 231/1988, de 2 de diciembre, FJ 3º.

[801] DÍEZ-PICAZO GIMÉNEZ. *Sistema de derechos Fundamentales*, ob. cit., pp. 286 ss.

[802] Cfr. PÉREZ TREMPS. *Derecho constitucional. El ordenamiento constitucional. Derechos y deberes de los ciudadanos*, ob. cit., p. 204.

[803] Por todas, STC 23/2010, de 27 de abril.

persona"[804] pues se entiende que la imagen de una persona forma parte de la esfera personal de todo individuo en tanto que permite su identificación. No obstante, además de su faceta privada, el derecho a la imagen tiene un elemento extrínseco relativo a la evocación social de toda persona que se plasma a través de su aspecto.

Puede distinguirse así, entre un contenido positivo y otro negativo de dicho derecho. Éste último consiste en la facultad de impedir que terceras personas obtengan, reproduzcan o divulguen la imagen de una persona sin su consentimiento, mientras que la faceta positiva estriba en la facultad del propio sujeto de decidir acerca de la reproducción y divulgación de su imagen, lo que incluye la posibilidad de comercializar con ella. Este último aspecto ha servido a muchos autores para distinguir en este derecho dos vertientes distintas, una relativa a la protección de la personalidad, y otra relativa a su contenido patrimonial[805].

Como pasa con el derecho a la intimidad, el derecho a la propia imagen es permeable a sufrir variaciones en función del comportamiento de cada persona que puede determinar la extensión de la protección de un determinado derecho así, por ejemplo, la participación en determinadas actividades públicas priva de legitimidad al sujeto para reclamar contra la utilización de su propia imagen, pues dicho derecho "*se encuentra delimitado por la propia voluntad del titular del derecho que es, en principio, a quien corresponde decidir si permite o no la captación o difusión de su imagen por un tercero*"[806].

Así, en tanto que diverge de las circunstancias, su contenido puede quedar amparado por el interés informativo del mismo modo que su extensión difiere según las personas en concreto de las que se trate por lo que, pese a estar relacionado con los conceptos de intimidad y reputación, su protección se extiende incluso cuando no afecte a dichos ámbitos. También este derecho se encuentra relacionado con la protección de la dignidad humana y de un ámbito libre de intromisiones ajenas, pues en última instancia su garantía tiene como objeto la autodeterminación consciente del ser humano con total libertad.

---

[804] STC 117/1994, de 25 de abril, FJ 3º.

[805] MARTÍNEZ DE AGUIRRE ALDAZ, C. "Los derechos de la personalidad", ob. cit., p. 269.

[806] Por todas, STC 156/2001, de 2 de julio, FJ 6º.

Destacar también la inevitable relación del derecho a la protección de datos con el derecho a la propia imagen en tanto que ambos derechos afectan a la privacidad del individuo así como que, en el ámbito de Internet, una imagen se asemeja a un dato personal pues permite identificar a una persona. Publicar en la Red una fotografía que reproduzca la imagen de una persona de forma claramente identificable, sin su consentimiento, legitima al sujeto de que se trate para accionar los mecanismos jurídicos previstos para obtener el borrado de dicha imagen así como un resarcimiento en caso de haber sufrido daños o perjuicios.

Como afirma DÍEZ-PICAZO GIMÉNEZ, existe una contraposición entre la concepción tradicional del derecho a la propia imagen, entendida como una manifestación o faceta del derecho a la intimidad y al honor, con íntima conexión con la dignidad humana, lo que conduce a proclamar la imposibilidad de reconocer dicho sujeto a las personas jurídicas o su extinción con la muerte de su titular; y una concepción más actual según la cual se trata de un derecho fundamental autónomo del derecho al honor y a la intimidad, por lo que el aspecto físico de una persona resulta protegido incluso cuando, habida cuenta de sus circunstancias, no tiene nada de íntimo o no afecta a su reputación[807].

Por último, señalar que el derecho a la imagen puede mostrarse en conflicto con el derecho a la libertad de expresión, principalmente cuando se trata de una persona de naturaleza pública o de un espacio público y en relación a ello, el Tribunal Constitucional ha otorgado a la libertad de información por medio de la imagen, la misma protección constitucional que la libertad de comunicar información por medio de palabras escritas u oralmente vertidas[808].

7.4. El derecho a la protección de datos personales

Como ya se ha apuntado en páginas anteriores, el derecho a la protección de datos –o a la autodeterminación informativa, como lo llaman algunos autores- es un derecho fundamental por sí mismo, consistente en la "*libertad frente a las potenciales agresiones a la dignidad y a*

[807] Cfr. *Sistema de derechos Fundamentales*, ob. cit., p. 291.

[808] Cfr. STC 132/1995, de 11 de septiembre.

la libertad provenientes del uso ilegítimo de datos mecanizados"[809] y cuyo bien jurídico protegido es la libertad del individuo frente a los abusos de la informática y del tratamiento automatizado de datos personales.

Pese a la referencia del artículo 18.4 CE a la limitación de la informática, en el que hoy en día se entiende insertado el derecho a la protección de datos, puede decirse de éste que es una figura jurídica relativamente reciente pues es desde hace unas décadas cuando se desarrolla formalmente la doctrina y jurisprudencia a su respecto. El legislador constituyente se avanza al futuro al prever el apartado cuarto del artículo 18 y gracias a dicha previsión constitucional y mediante la STC 292/2000, de 30 de noviembre, se reconoció el carácter fundamental y autónomo del derecho a la protección de datos personales -principalmente debido a su íntima relación con la dignidad humana- una vez las circunstancias tecnológicas y sociales lo aconsejaron. Su regulación material se encuentra en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal cuyo objeto, tal y como indica su artículo 1, es "*garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*".

Como señala GARRIGA DOMÍNGUEZ, pronto se constató que la tecnología de procesamiento de datos personales supone claros peligros para la libertad, para el derecho a no ser discriminado y para la propia dignidad personal, y dichos riesgos van mucho más allá de la mera protección de la intimidad personal o familiar. Por su propia concepción, el desarrollo tecnológico de la segunda mitad del siglo XX hizo insuficiente el derecho a la intimidad para dar respuesta a los riesgos que se sucedían para los derechos fundamentales, principalmente debido a las posibilidades de tratamiento automatizado de la información personal, lo que hizo imprescindible la creación de un nuevo derecho fundamental, esto es, el derecho a la protección de datos personales, como instrumento de garantía[810].

[809] STC 254/1993, de 20 de julio.

[810] Cfr. "Nuevas tecnologías, derecho a la intimidad y protección de datos personales" en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. VI, Libro II, Dykinson, Madrid, 2013, p. 897.

Pueden discernirse dos facetas de este mismo derecho, una negativa, en cuanto a la imposición de límites por parte de los poderes públicos o entidades privadas sobre el almacenamiento, tratamiento y difusión de los datos personales; y una vertiente positiva, relativa a la posibilidad del titular de los datos de acceder a ellos, instar su corrección en el supuesto de que éstos sean falsos o erróneos, oponerse a su tratamiento o solicitar su cancelación en caso de que se esté llevando a cabo una utilización ilegítima o abusiva de ellos e, íntimamente relacionado con ello, faculta al interesado para ejercitar el derecho al olvido frente a sus datos personales para que éstos sean borrados digitalmente.

Así, el derecho de datos en su vertiente positiva ha recibido la denominación de *habeas data*, pues en sus principios de calidad de los datos y del consentimiento, determina cómo, en qué circunstancias y hasta qué momento pueden tratarse los datos personales. Dentro de la calidad de los datos se encuentra el principio de finalidad, que exige la existencia de una finalidad legítima y que los datos personales sean cancelados desde el momento en que han dejado de ser necesarios para la finalidad para la que fueron recogidos y tratados. Y es precisamente, en este principio de finalidad que permite que se cancelen los datos cuando no exista finalidad legítima que justifique el tratamiento, en el cual, según SIMÓN CASTELLANO, reside el fundamento más fuerte del derecho al olvido[811].

Ciertamente, el derecho a la protección de datos es el fundamento principal del actual derecho al olvido pues, pese a la flexibilidad y adaptabilidad que hasta ahora había demostrado el derecho a la protección de datos personales, y que había ocasionado que toda la problemática de las nuevas tecnologías se resolviese mediante éste, dado el avance de la técnica y la informática actual, no podía prolongarse mucho más sin desvirtuar el contenido propio de dicho derecho, por lo que se reclamaba la creación de un nuevo derecho fundamental, esto es el derecho al olvido, capaz de dar cobertura jurídica a la realidad vigente, mucho más amplia y compleja.

[811] Cfr. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, ob. cit., p. 293.

7.5. El derecho a la dignidad personal y al libre desarrollo de la personalidad

En el origen de los derechos fundamentales se halla la dignidad humana, así lo ha declarado el Tribunal Constitucional, afirmando que se trata de un valor jurídico fundamental que actúa a modo de germen o núcleo "*que le son inherentes*"[812], en consonancia con el artículo 10.1 CE que dispone "*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*".

Pese a que en nuestro ordenamiento jurídico no se reconoce material y procesalmente como un derecho fundamental, ésta se erige como fuente y razón de los mismos, actuando como principio inspirador pues deviene el punto de referencia de todas las facultades que se dirigen al reconocimiento y afirmación de la dimensión moral de la persona[813]. Sobre la relevancia y significación de la dignidad en el sistema constitucional ha dispuesto el Tribunal Constitucional que se considera "*el punto de arranque, como el prius lógico y ontológico para la existencia y especificación de los demás derechos*"[814].

Así las cosas, su valor como fundamento de los derechos humanos es incuestionable[815] y tiene consecuencias que perfilan no sólo el respeto, sino además la protección y la promoción de la personalidad[816]. Ello implica que los derechos y las libertades fundamentales se configuran como garantías subjetivas de los individuos que no pueden verse limitados ni condicionados por interferencias o impedimentos externos que coarten su libre desarrollo.

---

[812] STC 120/1990, de 27 de junio, FJ 4º.

[813] Cfr. GUTIÉRREZ GUTIÉRREZ. *Dignidad de la persona y derechos fundamentales*, Marcial Pons, Madrid, 2005.

[814] STC 53/1985, de 11 de abril, FJ 3º.

[815] Así lo recogen la mayoría de las constituciones así como numerosos textos internacionales, entre ellos, la Declaración Universal de Derechos Humanos de 1948 con constantes referencias a la dignidad, como su preámbulo que dispone "*el reconocimiento de la dignidad intrínseca y de los derechos iguales e inalienables de todos los miembros de la familia humana*" o la Carta Europea de Derechos Fundamentales de 2000, la cual dedica su Título I a la dignidad, a quien vincula cuatro derechos: el derecho a la vida, el derecho a la integridad de la persona, la prohibición de la tortura y de las penas o tratos inhumanos o degradantes y la prohibición de la esclavitud y del trabajo forzado.

[816] GONZÁLEZ PÉREZ. *La dignidad de la persona*, Civitas, Madrid, 2017, p. 61.

Partiendo de esta base, ya ha quedado patente como la nueva realidad sociotecnológica supone un riesgo para los derechos fundamentales de las personas y, en dicho contexto, la dignidad actúa como dique de contención para que la autodeterminación del sujeto sea totalmente libre, en lo que PÉREZ LUÑO ha descrito como "la autodeterminación que surge de la libre proyección histórica de la razón humana, antes que de una predeterminación dada por la naturaleza de una vez por todas"[817].

Esta autodeterminación implica necesariamente un poder de los individuos de control de sus datos personales, de decidir cuándo y centro de qué limites procede revelar situaciones o aspectos de su propia vida, pues es precisamente en esa "autodeterminación consciente y responsable" del sujeto, donde radica el derecho fundamental a la protección de datos de carácter personal[818] y, en consecuencia, el derecho al olvido.

El Tribunal Constitucional se ha referido asimismo a la vinculación de la dignidad con la autonomía y la libertad del individuo disponiendo 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*"[819] reconociendo así la existencia de ciertos derechos que corresponden al individuo por el mero hecho de ser persona.

Y es que no sólo existe una indudable conexión entre la dignidad y la autodeterminación personal, sino que la concepción moral de los derechos de la persona viene dada por la consideració del derecho de libertad como vehículo para alcanzar la dignidad, como dispuso FROSINI "la libertad informativa representa una nueva forma de desarrollo de la libertad personal; no consiste únicamente en la libertad negativa del *right of privacy* […] sino que

[817] Cfr. *Teoría del derecho. Una concepción de la Experiencia Jurídica*, Tecnos, Madrid, 2012, p. 225.

[818] DEL CASTILLO VÁZQUEZ. *Protección de datos: cuestiones constitucionales y administrativas. El derecho a saber y la obligación de callar*, ob. cit., p. 138.

[819] STC 53/1985, de 11 de abril, FJ 4º.

consiste también en la libertad de informarse, es decir, de ejercer un control autónomo sobre los datos propios, sobre la propia identidad informática"[820].

Parece claro pues, que el fin último que el derecho al olvido persigue, junto con los bienes jurídicos anteriores, una protección de la dignidad, como fundamento inherente de los anteriores, proporcionando a los individuos un control sobre su privacidad, permitiéndoles tomar decisiones sobre el uso de su información personal para evitar o corregir lesiones a su dignidad personal.

Al igual que el Tribunal Constitucional consagró en el artículo 18.4 CE el derecho fundamental a la protección de datos, en base a la dignidad humana del articulo 10.1 CE[821], como derecho autónomo del derecho a la intimidad y con un contenido esencial propio que lo define y caracteriza, parece lógico pues que el derecho al olvido se configure asimismo como garantía independiente de la privacidad del individuo teniendo en cuenta la interconexión entre ambas figuras. De este modo, la dignidad humana constituye no sólo la garantía negativa de que la persona no va a ser objeto de injerencias no deseadas de terceros, sino que se reafirma como una libertad positiva para el pleno desarrollo de la personalidad de cada individuo.

Procede recordar aquí que el honor, la intimidad y la propia imagen han sido considerados por la teoría jurídica tradicional como manifestaciones de los derechos de la personalidad[822] y, en el sistema actual de los derechos fundamentales, como expresiones del valor de la dignidad humana. Procede añadir a dicho grupo, el derecho a la protección de datos personales así como el derecho al olvido, como miembros integrantes del conjunto de lo que podríamos denominar los "derechos de la privacidad".

En definitiva, el honor, la intimidad, el derecho a la propia imagen y la protección de datos personales son derechos fundamentales que operan de manera distinta pues, por ejemplo, la intromisión en la intimidad no tiene porqué conllevar una vulneración del derecho a la propia

[820] FROSINI, V. *Informática y Derecho*, Temis, Bogotá, 1988, p. 23.

[821] Por todas, STC 254/1993, de 20 de julio.

[822] PÉREZ LUÑO. "El derecho al honor y a la intimidad", en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. I, Libro II, Dykinson, Madrid, 2013, p. 1063.

imagen ni la protección de datos personales se activa cuando se quebranta asimismo el derecho al honor[823]. Éstos tienen, en mayor o menor medida, una íntima conexión con la figura del derecho al olvido, se trata, en cierto modo, de bienes jurídicos distintos aunque íntimamente relacionados[824], pues todos ellos inciden en la esfera de la privacidad de los individuos y comparten unos valores y principios comunes que, en última instancia, protegen la dignidad de las personas y el Estado social y democrático de Derecho.

8. Contenido

Tradicionalmente los derechos fundamentales se han clasificado dos categorías: los derechos de libertad y los derechos de prestación. Así, mientras que los primeros (como el derecho de reunión o la libertad de expresión) conceden al individuo una esfera libre de injerencias externas -lo que conlleva para los poderes públicos una acción negativa-, los segundos (como el derecho a la educación) requieren de la Administración pública una intervención positiva para hacer efectivos los derechos reconocidos a los ciudadanos.

Teniendo en cuenta esta distinción clásica, el derecho al olvido parece encajar mejor en la primera de las categorías pues, con él, se pretende dotar al individuo de un poder real para la autogestión de sus datos personales, posibilitándole una salvaguarda para su vida privada. Sin embargo, esta clasificación de los derechos fundamentales tiene un sentido meramente académico y no refleja fielmente la realidad, mucho más compleja, en la que ambas figuras se entremezclan constantemente siendo imposible una disociación total y absoluta entre ambas categorías, en lo que se ha denominado "la continuidad entre derechos de libertad y derechos de prestación" [825].

[823] STC 156/2001, de 2 julio, FJ 3º.

[824] "*Si bien todos los derechos identificados en el art. 18. CE mantienen una estrecha relación, en tanto que se inscriben en el ámbito de la personalidad, cada uno de ellos tiene un contenido propio y específico*", STC 208/2013, de 16 de diciembre, FJ 3º.

[825] DÍEZ-PICAZO GIMÉNEZ, por su parte, distingue entre derechos de defensa (los que facultan a su titular a la no interferencia ajena), derechos de participación (que le facultan a realizar actos con relevancia pública) y derechos de prestación (que lefacultan a reclamar un beneficio) y, reconoce también, que dichas clasificaciones son meras generalizaciones pues sus compartimentos no son estancos por lo que debe de estarse al régimen concreto de cada derecho. Cfr. *Sistema de derechos Fundamentales*, ob. cit., pp. 35 y 36.

Asumiendo como cierta la conexión entre ambas categorías, el contenido del derecho al olvido no permanece ajeno a esta concordancia pues, si bien predomina su faceta de libertad para que el individuo pueda autónomamente administrar su información personal y pueda salvaguardar ciertas facetas privadas frente a otras personas; lo cierto es que requiere de la acción del poder público (para la reglamentación jurídica así como para ejercitar la potestad sancionadora) así como de otras personas jurídicas particulares (los encargados del tratamiento de datos, por ejemplo, quienes deben de actuar con transparencia y con sujeción a la legalidad, y a quienes el GDPR les exige una conducta de "responsabilidad proactiva").

Asimismo, como más tarde se examinará, el derecho al olvido encuentra sus límites en la colisión con otros derechos fundamentales, por lo que la "libertad" inherente a su contenido es susceptible de intromisiones y no se puede afirmar en términos absolutos. De este modo, el Estado no sólo debe velar para que una persona pueda realizar con éxito su derecho de supresión, sino que también ha de permitir que otros puedan ejercer correctamente su derecho de expresión o su libertad de información[826].

Por otro lado, podría decirse que el derecho al olvido tiene una doble naturaleza –subjetiva y objetiva- pues, por una parte se protege la propia percepción de si mismo como sujeto libre para desarrollar su personalidad sin injerencias externas –incluyendo aquí su propia consideración sobre la estima y los límites de la privacidad- y, de otra, la que le otorga la propia comunidad, manifestada principalmente a través de la reputación.

Puesto que el derecho al olvido, según ya se ha defendido, deriva en última instancia del valor de dignidad humana, éste debería protegerse con igual grado de intensidad, al margen de las circunstancias subjetivas u objetivas del titular del derecho. Sin embargo, dado el contexto concreto en que se produce la interacción del derecho al olvido, ello debe ponerse en relación con las condiciones propias en que éste tiene lugar pues, igual que en el derecho a la propia

[826] Señala PÉREZ TREMPS que la conexión entre las diferentes categorías de derechos no es sólo técnica sino que desde el punto de vista ideológico y conceptual tampoco es posible una separación drástica entre derechos pues, siguiendo la categorización entre derecho de libertad y derechos de prestación, ambos representan manifestaciones básicas del Estado de Derecho que ha pasado del abstencionismo del Estado liberal al intervencionismo del Estado social. Cfr. *Derecho constitucional. El ordenamiento constitucional. Derechos y deberes de los ciudadanos*, ob. cit., p. 131.

imagen, debe tenerse en cuenta la naturaleza pública o privada del sujeto en cuestión así como la relevancia de la información que se pretende suprimir, el transcurso del tiempo o incluso si ésta se ha proporcionado por el propio interesado o por terceros.

El contenido del derecho al olvido viene determinado por el Reglamento europeo de protección de datos -anteriormente ya comentado- el cual contempla, por vez primera y de forma expresa, el derecho de toda persona a que se supriman sus datos personales digitales.

Así, el artículo 17 GDPR dispone:

> 1. *El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando 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 de otro modo;*
>
> *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".*

2. "Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, 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.

Así, todo interesado, esto es, toda persona física cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador -como por ejemplo "*un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*"(artículo 4.1 GDPR)- puede solicitar frente al responsable del tratamiento – "*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento*"(art. 4.7 GDPR)- la supresión de aquéllos datos personales que representen cualquier información sobre su persona cuando se den las circunstancias previstas en el art. 17.1 del Reglamento.

Respecto de las situaciones concretas que deben tener lugar para proceder a la supresión de los datos, deben hacerse algunas aclaraciones. En primer lugar, en cuanto al apartado *a)*, referido a los datos que ya no sean necesarios para el cumplimiento de los fines para los que fueron recogidos o tratados en origen, ello se vincula directamente al principio de proporcionalidad y finalidad de los datos. En base a dichos principios, un tratamiento en principio lícito por llevarse a cabo conforme a todos los requisitos legales, puede dejar de serlo por el mero transcurso del tiempo.

Pasando al apartado *c)*, éste alude a la posibilidad de que el interesado se oponga al tratamiento conforme al derecho de oposición, el cual viene regulado en el artículo 21 del GDPR y que guarda ciertas similitudes con el derecho de supresión pese a que éste no supone el borrado de los datos, sólo pone fin a su tratamiento.

El apartado *d)* por su parte, prevé el ejercicio del derecho al olvido como reacción ante un caso de tratamiento ilícito[827] lo que exige asimismo, un deber de transparencia y lealtad en el tratamiento –art. 5.1.a) GDPR-.

Por último, conviene clarificar el apartado *f)* que hace remisión al artículo 8.1 GDPR referido al consentimiento de los menores para el tratamiento de datos personales. En concreto, dicho precepto dispone que para que el tratamiento de datos personales de un menor sea lícito, éste debe tener mínimo 16 años o, siendo menor de dicha edad, contar con el consentimiento de ambos padres titulares de la patria potestad o tutela[828]. A continuación, dispone el precepto que "*los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años*", en el caso español dicha edad está fijado en 14 años[829].

En relación a esta cuestión, el considerando 65º del Reglamento prevé expresamente la posibilidad de ejercitar el derecho al olvido en aquellos casos en que una persona, siendo menor de edad, prestase el consentimiento idóneo para el tratamiento de datos y, habiendo alcanzado ahora ya mayoría de edad, quiera suprimir tal información personal[830].

En otro orden de cosas, y para el caso de que el titular ejercite correctamente el derecho al olvido así como que se den las circunstancias legales concretas existen dudas acerca del alcance concreto que puede llegar a tener la supresión solicitada. Mientras que del tenor literal

---

[827] Para que un tratamiento sea lícito, dice el artículo 6.1 GDPR, que debe cumplir alguna de las circunstancias siguientes: "*a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño*".

[828] Ello supone una modificación del régimen dispuesto hasta entonces por la LOPD pues el Reglamento europeo obliga necesariamente a que ambos progenitores presten el consentimiento cuando se tenga la patria potestad o la tutela compartida, no bastando con el de uno de ellos solamente.

[829] Artículo 13 del Real decreto 1720/2007, de 21 de diciembre, por el que se aprueba el reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[830] "*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*".

del artículo 17.1 GDPR parece desprenderse que, un ejercicio adecuado del derecho al olvido permitiría obtener el borrado de los datos personales solicitados de la webmaster u otra fuente original, respecto del ejercicio del derecho de supresión frente a los buscadores web, la sentencia del *caso Google*[831] limitó la pretensión del interesado a los resultados obtenidos en las búsquedas llevadas a cabo mediante la introducción del nombre de una persona. En consecuencia, una vez ejercitado y estimado el derecho efectivo, ello implicaría que, realizado dicha búsqueda con los mismos parámetros, la información en cuestión dejaría sólo de ser visible, lo que no impediría mostrar los resultados lesivos cuando la búsqueda se lleve a cabo mediante cualquier otra palabra o término distinto, al permanecer inalteradas las fuentes de origen.

Entendemos que dicha limitación dispuesta por el TJUE obedece al origen embrionario del derecho al olvido y se circunscribe al supuesto de hecho concreto pero que, con la regulación expresa del derecho de supresión en el GDPR su contenido se ha ampliado notoriamente para proteger de forma efectiva el control sobre sus datos personales[832]. Por el contrario, circunscribir el alcance del derecho al olvido al mero borrado de los resultados ofrecidos por un buscador, basados exclusivamente según los parámetros de búsqueda proporcionados por el interesado y cuando se haga referencia a su nombre y apellidos[833], supondría cierta indefensión para el interesado pues, por una parte le obligaría a interponer tantas nuevas pretensiones como variables existieren que proporcionasen el resultado lesivo de derechos, y de otra, porque en consecuencia, dicha información no desaparecería nunca de Internet.

---

[831] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

[832] Una prueba del carácter evolutivo del derecho al olvido es la *Guidelines on the implementation of the Court of Justice of the European Union Judgment on "Google Spain an Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"* que dictó el Grupo de Trabajo del artículo 29 para establecer las ideas básicas sobre las que se versaba el fallo del caso Google así como sus consecuencias jurídicas. En él, no se hace mención alguna al derecho al olvido sino que se emplean términos como "*de-listing*" o remoción de una lista como denominación provisional del ahora derecho de supresión o al olvido.

[833] Esto fue ampliado por las "*Guidelines on the implementation of the Court of Justice of the European Union Judgment on "Google Spain*" del Grupo de Trabajo del artículo 29, antes mencionadas, a las búsquedas mediante pseudónimos o apodos ligados indiscutiblemente a la identidad del interesado.

Así las cosas, suscribimos la tesis según la cual, el contenido del derecho al olvido permite al interesado obtener el borrado de la información en su fuente original –siempre que ello sea posible técnicamente y cuando no se vulneren otros derechos fundamentales con los que entre en posible colisión, ni tampoco otros límites-[834]. Ello viene ciertamente sustentado por el segundo apartado del artículo 17 GDPR así como por su considerando 66º en el que se dispone que el responsable del tratamiento está obligado a indicar a los responsables del tratamiento que estén tratando los datos personales que éste haya hecho públicos, para que supriman todo enlace a ellos, así como 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[835], para informar de la solicitud del interesado a los responsables que estén tratando también sus datos personales.

Se refuerza así el derecho al olvido en el entorno en línea, ampliándose de tal manera que no sólo el responsable de dicho tratamiento al que se ha acudido en primer lugar debe suprimir los datos personales del interesado sino que éste debe de comunicarle al resto de responsables que, al estar nutriéndose de la misma base de datos, están tratando dicha información personal del interesado, que lleven a cabo la supresión igualmente de las copias, réplicas o *links* correspondientes o, de lo contrario, serán responsables por los daños que de ello se deriven.

Así, podría decirse que el régimen del artículo 17.1 GDPR es multidireccional, en tanto que se aplica a varios destinatarios, y unívoco , pues se emplea el mismo régimen a todos ellos. De este modo, el derecho al olvido recae sobre cualquier responsable del tratamiento de los datos, a quienes se les atribuye el deber de atender las reclamaciones que, en el ejercicio del

[834] BERROCAL LANZAROT suscribe esta postura "quien debe suprimir los datos inexactos cuando se den las circunstancias previstas en el artículo 17.1 es todo responsable del tratamiento, por lo que no solo se circunscribe como la sentencia de Tribunal de Justicia de la Unión Europea en el caso Google al motor de búsqueda, sino a cualquier responsable que trate datos (redes sociales, blogs, páginas web, hemerotecas, etc.)". Cfr. *Derecho de supresión de datos o derecho al olvido*, ob. cit., p. 228.

[835] Entre dichas medidas se encuentra el uso de protocolos de exclusión como *robot.txt* o de códigos como *noindex* o *noarchive*, así como el uso de etiquetas metas, el empleo de estrategias *digital ephemerality* o cualquier sistema de encriptación de los datos cuya función sea la autodestrucción. Cfr. SIMÓN CASTELLANO. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, ob. cit., pp. 279-280.

derecho al olvido, se formulen contra ellos y, en consecuencia, el interesado puede dirigirse contra cualquiera de los intervinientes: webmaster, motores de búsqueda, editores de redes sociales, responsables de hemerotecas digitales, etc.

Surge aquí nuevamente el problema respecto del alcance de la eficacia del derecho al olvido, si bien no hay duda cuando el interesado se dirige en primer lugar contra la webmaster o la fuente de origen para llevar a cabo el derecho al olvido y, en consecuencia ésta deberá de hacérselo saber al resto de responsables de tratamiento que estén empleando los datos de la fuente original, para que lleven a cabo e cumplimiento del derecho de supresión; podría dudarse de la eficacia del proceso inverso[836].

Como ya se ha visto antes, las "*Guidelines on the implementation of the Court of Justice of the European Union Judgment on "Google Spain*" del Grupo de Trabajo del artículo 29, pueden llevar a pensar que los motores de búsqueda no deben, como práctica general, informar a los webmasters de las páginas afectadas. Sin embargo, los motores de búsqueda, aunque de forma indirecta, hacen públicos los datos personales de los interesados publicados por terceros al ponerlos a disposición de quien los quiera consultar, multiplicando exponencialmente el alcance y los efectos de la publicación original.

Por ello, la concepción anterior debe superarse actualmente por obsoleta pues, el transcurso del tiempo así como el desarrollo de la doctrina y jurisprudencia a tal efecto y, principalmente, el texto final del GDPR, permiten sostener todo lo contrario[837], y así resulta

[836] Así lo hace la AEPD que, en su resolución de 14 de octubre de 2016 (RAEPD 2232/2016) dispone en relación al artículo 17.2 GDPR que "*ante todo, cabe señalar que este artículo no sería aplicable a la actividad del motor de búsqueda, toda vez que Google no 'ha hecho públicos los datos', puesto que lo eran al menos desde el momento en que los webmasters los incorporaron a sus páginas web. En cualquier caso, este artículo no puede entenderse sino como una regla para los casos en que el responsable de un tratamiento ha comunicado los datos mediante su difusión pública y debe informar a los posibles destinatarios de la voluntad del interesado de que esos datos sean suprimidos*" (FJ 5º).

[837] Una opción intermedia entre ambas posturas es la que propone DI PIZZO CHIACCHIO según la cual, los motores de búsqueda sólo tendrían que cumplir el deber de comunicación entre responsables que establece el artículo 17.2 GDPR cuando hayan hecho públicos los datos y cuando deban suprimirlos por alguna de las causas previstas en el Reglamento. Cfr. *La expansion del derecho al olvido digital. Efectos de "Google Spain" y el Big Data e implicaciones del nuevo Reglamento Europeo de Protección de Datos*, ob. cit., p. 270.

pertinente para una mayor salvaguarda de los derechos de los interesados[838]. No obstante, el artículo 70.1.d) GDPR deja en manos del Comité Europeo de Protección de Datos la función de emitir "*directrices, recomendaciones y buenas prácticas relativas a los procedimientos para la supresión de vínculos, copias o réplicas de los datos personales*".

De hecho, la extensión de la garantía se observa en el hecho de que el Reglamento europeo de datos exige del responsable del tratamiento de datos una conducta de "responsabilidad proactiva" lo que implica que, de *motu propio* y de forma activa, debe dar cumplimiento a la normativa de protección de datos así como evitar posibles quebrantos de la regulación a tal efecto, como así lo señala el artículo 5.2 del GDPR "*El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)*"[839].

9. Límites

Los derechos fundamentales no son derechos absolutos que puedan ejercitarse incondicionalmente frente a todos y en todas las situaciones pues su ejercicio, tal y como ha establecido reiteradamente el Tribunal Constitucional[840], está sujeto a límites necesarios para salvaguardar la garantía y la coherencia de todo el conjunto del ordenamiento jurídico.

Pueden señalarse dos tipos de límites de los derechos fundamentales, aquéllos comprendidos expresamente en la Constitución que, a su vez, pueden establecerse con carácter general (lo que el artículo 10.1 CE llama "*el ejercicio de los derechos de los demás*") o bien para un derecho en concreto (por ejemplo, la persecución de un delito flagrante como límite a

[838] No se es ajeno a las proporciones de la labor de control y comunicación que deberán llevar a cabo los motores de búsqueda, lo que conlleva sin duda una gran inversión en capital económico y humano, pero todo ello es necesario y justificable en aras de un cumplimiento riguroso de los derechos y las libertades contempladas en el GDPR.

[839] El principio de responsabilidad proactiva, se manifiesta asimismo en otros mecanismos previstos en el Reglamento, como la elaboración de códigos de conducta o la implementación de instrumentos de certificación en materia de protección de datos –artículo 40 y 42, respectivamente-.

[840] "*La Constitución establece por si misma los límites de los derechos fundamentales en algunas ocasiones. En otras ocasiones, el límite del derecho deriva de la Constitución sólo de una manera mediata o indirecta, en cuanto que ha de justificarse por la necesidad de proteger o preservar no sólo otros derechos constitucionales, sino también otros bienes constitucionalmente protegidos*" STC 11/1981, de 8 de abril.

la inviolabilidad del domicilio), y aquellos otros que, sin estar expresamente comprendidos, derivan de su propia naturaleza[841].

Estas últimas restricciones se desprenden de la jurisprudencia constitucional que, en su tarea de interpretación, acota los derechos y las libertades fundamentales y los adecua a la realidad social imperante así como los perfila en relación con situaciones concretas. Sin embargo, establecer límites a los derechos fundamentales no supone violar el contenido esencial de los mismos que debe preservarse en todo caso para no desvirtuar el sentido de los bienes jurídicos que protege.

No obstante, la existencia de restricciones para los derechos fundamentales no implica que no deba hacerse una interpretación lo más generosa y amplia que sea posible pues, en cuanto a los límites de los derechos fundamentales se refiere, debe tenerse en cuenta, en primer lugar, el principio de optimización de los derechos fundamentales, el cual exige maximizar su eficacia, otorgándoles la mayor efectividad posible que permitan las circunstancias concretas del caso. Así, en el supuesto de que no exista colisión alguna con otros valores protegidos, no hay motivos para imponer ningún tipo de restricción a la completa virtualidad de un derecho fundamental.

Sin embargo, esto no siempre es posible pues puede darse el caso en que distintos valores jurídicamente protegidos entren en conflicto y, en consecuencia, los derechos no puedan desplegar sus efectos en toda su extensión. En esta situación, se debe llevar a cabo una ponderación entre los intereses en juego, estableciendo una evaluación del supuesto de hecho que permita encontrar una situación de equilibrio entre distintos derechos fundamentales.

Esta ponderación exige en primer lugar -y sobre todo para evitar caer en el subjetivismo- hacer un cuidadoso análisis de los aspectos fácticos y jurídicos del caso concreto, que permita

[841] Junto a estas categorías, PÉREZ TREMPS distingue una más: los límites internos de los derechos fundamentales comprendidos por aquéllas restricciones inherentes a la propia definición del derecho que se trate, cuya definición "sólo puede provenir de los operadores jurídicos; al legislador le corresponde fijar esas fronteras en la regulación de os derechos fundamentales; los tribunales tienen que controlar que dicho trazado sea correcto, completándolo y adecuándolo ante las exigencias de la cambiante realidad social". Cfr. *Derecho constitucional. El ordenamiento constitucional. Derechos y deberes de los ciudadanos*, ob. cit., p. 137.

extraer cuales son los puntos de conflicto entre valores así como hallar eventuales confluencias. No encontrando solución que evite la colisión, en segundo lugar, es preciso determinar cual de los valores en conflicto es más digno de protección, teniendo en cuenta el grado en que cada uno de los bienes jurídicos en colisión se ve afectado y la proximidad al núcleo de su significado[842].

En cuanto al derecho al olvido, éste no está exento de limitaciones como se deriva de su peculiar naturaleza así como de su objeto y el carácter poliédrico de los bienes jurídicos que tutela. Así, al igual que el derecho al honor y a la intimidad, el derecho de supresión actúa como potencial restrictivo de la libertad de información y expresión[843].

Las características aparejadas a los derechos de la personalidad hacen que de éstos se desprenda una notable restricción al radio de acción de la autonomía de la voluntad. En algunos casos, el ordenamiento jurídico dispone de manera específica la nulidad de los actos y negocios jurídicos que vulneren los derechos de la personalidad y en otras ocasiones recurre a la cláusula genérica del artículo 1.255 CC según la cual la autonomía privada estará limitada por el respeto al orden público, la moral y a las buenas costumbres[844].

Ante la conflictividad de distintos derechos fundamentales, no deben preestablecerse reglas jurídicas muy concretas o detalladas para interponer limitaciones, pues ello conllevaría a soluciones injustas para según qué casos. En su lugar, se exige llevar a cabo una operación hermenéutica, de carácter casuístico, mediante los denominados test de razonabilidad y ponderación -que hoy se atribuyen a la labor jurisprudencial- cuyo resultado no tiene que conducir necesariamente a un equilibrio exacto entre los valores en conflicto, como tampoco existe una prevalencia ni superioridad de unos derechos frente a otros.

---

[842] DÍEZ-PICAZO GIMÉNEZ. *Sistema de derechos Fundamentales*, ob. cit., pp. 46-47.

[843] Ello se contempla expresamente en el apartado *b)* del artículo 17.3 del GDPR.

[844] Esta cláusula abierta, llena de conceptos jurídicos indeterminados, permite la modulación del contenido por parte del juzgador, que se ve obligado a interpretar las circunstancias concretas del caso según el contexto del mismo lo que, por un lado, posibilita adaptar el contenido del precepto a nuevas realidades y, de otro, permite modular la rigidez de las limitaciones en relación con algunos derechos de la personalidad, como la intimidad o el derecho al olvido.

Mediante la técnica de la ponderación, se pretende hallar un equilibrio entre los diversos intereses en juego[845], sin que del juicio de valor resulte una prioridad absoluta para ninguno de los valores en conflicto, en detrimento del otro, cuyo sacrificio sea total. Aplicando el principio de proporcionalidad, debe siempre optarse por la solución menos gravosa, que otorgue más efectividad a aquél valor jurídico que goce de mayor prioridad en el caso concreto.

Así, por ejemplo, podría determinarse la jerarquía superior de la libertad de información frente al derecho al olvido, cuando en un supuesto en concreto se crea necesario proteger con más intensidad el derecho de los sujetos a la libertad informativa, como base fundamental de la configuración de un Estado democrático en detrimento del derecho individual de un sujeto a que se supriman determinados datos personales de un portal web; y ello sería perfectamente ajustado a Derecho[846].

En segundo lugar, e íntimamente relacionado con el principio de proporcionalidad, conviene tener presente su efecto recíproco. Éste se produce entre los derechos fundamentales y las leyes que disciplinan su ejercicio, generándose así un régimen de concurrencia normativa que supone que, tanto las normas que regulan una determinada libertad fundamental como aquéllas que establecen límites a su ejercicio, actúan recíprocamente y, como resultado de dicha interacción, la fuerza expansiva propia de todo derecho fundamental restringe el alcance de las normas limitadoras que actúan sobre el mismo; de ahí deriva la exigencia de que cualquier límite a un derecho fundamental deba ser interpretado necesariamente mediante criterios descriptivos y en el sentido más beneficioso para su eficacia[847].

---

[845] Esta técnica de ponderación ha sido empleada tradicionalmente por la jurisprudencia constitucional para resolver conflictos entre derechos. Así, por ejemplo, para dirimir una disputa entre el derecho al honor del artículo 18 CE y a la libertad de expresión del artículo 20 CE, el Tribunal Constitucional ha exigido, en primer lugar, que se realice "*una necesaria y casuística ponderación entre uno y otro*" y, en segundo lugar, que se tenga en consideración "*la dimensión de garantía de una institución pública fundamental, la opinión pública libre, que no se da en el derecho al honor*", STC 104/1986, de 17 de julio, FJ 4º.

[846] Sobre la interacción entre los medios de comunicación y su libertad informativa y el derecho a la protección de datos personales, PAUNER CHULVI. "La actividad periodística en los ordenamientos nacionales y europeo sobre protección de datos" en *Hacia un nuevo Derecho europeo de Protección de Datos* (Rallo Lombarte/García Mahamut eds.), Tirant lo Blanch, València, 2015.

[847] BASTIDA FREIJEDO/VILLAVERDE MENÉNDEZ et al. *Teoría general de los derechos fundamentales en la Constitución española de 1978*, Tecnos, Madrid, 2001, p. 54.

Para MUÑOZ RODRÍGUEZ[848] el juicio de ponderación del derecho al olvido digital debe resolverse atendiendo a cuatro factores: la naturaleza de la información (veracidad, adecuación o actualidad de los datos); el carácter sensible de esta información para la vida privada del individuo; el interés público ínsito en dicha información (*ratione materiae*); y el interés público de la persona referida (*ratione personae*).

En la propia sentencia del *caso Google* el TJUE ya dejaba entrever los límites a los que debía de someterse el nuevo derecho al olvido (punto 81 y siguientes), empezando por las excepciones señaladas por la normativa de protección de datos (la Directiva 95/46/CE, vigente en dicho momento), así como el interés del titular y la naturaleza concreta de los datos, el carácter sensible para la vida privada de la persona afectada, el interés público en disponer de dicha información y el papel que el afectado desempeñe en la vida pública.

Finalmente, el GDPR, al regular el derecho al olvido, contempla expresamente aquéllas limitaciones que pudieron desprenderse de la jurisprudencia y que condicionan su contenido en toda su extensión. Dispone así su artículo 17:

> *3. "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 i), y apartado 3;*

[848] MUÑOZ RODRÍGUEZ. "La desindexación de contenidos del índice de resultados de buscadores de internet tras la sentencia del TJUE sobre derecho al olvido", *Abogacía Española*, 2014. Disponible online en: https://www.abogacia.es/2014/10/13/la-desindexacion-de-contenidos-del-indice-de-resultados-de-buscadores-de-internet-tras-la-sentencia-del-tjue-sobre-derecho-al-olvido/ El autor, fue uno de los abogados de Mario Costeja en el procedimiento ante el TJUE del *caso Google*, que dio lugar a la creación del derecho al olvido.

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

Se deriva de ello la concepción del derecho al olvido como una suerte de regla general pues la existencia de este catálogo de límites implica, tal y como ha declarado la Comisión Europea, la inversión de la carga de la prueba, siendo el responsable del tratamiento de datos quien, ante un requerimiento por parte del interesado, deba probar que los datos personales controvertidos no deban suprimirse por incurrir en alguno de los supuestos anteriores[849].

Sobre las excepciones previstas en el precepto anterior procede, a continuación, hacer algunos comentarios acerca de las mismas, dejando las consideraciones sobre la libertad de expresión e información para más adelante pues, dada su relevancia, se analizará la cuestión en un apartado específico.

En cuanto al "*cumplimiento de una obligación legal*", poco se puede añadir, excepto que ello coincide con lo dispuesto en el artículo 6 GDPR que dispone aquellas condiciones cuyo cumplimiento determinará la licitud de un tratamiento de datos personales y entre las que se encuentra *c)* "*el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento*" y *e)* "*el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*".

Lo mismo ocurre con la excepción relativa a las "*razones de interés público en el ámbito de la salud pública*" que se corresponden con lo dispuesto en los apartados *h)* e *i)* del artículo 9,

[849] COMISIÓN EUROPEA, *Factsheet on the Right to be Forgotten Ruling* (C-131/12), 2014. Disponible online en: https://www.inforights.im/media/1186/cl_eu_commission_factsheet_right_to_be-forgotten.pdf

y que regulan las singularidades que pueden llevarse a cabo en el tratamiento de categorías de datos especialmente sensibles por motivos de salud pública[850].

Respecto de la exclusión relativa a los "*fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos*", ésta está en plena consonancia con el artículo 89.1 GDPR que exige la previsión de medidas técnicas y organizativas para garantizar el principio de minimización de los datos personales, entre las que se puede incluir la seudonimización.

En relación al conflicto entre el derecho a la privacidad y el libre acceso a la información se pronunció el TJUE en el caso *Markkinapörssi-Satamedia*[851] en el que el Tribunal dispuso la existencia de excepciones o restricciones a la protección de datos y a la privacidad en aras de garantizar la actividad periodística, artística o literaria. Así, reiteró la exigencia de interpretar extensivamente conceptos como "periodismo" en una sociedad democrática, así como la necesidad de imponer "límites estrictamente necesarios" a las empresas de medios de comunicación así como a toda persona que ejerza una actividad periodística en aras de garantizar la privacidad personal.

Del mismo modo, recuerda el TJUE que la publicación de información personal con ánimo de lucro no es elemento determinante para discernir si se trata o no de una actividad periodística y, partiendo de dicha base, concluyó que la publicación de datos personales procedentes de documentos públicos, podía considerarse como una actividad periodística en tanto que su finalidad es "divulgar al público información, opiniones o ideas, por cualquier medio de transmisión".

---

[850] "*h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3; i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la*

asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional".

[851] STJUE (Gran Sala), de 16 de diciembre de 2008, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, Asunto C-73/07.

En relación a la actividad periodística, procede reiterar brevemente aquí lo dispuesto por la STC 58/2018 de 4 de junio, analizada en páginas anteriores y que, cambiando el criterio mantenido hasta entonces por la STS 545/2015, de 15 de octubre acerca de la inalterabilidad de las hemerotecas como límite al derecho al olvido[852], decreta la prohibición general de indexación de los nombres y apellidos de las personas para su uso por el motor de búsqueda interno de las hemerotecas digitales[853].

Considera así que el derecho al olvido no viene limitado por las hemerotecas digitales que, a partir de ahora, deberán eliminar de sus buscadores internos la opción de búsqueda de informaciones acerca de una persona introduciendo su nombre y apellidos, aunque no deberán suprimir sus datos personales, ni anonimizarlos de sus fuentes originales, sino sólo desindexar dicha información privada.

Por último, respecto de la excepción acerca de la "*formulación, el ejercicio o la defensa de reclamaciones*", poco más se puede añadir, excepto que ello se aplica ya sea por un procedimiento judicial, un procedimiento administrativo o uno de carácter extrajudicial, incluidos asimismo los procedimientos ante organismos reguladores.

9.1. La libertad de expresión e información como límite del derecho al olvido

Este límite al derecho de supresión viene recogido expresamente por el apartado *a)* del artículo 17.3 GDPR e indirectamente por el artículo 23.1 de dicho Reglamento que, con carácter general prevé la posibilidad de interponer limitaciones a los derechos y libertades que reconoce "*cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática*".

Efectivamente, existen derechos cuyo contenido constitucional representa una frontera insalvable para las libertades de expresión e información: el honor, la intimidad personal y

[852] Para un análisis más detallado de la cuestión, PAZOS CASTRO. "El derecho al olvido frente a los editores de hemerotecas digitales" en *InDret*, nº 4, 2016.

[853] "*se trata de 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*" (FJ 8º).

familiar, la propia imagen, el derecho a la protección de datos y el derecho al olvido. El considerando 153º del Reglamento especifica que, a tal efecto, los Estados miembro deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar dichos derechos fundamentales ante el riesgo potencial de colisión[854], en particular "*al tratamiento de datos personales en el ámbito audiovisual y en los archivos de noticias y hemerotecas*"[855].

La posibilidad de que el derecho al olvido actuase como una herramienta de censura a la libertad de contenidos imperante en Internet, ha llevado a parte de la doctrina a rechazar desde un principio, su eficacia *erga omnes* e incluso a cuestionar la pertinencia de dicha figura, por el miedo a que supusiera un punto y final para la libertad de expresión e información en Internet[856]. El temor a que el derecho al olvido condicione dichas libertades se ve acrecentado por su dimensión institucional, pues el valor protegido por la libertad de expresión e información es la existencia misma de una opinión pública lo cual es, a su vez, una condición necesaria para el correcto funcionamiento de la democracia[857]. Asimismo, la libertad de expresión e información protege otros bienes jurídicos relacionados, como la búsqueda de la verdad, que exige el flujo libre y el contraste de ideas, o la necesidad del ser humano de comunicarse con sus semejantes para desarrollar su personalidad, elementos necesarios para la consecución de una "sociedad abierta"[858].

---

[854] "*Por tanto, los Estados miembros deben adoptar medidas legislativas que establezcan las exenciones y excepciones necesarias para equilibrar estos derechos fundamentales. Los Estados miembros deben adoptar tales exenciones y excepciones con relación a los principios generales, los derechos del interesado, el responsable y el encargado del tratamiento, la transferencia de datos personales a terceros países u organizaciones internacionales, las autoridades de control independientes, la cooperación y la coherencia, y las situaciones específicas de tratamiento de datos* […] *a fin de tener presente la importancia del derecho a la libertad de expresión en toda sociedad democrática, es necesario que nociones relativas a dicha libertad, como el periodismo, se interpreten en sentido amplio*".

[855] Sin embargo, y pese a que el plazo para llevar a cabo la adopción y la comunicación de dichas medidas expiró el 25 de mayo de 2018, el legislador español no ha adoptado normativa alguna al respecto, ni si quiera se comprenden medidas en este sentido en el Proyecto de Ley Orgánica de protección de datos de carácter personal.

[856] Cfr. FAZLIOGLU. "Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet" en *International Data Privacy Law*, Vol. 3, nº 3, 2013.

[857] Así lo ha afirmado reiteradamente el Tribunal Constitucional (por todas, STC 6/1981, de 14 de abril).

[858] DÍEZ-PICAZO GIMÉNEZ. *Sistema de derechos Fundamentales*, ob. cit., p. 313.

Brevemente, procede señalar que se pueden identificar paralelismos entre las figuras del derecho al olvido y la libertad de expresión e información pues ambas tienen una conexión íntima con la dignidad de la persona, las dos pueden ser predicables de las personas jurídicas[859] e, igualmente, pueden desplegar efectos jurídicos en las relaciones jurídicas entre particulares[860]. Del mismo modo, su contenido encuentra límites en el ejercicio de otros derechos y libertades fundamentales con los que puede entrar en colisión, cuyos bienes jurídicos comparten múltiples similitudes pues, en la regulación del derecho a la libertad de expresión e información, dispone el artículo 20.4 CE: "*estas libertades tienen su límite en el respeto a los derechos reconocidos en este Título, en los preceptos de las leyes que lo desarrollen y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia*" [861].

Así pues, no cabe duda de que el derecho al olvido encuentra restricciones en el derecho a la libertad de expresión e información y viceversa[862], la pregunta es, cómo debe llevarse a cabo la resolución de un eventual conflicto entre ambos valores jurídicos. En relación a dicha cuestión, el artículo 85 GDPR aporta alguna aclaración adicional en cuanto a dicho ejercicio de ponderación, permitiendo a los Estados miembros establecer exenciones o excepciones a la regla general de protección de datos en algunos aspectos y relacionados con "*el derecho a la*

[859] No obstante, las personas jurídico-públicas quedan excluidas de la titularidad de ambos derechos, en concreto respecto de la libertad de expresión e información. Al respecto conviene señalar el deber de neutralidad ideológica atribuido a los poderes públicos (art. 16 CE) así como las limitaciones constitucionales predicables de los medios de comunicación de titularidad pública (art. 20.3 CE).

[860] En cuanto a la libertad de expresión e información, por todas, STC 125/2007, de 21 de mayo.

[861] Recordar que, pese a la inclusión expresa del derecho al olvido en el GDPR así como en el Proyecto de LOPD, en el ordenamiento jurídico español su reconocimiento se deriva, hasta ahora, de la jurisprudencia del Tribunal Constitucional por lo que no pueden encontrarse menciones al respecto en el texto constitucional pese a que, ello se derivaría de una interpretación del texto de acuerdo con las circunstancias actuales, pues las analogías son muy frecuentes.

[862] El artículo 10 del CEDH prevé, asimismo, los límites a los que pueden verse sometidas la libertad de expresión e información: "*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*".

libertad de expresión y de información, incluido el tratamiento con fines periodísticos y fines de expresión académica, artística o literaria"[863].

Frente a dicha cuestión, por el momento, no encontramos pronunciamientos jurisprudenciales suficientes para dilucidar dicha controversia, dado el carácter novel del derecho al olvido. Sin embargo, y dadas las afinidades que encontramos entre el derecho de supresión y el derecho al honor y a la intimidad personal, podrían aplicarse, aunque sólo parcialmente, las teorías doctrinales vigentes al respecto, para la resolución del conflicto entre la libertad de expresión e información y el derecho al olvido.

Las directrices fijadas por el Tribunal Constitucional para resolver casos de conflicto entredichos derechos fundamentales, se recogieron en su día por el Tribunal Supremo en un caso de conflicto entre el derecho al honor y a la intimidad privada y, por otra parte, el derecho a la libertad de expresión e información[864]: "*1º. Para establecer la delimitación de tales derechos es preciso examinar caso por caso, sin fijar apriorísticamente los límites entre ellos; 2º. Para hacer la valoración debe tenerse en cuenta la posición preferente, no jerárquica, que sobre los derechos de la personalidad contenidos en el artículo 18 de la Constitución ostenta el derecho a la libertad de información del artículo 20.1.d) en función de su doble carácter de libertad individual y de garantía institucional de una opinión pública, libre e indisolublemente unida al pluralismo político dentro de un Estado democrático, siempre que la información transmitida sea veraz y esté referida a asuntos de relevancia pública que sean de interés público, pues, solo entonces puede 'exigirse a aquéllos a quienes afecta o perturba el contenido de la información que, pese a ello, la soportan en aras precisamente del conocimiento general y difusión de los hechos y situaciones que interesen a la comunidad'; 3º. Lo único que puede justificar que deba un sujeto soportar las molestias ocasionadas por la*

[863] El artículo 85.2 agrega "*Para el tratamiento realizado con fines periodísticos o con fines de expresión académica, artística o literaria, los Estados miembros establecerán exenciones o excepciones de lo dispuesto en los capítulos II (principios), III (derechos del interesado), IV (responsable y encargado del tratamiento), V (transferencia de datos personales a terceros países u organizaciones internacionales), VI (autoridades de control independientes), VII (cooperación y coherencia) y IX (disposiciones relativas a situaciones específicas de tratamiento de datos), si son necesarias para conciliar el derecho a la protección de los datos personales con la libertad de expresión e información*".

[864] STS 3433/1996, de 5 de junio.

difusión de determinada noticia, es la información comprobada desde el punto de vista de la profesionalidad informativa".

Sin embargo, tal y como dispone la STC 58/2018, de 4 de junio, las circunstancias del nuevo contexto deben reorientar la jurisprudencia dictada hasta ahora sobre la ponderación de dichos derechos en conflicto, por ello "*deben ser añadidas al canon dos variables determinantes en supuestos como el que nos ocupa, porque estamos ante el apartado cuarto del artículo 18 CE con carácter prevalente: 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*" (FJ 7º)

En cualquier caso, la determinación de los lindes entre ambos derechos, debe pasar necesariamente por llevar acabo la realización de un juicio de proporcionalidad entre ambos valores, teniendo en cuenta siempre el caso concreto, pues no procede hacer aquí generalizaciones y automatismos, sino que las restricciones que, en su caso, puedan imponerse deben de ser adecuadas, necesarias y proporcionadas al supuesto de hecho. Como sustenta ALEXY, la operación de ponderación no es un procedimiento que, en cada caso, conduzca exactamente a un resultado, pues el peso de los bienes jurídicos en conflicto no es determinable en sí mismo o absolutamente, sino que sólo lo es de forma relativa, conforme a un supuesto de hecho concreto[865].

Así las cosas, refundamentando los argumentos expuestos en páginas anteriores, a continuación se procede a presentar los elementos condicionantes que deben tenerse en cuenta a la hora de llevar a cabo un juicio de ponderación cuando se produzca una colisión entre intereses jurídicos.

a) La naturaleza del sujeto

Así, en primer lugar, debe tenerse en consideración el interés público de la información –si es una medida necesaria y proporcionada en una sociedad democrática- sobre la base de la

[865] Cfr. *Teoría de los Derechos Fundamentales*, ob. cit., pp. 557-161.

naturaleza del sujeto en cuestión, esto es, si la persona en concreto tiene la consideración de sujeto público o no[866].

Como ya se ha visto, los personajes públicos, por la relevancia que tienen sus actos para la formación de la opinión pública, tienen la obligación de soportar una mayor publicidad de sus actos así como de las informaciones relativas a su persona[867], por lo que en dichos supuestos, la libertad de expresión e información goza de una "posición preferente"[868].

Sin embargo con la regulación prevista en el GDPR, incluso éstos, podrían ejercitar el derecho al olvido –aunque no con la misma amplitud- cuando, por el transcurso del tiempo, dichas informaciones ya no se ajusten a la situación real y no resulten relevantes para la sociedad en general, es decir, cuando no se trate de informaciones relacionados con la organización y el funcionamiento de los poderes públicos"[869], en el caso de cargos políticos, o cuando dicha información sea ajena a cualquier aspecto de su actividad por los que ostentan notoriedad[870], en el caso del resto de personas con relevancia pública. Otro caso distinto es el de las personas cuya notoriedad pública deriva de su exposición voluntaria, sobre las cuales la jurisprudencia constitucional no ha llevado a cabo un pronunciamiento unánime, aunque ha establecido algunos parámetros: cabe la libertad de expresión e información con los límites generales de la veracidad de las informaciones y la prohibición del insulto, mientras que no es

[866] En el ya examinado *caso Google*, el TJUE consideró de forma expresa el derecho a la información sobre los datos de personajes públicos como único límite al derecho al olvido: "*en supuesto específicos, el interés del público prevalecerá en virtud de la naturaleza de la información y del carácter sensible para la intimidad de la persona afectada –como ocurría atendiendo a la función que esta persona desempeñe en la vida pública*-" (FJ 81º). En todo caso, el interés público deberá de valorarse y ponderarse en cada supuesto, pese a que los datos personales que pretendan borrarse de los índices de búsqueda afecten a un personaje conocidamente público o a un claro interés público, así como el impacto en la privacidad de la persona afectada. Además, recuerda el TJUE, el tratamiento de datos con fines exclusivamente periodísticos, se beneficia de la exención prevista en el art. 9 de la ya derogada Directiva 95/46, limitando la aplicación de la normativa de protección de datos tanto si lo llevan a cabo medios de comunicación online como otros editores de páginas web, en cuyo caso no será posible ejercer el derecho al olvido ante la webmaster.

[867] "No todo el mundo es igual: ni todas las personas tienen derecho a exigir un nivel de precaución exquisito en la exactitud de los que se dice acerca de ellas, ni todas lo tienen al mismo grado de intimidad y reserva". SALVADOR CODERCH. *El mercado de las ideas*, Centro de estudios constitucionales, Madrid, 1990, p. 243.

[868] Cfr. STC 104/1996, de 11 de junio.

[869] Cfr. STC 110/2000, de 5 de mayo.

[870] Cfr. STC 297/2000, de 11 de diciembre.

lícita la información no deseada sobre familiares y allegados[871] ni cabe utilizar la indiscreción de los empleados como fuente de información[872].

No obstante, y teniendo en cuenta la cultura de la exposición pública que hoy en día se produce mediante las redes sociales, principalmente, cualquier persona puede adquirir "relevancia pública" y, en tanto que la publicidad de sus datos personales (imágenes por ejemplo) pueden conllevar un perjuicio para otros derechos fundamentales, no hay motivo alguno para no reconocer la posibilidad de ejercitar el derecho al olvido en este caso, tanto si dicha trascendencia pública se deriva de una elección personal como si es ajena a su voluntad.

b) La veracidad de la información

En segundo lugar, hay que examinar si la información es veraz o no. Al contrario que a la expresión, a la libertad de información se le impone constitucionalmente el requisito de la veracidad -artículo 20.1.d) CE- de manera que la emisión de informaciones falsas, rumores o bulos no constituye legítimo ejercicio del derecho fundamental a la libertad de información[873]. Sin embargo, el requisito de la veracidad de la información no tiene un carácter absoluto, pues si se exigiera comprobar exhaustivamente la autenticidad de todas las noticias el coste para la libertad de información sería prohibitivo, por lo que la jurisprudencia constitucional entiende el requisito de la veracidad como un deber de buena fe y diligencia por parte del informador[874], predicándose más del sujeto que del objeto[875].

Sin embargo, la veracidad en el caso del derecho al olvido no es un elemento a tener en cuenta para que pueda llevarse a cabo su ejercicio[876], de hecho se presume que los datos personales son verdaderos siempre, puesto que permiten identificar correctamente a una

[871] Entre otras, STC 134/1999, de 15 de julio.

[872] STC 115/2000, de 5 de mayo.

[873] Así, la esfera de lo constitucionalmente protegido es más amplia para las opiniones que para las noticias, no operando de igual modo la *exceptio veritatis*, Cfr. STC 107/1988, de 8 de junio.

[874] Cfr. STC 61/2004, de 18 de mayo.

[875] DÍEZ-PICAZO GIMÉNEZ. *Sistema de derechos Fundamentales*, ob. cit., pp. 315-318.

[876] BROTONS MOLINA. "Caso Google: Tratamiento de datos y derecho al olvido. Análisis de las conclusiones del abogado general, asunto C-131712" en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 33, p. 108.

persona y, en consecuencia, invaden la privacidad del individuo. De este modo, el hecho de que una determinada información sea veraz no impide que pueda ejecutarse el derecho al olvido cuando, de las circunstancias concretas del caso, se determine la conveniencia de la supresión de una determinada información personal[877], tal y como lo ha afirmado el Tribunal Supremo[878] y el Tribunal Constitucional[879].

Ello está directamente vinculado con el problema de las *Fake News* y su incidencia en la democracia y nos lleva a preguntarnos acerca de la pertinencia de que los indexadores de información en Internet adopten un rol regulador en este sentido de forma que, por ejemplo Google, decida el nivel de veracidad de una noticia y, en consecuencia, la incluya o no en su buscador. En caso afirmativo, se estaría dejando en manos de los buscadores –que, al fin y al cabo son empresas privadas que obedecen a intereses particulares- una responsabilidad desproporcionada que, en cualquier caso, corresponde determinar en última instancia a los poderes públicos, que estarían llevando a cabo una dejación de funciones[880].

---

[877] "La divulgación de información que contiene datos personales, a pesar de ser veraz, si no responde a un interés público, no está protegida por el art. 20.1 de la CE […] la difusión de una información del pasado que pueda afectar el derecho al olvido, aunque sea veraz, no estaría protegida por el contenido del art. 20.1 de la carta magna". SIMÓN CASTELLANO. *El régimen constitucional del derecho al olvido digital*, ob. cit., p. 129.

[878] "*Ciertamente eran hechos veraces. Pero la licitud del tratamiento de los datos personales no exige solamente su veracidad y exactitud, sino también su adecuación, pertinencia y carácter no excesivo en relación con el ámbito y las finalidades para las que se haya realizado el tratamiento (art. 6.1.d de la Directiva y 4.1 LOPD). Y esos requisitos no concurren en un tratamiento de estos datos personales en que una consulta en un motor de búsqueda de Internet que utilice sus nombres y apellidos permita el acceso indiscriminado a la información más de veinte años después de sucedidos los hechos, y cause un daño desproporcionado a los afectados*", STS 545/2015, de 15 de octubre, FJ 7º.

[879] "*También el paso del tiempo había causado que la noticia careciese de veracidad a la fecha de su divulgación en Internet, porque quien protagonizaba la noticia había superado hacía años su adicción y sus antecedentes penales habían sido cancelados*", STC 58/2018, de 4 de junio, FJ 7º.

[880] La Comisión Europea ha descartado, al menos por el momento, poner coto a las *Fake News* a través de una regulación comunitaria en este sentido, dejándolo en manos de las legislaciones domésticas así como de la autorregulación, bajo el argumento de la preservar la libertad de expresión y el pluralismo. En palabras de la comisaria responsable de Economía Digital, Mariya Gabriel, "no queremos crear un ministerio de la Verdad o de la Censura". Así, se prevén una serie de medidas para combatir la desinformación online, principalmente basadas en la elaboración de códigos de buenas prácticas por parte de las plataformas digitales pero no se les impone ninguna obligación legal que combata expresamente éste fenómeno. En España, las iniciativas para combatir las *Fake News* no han sido, en nuestra opinión, muy acertadas. Por una parte se rechazó en el Congreso la Proposición No de Ley impulsada por el Partido Popular que proponía la creación de una especie de sello de calidad para diferenciar las noticias verdaderas de las falsas y, de otra, se creó un grupo de trabajo sobre las *Fake News* cuya iniciativa y coordinación asumió el Ministerio de Defensa –decisión altamente cuestionable- sin acciones ni acuerdos relevantes en la materia.

En relación a ello, en el momento de redacción de este Capítulo, está pendiente de resolución por parte del Tribunal Supremo, un recurso de casación interpuesto por *Google* para intentar fijar una doctrina sobre el derecho al olvido que permita dilucidar si los buscadores de Internet tienen la obligación de valorar la exactitud y veracidad de los hechos que indexan y que, en su caso, se quieran borrar por los interesados.

Esta cuestión es indudablemente controvertida ya que hay varios intereses en juego, por una parte el derecho a la libertad de expresión y de información, a la pluralidad informativa, y el "principio de neutralidad de la red" así como los intereses económicos y empresariales de los motores de búsqueda que no quieren dedicar más personal ni recursos para modular su actividad en Internet y, de otra, el interés de los particulares a la privacidad y a la protección de datos personales, canalizadas en el derecho al olvido digital, así como el interés de los poderes públicos de preservar la veracidad del la información y un ambiente adecuado para el desarrollo democrático[881].

Existen muchos ejemplos polémicos acerca de la conveniencia de conceder o no un derecho al borrado digital[882]así como los parámetros para hacerlo, pues otro aspecto importante de la cuestión es aquél relativo a determinar qué es verdad, ¿aquello que sucedió o aquello que los tribunales han determinado?[883]. En todo caso, consideramos que dichos juicios de valor

[881] Debe tenerse en cuenta que la libertad de información no sólo es un derecho a "comunicar" sino que dicha libertad comprende una segunda faceta consistente en el derecho a "recibir" información, pues su finalidad última consiste en crear opinión pública.

[882] Como ahora el supuesto de un ciudadano español que consiguió la retirada de un archivo de noticias en la que figuraba en el registro de la policía como culpable de haber atropellado con su coche a una persona y haberla matado hacía 50 años, dado el periodo trascurrido pese a la veracidad de la información.

[883] Como ejemplo, el caso que ha dado lugar al recurso de casación anteriormente comentado, pendiente de resolución por parte del Tribunal Supremo. En noviembre de 2007, tres cazadores furtivos fueron sorprendidos en Ourense por agentes forestales, a quienes amenazaron y encañonaron con sus armas. Una patrulla del Seprona se personó en el lugar de los hechos y, al constatar lo ocurrido, presentó una denuncia contra los cazadores. Dos de los cazadores ilegales tenían empleos relacionados con la defensa del medio ambiente y el tercero trabajaba en la diputación provincial. A consecuencia de los hechos, la sociedad de caza expulsó a los cazadores por mal uso de la licencia. Sin embargo el Tribunal Superior de Galicia anuló las sanciones por una cuestión formal, de plazos de notificación y en los hechos probados de la resolución, se limitó a afirmar que los cazadores estaban autorizados para cazar en términos generales, haciendo mención a ciertos altercados sin especificar nada al respecto. Esta noticia se publicó en el diario El País antes de que tuviera lugar la sentencia del Tribunal Superior de Galicia. En consecuencia, los afectados solicitaron a Google que dejase de indexar la noticia y, al no conseguirlo, acudieron a la AEPD y a la Audiencia Nacional que consideraron que la información no era veraz por no coincidir con el contenido "exacto" de la sentencia posterior, y resolvieron que Google la retirase de sus buscadores. Google

deben llevarse a cabo por los poderes públicos y no procede privatizar dicha cuestión[884], dejando en manos de los motores de búsqueda la ponderación entre dichos valores[885].

En relación a dicha cuestión, sin duda es necesario aplicar el principio de transparencia al que se alude reiteradamente en el GDPR, de una forma directa y proactiva, capaz de informar a los usuarios sobre el nivel de fiabilidad de los contenidos, así como informándoles sobre el funcionamiento de los algoritmos empleados para seleccionar y sugerir noticias a los usuarios.

c) El carácter público o privado de la información

El tercer lugar debe tenerse en cuenta si la información sobre la que pretende ejercitarse el derecho al olvido es de carácter público, pues deben ponderarse los propósitos que se persiguen con la publicidad de la información administrativa –la seguridad jurídica (art. 9.3 CE) y el derecho de acceso a la información (art. 105.b) CE) y el alcance de la protección de datos personales y del derecho al olvido en cada caso. Esta cuestión se planteó en su día en el caso *Google*[886] y sobre ello nada dijo el TJUE, rechazándo pronunciarse sobre la posibilidad de que los boletines y diarios oficiales traten o conserven datos inadecuados, no pertinentes y excesivos en relación con los fines y el tiempo transcurrido.

---

recurrió en casación y ahora la Sala Tercera del TS debe decidir sobre si el derecho al olvido incluye también que se valore la exactitud de los hechos que se pretenden suprimir. Este supuesto reviste un gran interés pues se trataría aquí de una falta de veracidad sobrevenida y, además, debido a un pronunciamiento judicial que absuelve a los interesados por cuestiones procesales sin entrar en el fondo de los hechos, sobre los que constan varias denuncias y hasta incluso los motivos de las retiradas de las licencias de caza a los afectados. Así pues, ¿la resolución judicial debe considerarse "la verdad" por encima de los hechos ocurridos verdaderamente?, ¿cuál de las dos verdades tiene prioridad?

[884] En su misma página *Google* afirma "se trata de decisiones difíciles y, como organización privada, es posible que no nos encontremos en una posición adecuada para decidir sobre tu caso". https://policies.google.com/faq?hl=es

[885] Como ejemplo, *Google*, evalúa cada solicitud de eliminación de forma individual, empleando la técnica de la ponderación, poniendo principalmente en relación el derecho de la persona a controlar sus datos personales con el derecho del público a conocer y distribuir información. Así, dicho buscador no siempre retira las páginas sino que, evalúa cada caso para tomar una decisión, teniendo en cuenta diversos factores como si el interesado es una persona pública, el momento en que se produjeron los hechos que ahora se quieren suprimir, si la información procede de documentos oficiales, si hay interés público en dicha información, si hay una sentencia judicial al respecto, etc.

[886] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

Sin embargo parece lógico sostener que, aunque estén contenidos dentro de fuentes públicas, a veces, los datos personales no deberían ser publicados si de la ponderación del derecho a la protección de datos con el derecho de acceso a la información administrativa, se deriva que el segundo puede ser igualmente efectivo o compatible con una menor afectación del primero[887]. De hecho, el nuevo marco regulatorio europeo se preocupa por esta cuestión y, en el artículo 86 del GDPR, se insta a las legislaciones domésticas a conciliar el acceso público a los documentos oficiales con el derecho a la protección de datos personales[888].

Ello esta íntimamente relacionado con el principio de transparencia, como eje vertebrador de la sociedad democrática y su eventual conflicto con el derecho a la protección de datos personales, cuestión sobre la que sí se ha pronunciado el TJUE en alguna ocasión y en relación a la cual ha concluido que el principio de transparencia de la información administrativa no siempre prevalece por encima del derecho a la protección de datos[889].

Trasladada dicha doctrina al derecho al olvido digital, podría extraerse la posibilidad de su ejercicio sobre información pública, principalmente en relación a las versiones digitales de los boletines oficiales que, en numerosas ocasiones pueden comportar una publicidad desproporcionada de información personal, de carácter sensible. Este es el caso de las resoluciones judiciales y los expedientes de antecedentes penales, sobre las cuales el Tribunal Supremo ha manifestado el carácter lesivo que para la dignidad e indemnidad personal pueden comportar según qué casos[890].

---

[887] SIMÓN CASTELLANO. *El régimen constitucional del derecho al olvido digital*, ob. cit, p. 153.

[888] Artículo 86: "*Los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento*".

[889] Por todas, STJUE de 9 de noviembre de 2010, *Volkerund Markus Schecke Gbr y Hartmut Eifert v. Land Hessen*, asuntos acumulados C-92/09 y C-93/09.

[890] En relación a la publicación de los antecedentes penales, afirma el Alto Tribunal que dichos datos "*son de carácter superfluo e innecesario y que, desde luego, afectan a la probidad, reputación e, incluso, dignidad personal del interesado*", STS 6652/1999, de 25 de octubre, FJ 5º.

Si bien es cierto que, en el sector público, el interés legítimo que en su día originó una información se consuma con bastante rapidez, por lo que la perennidad de una información contenida en una fuente oficial puede motivar el ejercicio del derecho al olvido –pensemos por ejemplo en la publicidad de un embargo por impago, la concesión de una beca, subvención o ayuda social, o la imposición de una sanción administrativa como una multa de tráfico, cuando ésta ya ha sido satisfecha o ha transcurrido un largo periodo de tiempo- no puede ignorarse el principio de transparencia o seguridad jurídica que exige una sociedad democrática por lo que, de nuevo, se exige una ponderación de los bienes jurídicos en conflicto en el caso concreto, pese a que la jurisprudencia española y europea han admitido que la transparencia administrativa y el derecho de acceso a la información pública tienen su límite en la protección de datos personales[891].

Así pues, puede concluirse que, aquéllos hechos pasados que hoy en día tengan relevancia de interés público, ya sea en relación con el asunto de que se trate, debido a las fuentes de las que proviene dicha información o por sus protagonistas, ello se enmarca dentro de los límites de las libertades informativas y, no habría duda en razonar que el derecho al olvido decaería frente a éstos.

Cabe destacar que, en la ponderación entre la libertad de expresión e información con otros derechos fundamentales, la jurisprudencia tradicionalmente ha concedido una posición preferente a la primera, por lo que puede concluirse que el derecho a recibir información veraz por cualquier medio de difusión suele prevalecer frente a otros derechos constitucionales. Así lo ha expresado en más de una ocasión el Tribunal Constitucional[892], en caso de conflicto con

[891] SIMÓN CASTELLANO señala aquí que desindexar todo el contenido de los boletines oficiales es una limitación desproporcionada e innecesaria del derecho de acceso a la documentación pública, y defiende una desindexación individual mediante la previa solicitud del interesado. En este último caso, sostiene el autor que el empleo de *robots.txt* es un error ya que sólo evita el rastreo y no la indexación por parte de los motores de búsqueda, defendiendo como sistema más garantista la utilización de etiquetas meta o controlar el *referer* del navegador. Cfr. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, ob. cit., p. 310.

[892] "*Dada su función institucional, cuando se produzca una colisión de la libertad de información con el derecho a la intimidad y honor, aquélla goza, en general, de una posición preferente y las restricciones que dicho conflicto puedan derivarse a la libertad de información, deben interpretarse de tal modo que, el contenido fundamental del derecho a la información no resulta, dada su jerarquía institucional, desnaturalizado ni incorrectamente relativizado*", STC 171/1990, de 12 de noviembre, FJ 5º.

el derecho a la intimidad y el honor, por lo que procede esperar a la creación de un cierto acerbo constitucional para comprobar si se produce un cambio de tendencia frente a la protección de datos personales y el derecho al olvido o, si por el contrario, se mantiene el predominio de la libertad de expresión e información.

d) El transcurso del tiempo

En primer lugar, y pese a que no se alude a ello de forma expresa en el artículo 17 GDPR, el tiempo transcurrido desde la publicación de una determinada información, juega un papel esencial a la hora de determinar si ésta es "indebida", "necesaria" o "adecuada" a los efectos del GDPR así como para garantizar que los datos no se conserven más allá del tiempo necesario para los fines del tratamiento, como parte de los principios relativos del Reglamento -artículo 5.1. *e)*-.

Así se ha expresado de forma directa por las resoluciones de los órganos jurisdiccionales, como la STJUE del *caso Google* donde se consideró que el tiempo revestía una importancia fundamental en la cuestión, puesto que, con arreglo a la normativa de datos, el tratamiento debía cumplir con los principios de calidad no solo en el momento en que los datos eran recogidos sino durante todo el tiempo en que éste se desarrollaba, por lo que un tratamiento inicialmente adecuado a la finalidad que lo justaba, podría devenir inadecuado o excesivo con el transcurso del tiempo (punto 97), la STS 545/2015 de 15 de octubre ("*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*", FJ 6º) o la STC 58/2018 de 4 de junio en la que, en el caso en concreto, se concluía que "*el paso del tiempo había causado que la noticia careciese de veracidad a la fecha de su divulgación en Internet, porque quien protagonizaba la noticia había superado hacía años su adicción y sus antecedentes penales habían sido cancelados*" (FJ 7º). Precisamente este última resolución del TC dispone la necesidad de la jurisprudencia de adaptar sus postulados a las circunstancias actuales y, entre los nuevos parámetros a tener en cuenta menciona también la virtualidad del tiempo: "*deben ser añadidas al canon dos variables determinantes en supuestos como el que nos ocupa, porque estamos ante el apartado cuarto del artículo 18 CE con*

carácter prevalente: 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" (FJ 7º).

Por último, como se puede observar en las líneas anteriores, la importancia del tiempo transcurrido se deriva de forma indirecta del resto de criterios a tener en cuenta para la ponderación sobre los que tiene un peso muy específico, e igualmente, es un criterio general expuesto en a lo largo del GDPR, como se puede observar, por ejemplo, en sus considerandos 39º, 68º o 89º.

Sin embargo, el factor tiempo no es estable ni existen criterios unánimes respecto de cuántos días, meses o años son necesarios para que pueda justificarse la aplicación del derecho al olvido (encontramos criterios de lo más dispares en la jurisprudencia nacional anteriormente analizada que concede a los sujetos el derecho al olvido pasados 3, 20 o 50 años), pues por su propia naturaleza, necesita ponerse en relación con el conjunto de parámetros a tener en cuenta en el caso concreto, necesitando siempre de una ponderación al supuesto de hecho.

e) Otras consideraciones de cara al ejercicio de ponderación

Por último, procede hacer algunas consideraciones en relación con los límites aplicables al derecho al olvido, en primer lugar, en torno al hecho de que, mientras que tradicionalmente el ejercicio de la libertad de expresión e información se ha llevado a cabo por un profesional de la información, a través de un medio de comunicación, con la revolución de Internet, el contexto se ha modificado sustancialmente y el ejercicio de información ya no se lleva a cabo necesariamente en los términos anteriores[893]. Así pues, procede preguntarse si, la preponderancia y la superprotección que gozaba la libertad de información y expresión ante un

[893] Cualquier ciudadano puede hoy en día difundir información al resto del mundo teniendo acceso a un ordenador y a Internet, por lo que el monopolio informativo ya es cosa del pasado, de hecho se ha acuñado el término "periodismo ciudadano" para referirse a la participación de los usuarios como generadores de información. Sobre la actuación de los medios digitales y su incidencia en la privacidad de los ciudadanos, PAUNER CHULVI. "El impacto de las nuevas tecnologías en los derechos fundamentales: el reto de la privacidad en la prensa digital" en *Nuevas tecnologías y derechos humanos* (Pérez Luño ed.), Tirant lo Blanch, València, 2014.

eventual conflicto con otros derechos fundamentales es hoy en día igualmente predicable pese al nuevo escenario[894].

En segundo lugar, con independencia de que se produzca una colisión entre los derechos al honor, intimidad y propia imagen y el derecho a la información, cuando se incluyan expresiones vejatorias, insultantes o atentatorias al prestigio personal o profesional, el cauce para dirimir tales supuestos no se encuentra en la normativa relativa a la protección de datos personales sino en la Ley Orgánica 2/1982, de 5 de mayo, de Protección Civil del derecho al Honor, a la Intimidad Personal y familiar y a la Propia Imagen como supuestos de intromisión ilegítima. Así, mientras que esta legislación se aplica a los supuestos de divulgación de informaciones atentatorias a determinados derechos fundamentales como son el honor o la propia imagen, la normativa protectora de datos se aplica a aquellos supuestos en los que se hace necesario someter a determinados controles el empleo de datos personales para evitar usos no consentidos, excesivos o los tratamientos ilegítimos[895].

Así, sólo cabe concluir que, ante un eventual conflicto entre el derecho al olvido y la libertad de expresión e información, deberá de llevarse a cabo un juicio de proporcionalidad en el supuesto concreto de que se trate para determinar la prevalencia de uno u otro, teniendo en cuenta las diferentes circunstancias del caso en cuestión: la naturaleza pública o privada de la información, el contexto en que se lleva a cabo, el carácter público o privado del sujeto interesado, la concurrencia o no de vulneraciones de otros derechos fundamentales… Por el contrario, como ya se ha explicado anteriormente, la *exceptio veritatis* no juega un papel relevante en dicha determinación por lo que la veracidad de la información no es un parámetro a tener en cuenta en dicha operación hermenéutica, mientras que sí que lo será la adecuación, pertinencia y significación de los datos personales concretos así como el tiempo transcurrido desde que se vertió la información.

---

[894] Si bien es cierto que los profesionales de la información tienen un estatus reforzado para ejercitar la libertad de información y expresión, como demuestra su derecho a la cláusula de conciencia y el secreto profesional, el Tribunal Constitucional ha extendido la libertad de información y expresión "*tanto a los medios de comunicación, a los periodistas, así como a cualquier otra persona que facilite la noticia veraz de un hecho y a la colectividad en cuanto receptora de aquélla*", STC 225/2002, de 9 de diciembre, FJ 1º.

[895] BERROCAL LANZAROT. *Derecho de supresión de datos o derecho al olvido*, ob. cit., p. 249.

Así las cosas, frente a aquéllos que sostienen que el derecho de supresión colisiona frontalmente contra el derecho a la libertad de expresión e información, podría defenderse todo lo contrario, pues el derecho al olvido digital es la manifestación del equilibrio entre aquéllos y los derechos de la personalidad en Internet, como nuevo marco para la comunicación interpersonal.

9.2. El principio de buena fe y la prohibición del abuso del derecho como límite del derecho al olvido

Como regla general, hay que tener presente el principio de buena fe y la prohibición del abuso de derecho, comprendidos en el artículo 7 CC[896], que actúan como límites al ejercicio abusivo de los derechos fundamentales. Aunque dichos principios no estén consagrados en la Constitución, tienen un alcance general[897] al constituir innegablemente principios generales del ordenamiento jurídico, siendo además un concepto básico de la cultura jurídica europeo-continental[898].

Teniendo esto presente, no puede invocarse el derecho al olvido para configurar una suerte de memoria selectiva ni una reputación online "a la carta", el interesado debe demostrar como la situación actual que motiva el recurso al derecho al olvido, cumple necesariamente con los requisitos establecidos por la Ley -no siendo necesario probar la causación de daños y perjuicios ni tampoco la lesión de otros derechos fundamentales que puedan verse afectados-, y no es fruto de un mal uso de dicha figura.

---

[896] *Artículo 7 CC:*

1. "*Los derechos deberán ejercitarse conforme a las exigencias de la buena fe.*

2. *La ley no ampara el abuso del derecho o el ejercicio antisocial del mismo. Todo acto u omisión que por la intención de su autor, por su objeto o por las circunstancias en que se realice sobrepase manifiestamente los límites normales del ejercicio de un derecho, con daño para tercero, dará lugar a la correspondiente indemnización y a la adopción de las medidas judiciales o administrativas que impidan la persistencia en el abuso*".

[897] Así parece reconocerlo el Tribunal Constitucional que, en numerosas ocasiones, ha exigido buena fe en el ejercicio de derechos fundamentales, en contextos de relaciones jurídicas entre particulares (Entre otras: STC 241/1999, de 20 de diciembre; STC 115/2000, de 5 de mayo; STC 177/2007, de 23 de julio).

[898] DÍEZ-PICAZO GIMÉNEZ. *Sistema de derechos Fundamentales*, ob. cit., p. 148.

En relación a esta cuestión RALLO LOMBARTE señala que "el derecho al olvido nada tiene que ver con el fin de la memoria, con prescindir del pasado, con el falseamiento de la historia o con la supuesta instauración de un filtro censor universal al ejercicio del derecho a la información" dejando claro que cualquier otra interpretación *sensu contrario* sólo pretende confundir a quienes se aproximan a este debate de buena fe[899].

Para asegurar la adecuación de la figura del derecho al olvido, esto es que se lleve a cabo respecto de informaciones personales relativas a individuos que ni tienen ni pretenden gozar de interés público alguno, deben tenerse siempre en cuenta las condiciones personales, materiales y espacio-temporales del supuesto en concreto, así como la colisión con otros derechos fundamentales y los eventuales daños y perjuicios que podrían derivarse en caso de no producirse la supresión de datos personales demandada. No es lo mismo que, por ejemplo, se invoque el derecho al olvido por un trabajador autónomo que años atrás se vio envuelto en unos puntuales impagos a Hacienda hoy en día ya subsanados, y que observa como al introducir su nombre o el de su empresa de servicios los primeros resultados del buscador web hacen referencia a este suceso; que el caso de un actor que ha sido grabado en la calle, teniendo actitudes hostiles y reprochables contra otra persona.

9.3. Otros límites y restricciones al derecho al olvido

Existen otras limitaciones para la operatividad del derecho de supresión que, bien por su carácter residual bien por ser cuestiones accidentales, no se contemplan de manera conjunta bajo las cláusulas limitativas generales del GDPR aunque se encuentran expresamente recogidas en dicho instrumento y su operatividad como restricciones al contenido del derecho al olvido es ciertamente tangible.

En primer lugar, como ya se ha visto anteriormente, el interés público es un criterio a tener en cuenta a la hora de determinar la preponderancia del derecho al olvido o la libertad de expresión e información cuando exista una colisión entre ambos derechos. Procede mencionar,

[899] Cfr. "El debate europeo sobre el derecho al olvido en Internet" en *Hacia un nuevo Derecho europeo de Protección de Datos* (Rallo Lombarte/García Mahamut eds.), Tirant lo Blanch, València, 2015, p. 704.

nuevamente, el interés público de una determinada información junto con el interés legítimo del responsable del tratamiento de datos personales como límites al derecho al olvido, pues así se deriva del artículo 17.3 *d)* GDPR.

En relación a dicha cuestión, el Grupo de Trabajo del Artículo 29 analizó el concepto de "interés legítimo del responsable" contenido en la Directiva 95/46/CE derogada por el vigente GDPR aunque que, debido a la línea continuista argumental y reglamentaria entre ambos instrumentos, dichas observaciones pueden considerarse ciertamente vigentes. Así, a resultas de un examen exhaustivo se determinó que debía aplicarse "una prueba de sopesamiento" entre el interés legítimo del responsable del tratamiento y los intereses, derechos y libertades fundamentales del interesado[900], para determinar así el fundamento jurídico del tratamiento y si éste es o no adecuado. En dicho informe, se puso de relevancia la relación entre el interés legítimo -entendido como el beneficio que se obtiene del tratamiento- que debe ser en todo caso lícito, actual, necesario y proporcionado, y la finalidad del tratamiento -como la razón última por la que se tratan los datos-, así como con el principio de responsabilidad proactiva y de transparencia predicable respecto de los encargados del tratamiento.

En segundo lugar, e íntimamente relacionado con el caso anterior, el artículo 21 GDPR dispone que el interesado tiene derecho a oponerse al tratamiento de sus datos personales, en cualquier momento y por motivos relacionados con su situación particular, frente a lo cual "*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*". No obstante, si se opone al tratamiento, el interesado puede solicitar la supresión de sus datos en base al derecho al olvido, si no hay motivos legítimos para el tratamiento. Se evidencia de este modo, la interrelación entre los derechos de supresión y de oposición, y las limitaciones que de ello se derivan para el derecho al olvido.

[900] Dictamen del Grupo de Trabajo del Artículo 29 adoptado el 9 de abril de 2014 (WP 217).

En tercer lugar, hay que tener en cuenta que la tecnología disponible y el coste de su aplicación pueden operar como límites a la efectividad del derecho de al olvido, en tanto que puede dificultar o incluso impedir la supresión de los datos personales solicitada por el interesado, como así parece desprenderse del apartado segundo del artículo 17 GDPR: "*Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, 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*". Y ciertamente no es descabellado que en algún punto la propia tecnología actúe como límite al cumplimiento del derecho al olvido pues existen multiplicidad de instrumentos para hacer copiados íntegros de páginas web, y ello se lleva a cabo diariamente por distintos servidores que permiten acceder al contenido que una URL tenía en un momento determinado, por lo que llevar a cabo un borrado total de la información sobre la que se ha ejercitado el derecho al olvido, puede no ser ciertamente efectivo o posible.

Por último, el artículo 23 del GDPR permite a los Estados introducir, mediante medidas legislativas, limitaciones al alcance de las obligaciones y de los derechos establecidos en determinados artículos del Reglamento, entre los cuales se encuentra el derecho al olvido. Eso sí, siempre que tal limitación respete su contenido esencial y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar "*a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención; e) otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social; f) la protección de la independencia judicial y de los procedimientos judiciales; g) la prevención, la investigación, la*

detección y el enjuiciamiento de infracciones de normas deontológicas en las profesiones reguladas; h) una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en las letras a) a e) y g); i) la protección del interesado o de los derechos y libertades de otros; j) la ejecución de demandas civiles". En esta misma línea se manifiesta el Considerando 73 del Reglamento que, matiza, que dichas restricciones deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales[901].

10. Cuestiones procesales

La protección de los derechos de la personalidad puede dar lugar a distintas reacciones: constitucional, si los derechos lesionados merecen la consideración jurídico-constitucional de derechos fundamentales; penal, si la violación de la que se trata está tipificada como delito o como falta; civil, cuando la vulneración del derecho haya sido obra de particulares; o contencioso-administrativa, si la lesión procede de una Administración Pública[902].

10.1. Protección constitucional del derecho al olvido

Entre los mecanismos jurídicos para la protección de los derechos fundamentales, se encuentran las garantías legales que derivan de su propia naturaleza pues los preceptos comprendidos bajo el Capítulo 2º del Título I de la CE son directamente aplicables, exista o no

---

[901] "*El Derecho de la Unión o de los Estados miembros puede imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, al derecho de oposición, a las decisiones basadas en la elaboración de perfiles, así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública o de violaciones de normas deontológicas en las profesiones reguladas, y su prevención, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, la llevanza de registros públicos por razones de interés público general, el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios*".

[902] MARTÍNEZ DE AGUIRRE ALDAZ, C. "Los derechos de la personalidad", ob. cit., p. 265.

norma que desarrolle los mismos. Este efecto impide que la legislación negativa prive de eficacia a los derechos fundamentales.

El artículo 53.1 CE establece que dichos derechos y libertades "*vinculan a todos los poderes públicos*" y es que, dada la naturaleza que los derechos fundamentales poseen de auténticos derechos subjetivos, éstos resultan plenamente exigibles frente a los poderes públicos. Así lo ha reconocido el Tribunal Constitucional en varias ocasiones, llegando a señalar que "*los derechos y libertades fundamentales vinculan a todos los poderes públicos y son origen inmediato de derechos y obligaciones, y no meros principios programáticos*"[903]. Ello también se deriva del artículo 7.1 de la Ley Orgánica 6/1985, del Poder Judicial que dispone: "*los derechos fundamentales y las libertades públicas vinculan, en su integridad, a todos los jueces y tribunales, y están garantizados bajo la tutela efectiva de los mismos*".

Además de su directa aplicabilidad, la Constitución otorga a los derechos fundamentales cierto estatus de privilegio al exigir, en su artículo 53 CE que su regulación se lleve a cabo forzosamente por ley, siendo además necesario, que dicha ley tenga carácter orgánico cuando desarrolle derechos y libertades comprendidas bajo la Sección 1ª del Capitulo 2º del Título I de la CE.

Asimismo, los derechos fundamentales gozan de unas garantías jurisdiccionales específicas y privilegiadas, ante supuestos de vulneración. Así, en la jurisdicción ordinaria gozan de un "*procedimiento basado en los principios de preferencia y sumariedad"* y, de manera extraordinaria, pueden acceder al recurso de amparo constitucional ante el Tribunal Constitucional[904].

Así las cosas, dado el carácter de derecho fundamental del que goza el derecho al olvido -bien por entenderse comúnmente que queda integrado dentro del artículo 18.4 CE, bien porque

[903] STC 21/1981, de 15 de junio, FJ 17º.

[904] Artículo 53.2 CE: "*Cualquier ciudadano podrá recabar la tutela de las libertades y derechos reconocidos en el artículo 14 y la Sección primera del Capítulo segundo ante los Tribunales ordinarios por un procedimiento basado en los principios de preferencia y sumariedad y, en su caso, a través del recurso de amparo ante el Tribunal Constitucional*".

así lo ha afirmado la jurisprudencia constitucional[905]- ello conlleva su directa aplicabilidad, sin necesidad de mediación o intermediación legislativa alguna, ya que se deriva de su propio reconocimiento constitucional[906]. Además de dotarle de carácter fundamental, el TC ha dispuesto que el derecho al olvido goza de autonomía propia lo que significa que, para solicitar el ejercicio del derecho al olvido no hace falta probar la vulneración simultánea de otros derechos fundamentales, como pueda ser el honor o la intimidad, pues éste tiene sustancialidad propia.

La doble protección jurisdiccional antes mencionada, configura al derecho al olvido como un auténtico derecho subjetivo susceptible de ser protegido mediante el recurso ante los Tribunales. Esta tutela del derecho al olvido tiene carácter alternativo y compatible pues, en base al artículo 24 CE, su protección jurisdiccional puede instarse, bien por los cauces previstos en la legislación ordinaria, bien por el procedimiento especial de amparo.

10.2. La protección del derecho al olvido en el ámbito de la jurisdicción civil y contencioso-administrativo

La experiencia histórica ha demostrado que el mero reconocimiento constitucional de un derecho no es condición suficiente, aunque sí necesaria, para el efectivo respeto a los derechos fundamentales. Así, para lograr la efectividad de éstos, se debe acompañar su reconocimiento formal con garantías jurídicas suficientes.

El artículo 249 de la Ley de Enjuiciamiento Civil[907] dispone como mecanismo de defensa de los derechos fundamentales, el juicio ordinario[908]. Puesto que el derecho al olvido,

[905] STC 58/2018, de 4 de junio.

[906] El principio de vinculación general de las normas constitucionales sobre los derechos evidencia el carácter prevalente de los derechos fundamentales sobre el resto de derechos y libertades así como de la actividad de los poderes púbicos. Cfr. MEDINA GUERRERO. *La vinculación negativa del legislador a los derechos fundamentales*, McGraw-Hill, Madrid, 1996.

[907] Artículo 249 LEC: 1. *Se decidirán en el juicio ordinario, cualquiera que sea su cuantía:*

1.º Las demandas relativas a derechos honoríficos de la persona.

2.º Las que pretendan la tutela del derecho al honor, a la intimidad y a la propia imagen, y las que pidan la tutela judicial civil de cualquier otro derecho fundamental, salvo las que se refieran al derecho de rectificación. En estos procesos, será siempre parte el Ministerio Fiscal y su tramitación tendrá carácter preferente.

como ya se ha defendido, es también un derecho fundamental, éste sería el cauce para obtener tutela jurisdiccional frente a su vulneración, junto al recurso de amparo.

Sin embargo, para acudir a los tribunales para ejercitar el derecho de supresión, debe de agotarse previamente otras vías. El GDPR parece disponer un orden concreto a la hora de ejercitar el derecho al olvido así, en primer lugar, el derecho de supresión debe ejercitarse por cualquier interesado frente al responsable del tratamiento de los datos (al editor de una página web para que elimine los datos personales, o al gestor de una red social para que suprima la cuenta de un usuario, o bien a una webmaster o el motor de búsqueda para que retiren los enlaces en cuestión) quien deberá informar al interesado sobre el transcurso de las actuaciones, en el plazo máximo de un mes a partir de la recepción de la solicitud (prorrogable a 2 meses, según la complejidad y el número de solicitudes) –artículo 12.3 GDPR-.

A consecuencia de la *sentencia Google*[909], el derecho al olvido puede ejercitarse directamente frente al editor del contenido o, alternativamente, frente al motor de búsqueda, que es el que facilita la difusión masiva de los resultados así como su ordenación jerárquica. A tal efecto, los buscadores mayoritarios han habilitado sus propios formularios para que los usuarios puedan ejercitar su derecho al olvido de manera online[910] -la información, igualmente, se facilitará por medios electrónicos cuando sea posible a menos que el propio interesado solicite lo contrario-. De no ser así, el interesado puede ponerse en contacto con el encargado o el responsable del tratamiento, identificándose y exponiendo las particularidades de su caso,

---

[908] Hay que tener en cuenta la existencia de mecanismos procesales específicos previstos para proteger ciertos derechos fundamentales, entre los que se encuentra la protección civil del derecho al honor, la intimidad y la propia imagen, contemplada en la Ley Orgánica, de 5 de mayo, sobre protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

[909] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

[910] Por ejemplo, el formulario de *Google* a tal efecto está disponible online en https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=1-636692515888389079-4095107962&hl=es&rd=1&pli=1. Dicho formulario es muy breve y sencillo de rellenar, y permite llevarse a cabo no sólo por el propio interesado sino también por otra persona en su nombre. Entre la información que solicita para poder llevar a cabo la supresión, ésta se limita a: información de identificación personal (con una copia legible de un documento de identidad que lo acredite), identificación de la información personal que se quiera retirar así como su ubicación (URL), motivo de la eliminación, el nombre utilizado para llevar a cabo las búsquedas, así como una declaración jurada de la veracidad de todo lo anterior y el consentimiento para el tratamiento de datos a tal efecto.

adjuntando prueba de ello y solicitando, por escrito[911] y de manera motivada y detallada, los datos que desean suprimirse y el porqué[912].

Pasado dicho plazo sin obtener respuesta alguna a su petición o cuando, recibiendo contestación, el interesado considere que ésta no ha sido adecuada, podrá interponer una reclamación ante la Agencia Española de Protección de Datos[913] u otra autoridad de control. La AEPD determinará en cada caso y, en función de sus circunstancias, estimará o no tal reclamación (en el plazo de 3 meses) y, de hacerlo, valorará el supuesto en cuestión y llevará a cabo una decisión[914] que, a su vez, es susceptible de recurso ante los Tribunales[915]. A tal efecto,

---

[911] A tal efecto, la AEPD dispone en su página web, de una instancia modelo para rellenar por el interesado que desee ejercitar el derecho al olvido: https://www.aepd.es/media/formularios/formulario-derecho-de-supresion.pdf

[912] Procede recordar aquí que el responsable de todo tratamiento de datos personales debe de informar a los interesados de la existencia del derecho al olvido así como de los cauces para, en su caso, ejercitar dicho derecho. Así lo dispone el artículo 12.1 del GDPR: "*El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios*".

[913] "*Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales*", Artículo 12.4 del GDPR.

[914] Puesto que no se han establecido directrices generales, deben examinarse las circunstancias concretas de cada caso en cuestión para poder determinar si procede o no la concesión del derecho al olvido solicitada. A tal efecto, el Grupo de Trabajo del artículo 29 elaboró unas directrices a tener en cuenta en las solicitudes de supresión de datos, cuya traducción no oficial al español, por la AEPD está disponible en el siguiente enlace: https://www.aepd.es/media/criterios/criterios-gt29-wp225.pdf

[915] Artículo 65 Proyecto de LOPD. Admisión a trámite de las reclamaciones. 1. "*Con carácter previo a la iniciación de un procedimiento por reclamación, la Agencia Española de Protección de Datos deberá evaluar la admisibilidad a trámite de dicha reclamación, de conformidad con las previsiones de este precepto. 2. La Agencia Española de Protección de Datos inadmitirá las reclamaciones presentadas cuando no versen sobre cuestiones de protección de datos de carácter personal, carezcan manifiestamente de fundamento, sean abusivas o no se aporten elementos que permitan investigar la existencia de una vulneración de los derechos reconocidos. 3. Igualmente, la Agencia Española de Protección de Datos podrá inadmitir la reclamación cuando el responsable o encargado del tratamiento, previa advertencia formulada por la Agencia, hubiera adoptado las medidas correctivas encaminadas a poner fin al posible incumplimiento de la legislación de protección de datos y concurra alguna de las siguientes circunstancias: a) Que no se haya causado perjuicio al afectado en el caso de las infracciones previstas en el artículo 74 de esta ley orgánica. b) Que el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas. 4. Cuando las reclamaciones no se hayan formulado previamente ante el delegado de protección de datos designado por el encargado o responsable del tratamiento o ante el organismo de supervisión establecido para la aplicación de los códigos de conducta, la Agencia podrá remitírselas, antes de resolver sobre la admisión a trámite, a los efectos previstos en los artículos 37 y 38.2 de esta ley orgánica. 5. La decisión sobre la admisión o inadmisión a trámite, así como la que determine, en su caso, la remisión de la reclamación a la Autoridad de control principal que se estime competente, deberá notificarse al reclamante en el plazo de tres meses. Si, transcurrido este plazo, no se produjera dicha notificación, se entenderá que el procedimiento se ha iniciado en la fecha en que se cumpliesen tres meses desde que la reclamación tuvo entrada en la Agencia Española de Protección de Datos*".

dispone el Reglamento, "*las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual*[916]*, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos*" –artículo 79.2-. El plazo de tramitación de los procedimientos, según lo dispuesto en el Proyecto de LOPD, deberá regularse en el futuro por Real Decreto y, en ningún caso, podrá exceder los nueve meses[917].

Una de las novedades introducidas por el GDPR es el mecanismo de "ventanilla única" mediante el cual, los interesados podrán acudir a la autoridad nacional de su país a pesar de que el tratamiento, supuestamente vulnerador de derechos, se esté llevando a cabo en otro estado de la UE así como si el responsable no se encuentra domiciliado en dicho territorio nacional, cuando el tratamiento se esté llevando a cabo en suelo europeo[918], facilitando así que el

[916] Existe cuantiosa jurisprudencia del TJUE en base a la cual se reconoce el derecho de todo interesado a enjuiciar las lesiones de derechos en webs de Internet ante los tribunales del país en el que éste tenga su centro de intereses, es decir, el domicilio de su residencia habitual. Así, el Tribunal de Luxemburgo ha declarado que el criterio de competencia según la difusión (daño) resulta ciertamente inútil teniendo en cuenta el contexto de Internet, en el que los contenidos pueden consultarse por un número indefinido de usuarios en cualquier parte del Mundo. Por ello, a fin de garantizar una buena administración de la justicia, ha reiterado en numerosas sentencias, que la persona lesionada puede recurrir indistintamente: 1) Ante los órganos judiciales del Estado del lugar de establecimiento del emisor de dichos contenidos; 2) Ante los órganos judiciales del Estado donde esté su residencia habitual; o 3) ante los tribunales de cada Estado en cuyo territorio el contenido publicado en Internet hubiera sido accesible. Por todas, *caso eDate Advertising GmbH v. X*; Olivier *Martinez* and Others v. *Société MGN Limited* (Asuntos Acumulados C-509/09 y C-161/10), de 25 de octubre de 2011.

[917] Artículo 69. Plazo de tramitación de los procedimientos. 1. "*Los plazos máximos de tramitación de los procedimientos y notificación de las resoluciones que los terminen se establecerán mediante real decreto, que no podrá fijar un plazo superior a nueve meses. 2. Dichos plazos quedarán automáticamente suspendidos cuando deba recabarse información, consulta o pronunciamiento preceptivo de un órgano de la Unión Europea o de una autoridad de control conforme con lo establecido en el Reglamento (UE) 2016/679, por el tiempo que medie entre la solicitud y la notificación del pronunciamiento a la Agencia Española de Protección de Datos*".

[918] El considerando 23º del GDPR dispone a tal efecto que, "*Para determinar si dicho responsable o encargado ofrece bienes o servicios a interesados que residan en la Unión, debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión*".

interesado no tenga que dirigirse a distintas autoridades de control para la protección de sus derechos[919].

Así, cuando una autoridad nacional de control reciba una reclamación, deberá valorar si ésta tiene carácter transfronterizo para, en caso afirmativo, iniciar un procedimiento de cooperación con la Autoridad de control competente. Al efecto de salvaguardar la cooperación entre Autoridades de control, el GDPR crea el Comité Europeo de Protección de Datos –artículo 68 y siguientes GDPR-.

Del mismo modo, gracias al principio de extensión territorial del artículo 3 del Reglamento, cualquier interesado que resida en la Unión Europea puede solicitar que se supriman completamente sus datos personales cuando se dé de baja en un servicio o cuando tales datos dejen de ser necesarios para los fines para los que se recabaron respecto de cualquier responsable del tratamiento, estén o no establecidos en la UE, el cual estará obligado a cumplir las disposiciones del GDPR.

Procede mencionar que, tanto los trámites para ele ejercicio del derecho al olvido como toda información que se solicite y reciba el interesado para el ejercicio de sus derechos, tiene carácter gratuito. No obstante, para aquellos casos en que las solicitudes sean manifiestamente infundadas o excesivas, el responsable podrá cobrar un canon proporcional a los costes administrativos soportados o, incluso, negarse a actuar[920].

---

[919] Así lo explica el considerando 127º del GDPR: "*Cada autoridad de control que no actúa como autoridad principal debe ser competente para tratar asuntos locales en los que, si bien el responsable o el encargado del tratamiento está establecido en más de un Estado miembro, el objeto del tratamiento específico se refiere exclusivamente al tratamiento efectuado en un único Estado miembro y afecta exclusivamente a interesados de ese único Estado miembro, por ejemplo cuando el tratamiento tiene como objeto datos personales de empleados en el contexto específico de empleo de un Estado miembro. En tales casos, la autoridad de control debe informar sin dilación al respecto a la autoridad de control principal. Una vez informada, la autoridad de control principal debe decidir si tratará el asunto de acuerdo con la disposición aplicable a la cooperación entre la autoridad de control principal y otras autoridades de control interesadas («mecanismo de ventanilla única»), o si lo debe tratar localmente la autoridad de control que le haya informado*".

[920] Apartado quinto del artículo 12 GDPR: "*Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá: a) cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada, o b) negarse a actuar respecto de la solicitud. El responsable del tratamiento soportará la carga de demostrar el carácter manifiestamente infundado o excesivo de la solicitud*".

Conviene añadir que el GDPR prevé en su artículo 80, la posibilidad de que los individuos deleguen la representación de sus derechos y libertades, entre ellos ciertos aspectos del derecho al olvido, en entidades, organizaciones o asociaciones sin ánimo de lucro para que presenten, en su nombre, una reclamación ante una autoridad de control o, en su caso, un recurso ante los órganos jurisdiccionales.

Por último, y si bien hasta la fecha no hay ninguna norma ni reglamento de desarrollo que disponga como debe ejercitarse el derecho al olvido ante los tribunales, ello no obsta a la posibilidad de que un individuo afectado por la vulneración de éste y dándose los requisitos legales, interponga demanda en los juzgados para lograr la supresión de unos determinados datos personales que les estén afectando en sus derechos fundamentales. En efecto, pese a que la vía tuitiva preferente haya sido generalmente la administrativa, ello no implica la posibilidad de que los interesados ejerciten sus acciones en relación al derecho al olvido, directamente ante la jurisdicción ordinaria, pues dicha posibilidad, pese a que hasta ahora ha sido eminentemente excepcional en número, es perfectamente admisible, tal y como se deriva de los preceptos de la LEC y, en última instancia, de la Constitución española, anteriormente esgrimidos.

De hecho, este fue el procedimiento ejercitado por los interesados y que dio lugar al primer pronunciamiento sobre el derecho al olvido por parte del Tribunal Supremo, en su STS 545/2015, de 15 de octubre. Como se ha comentado en apartados anteriores, agotada la vía administrativa frente a la AEPD y, en lugar de interponer recurso ante la Audiencia Nacional, los demandantes de tutela interpusieron demandas ante la jurisdicción ordinaria, ajenas a la casuística dimanada hasta el momento, para solicitar la tutela de su derecho al olvido.

Ello, sin duda, puede explicarse en términos de economía procesal pues el procedimiento administrativo resultaba excluyente de cualquier otro *petitum*, como una indemnización por daños y perjuicios, lo que obligaría a los interesados a accionar la vía civil

para satisfacer el resto de pretensiones. Así, ejercitando directamente la vía civil, los interesados evitaron la duplicidad procesal y, con ello, todos los inconvenientes aparejados[921].

Así las cosas, tal y como se acaba de exponer, tanto el reconocimiento de carácter fundamental del derecho al olvido como la eficacia directa del GDPR, así como las consecuencias jurídicas que se derivaron del fallo del TJUE en el *caso Google*, hacen del derecho al olvido un derecho directamente ejercitable y garantizado por diversos mecanismos jurídicos.

Como reflexión final señalar que, para evitar un reconocimiento meramente retórico y lograr así una efectividad práctica del derecho al olvido éste debería quedar contemplado en una ley de desarrollo, en concreto una ley orgánica, dado su carácter fundamental. Hasta la fecha no se ha dictado disposición reglamentaria alguna[922] pese a que en el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, en tramitación parlamentaria en el momento de redactar estas líneas, hace un reconocimiento expreso y breve del derecho al olvido –remitiendo el contenido del derecho a lo dispuesto en el GDPR[923]-. Entre otras muchas cuestiones necesarias de un urgente desarrollo, sin duda ocupa un carácter preeminente la necesidad de acabar con la disparidad de procedimientos para el ejercicio del derecho al olvido, siendo necesaria una regulación unitaria al respecto.

a) La potestad del interesado de ejercitar o no el derecho al olvido

En cuanto al ejercicio del derecho al olvido, procede recordar como, una de las características de los derechos de la personalidad es que éstos no se extinguen por falta de

[921] Cfr. DI PIZZO CHIACCHIO. *La expansion del derecho al olvido digital. Efectos de "Google Spain" y el Big Data e implicaciones del nuevo Reglamento Europeo de Protección de Datos*, ob. cit., pp. 181 ss.

[922] Este comportamiento del legislador español resulta ciertamente reprochable pues, desde la entrada en vigor del GDPR en 2016, ha tenido dos años para poder llevar a cabo la modificación de su legislación doméstica para adecuarla al contenido del nuevo marco regulatorio, es decir, hasta que el GDPR fuera finalmente aplicable, cuyo plazo expiró el pasado 25 de mayo de 2018.

[923] Artículo 15. Derecho de supresión. 1. "*El derecho de supresión se ejercerá de acuerdo con lo establecido en el artículo 17 del Reglamento (UE) 2016/679. 2. Cuando la supresión derive del ejercicio del derecho de oposición con arreglo al artículo 21.2 del Reglamento (UE) 2016/679, el responsable podrá conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa*".

ejercicio, por lo que, la inactividad del titular frente a las eventuales agresiones que se produzcan contra éstos, no afectan al derecho en sí mismo.

Así las cosas, cualquier acción u omisión que de lugar al ejercicio del derecho al olvido puede motivar la interposición de una acción por parte del titular del derecho, si así lo decide éste pero, de no hacerlo, ello no implicaría ningún modo la extinción de dicho derecho. No obstante, sí que puede ocurrir que al no ejercitar el titular ninguna acción, ésta prescriba[924], pero ello no quiere decir que se haya extinguido el derecho al olvido, pues ante una nueva agresión, su titular podría reaccionar nuevamente para defender dicho derecho, cuyo ejercicio queda intacto.

La modalidad de tutela del derecho al olvido prevista, exige una participación activa del sujeto para la defensa de sus propios intereses, por lo que puede aludirse a un *status activus processualis* para la realización de los derechos fundamentales. DENNINGER concibe dicho estatus como el reconocimiento de la facultad de cada persona para participar activamente y asumir su propia responsabilidad en los procedimientos que le afectan, así como en el seno de las estructuras organizativas más directamente vinculadas con el ejercicio de los derechos fundamentales[925].

Sin embargo, dejar en manos de los individuos la iniciativa del ejercicio de un derecho fundamental exige necesariamente un contexto y procedimiento mediante los cuales pueda garantizarse un equilibrio de posiciones entre los miembros de la sociedad democrática, no sólo en las relaciones de los particulares con los poderes públicos, sino también entre los propios individuales[926].

---

[924] Esto queda evidenciado, por ejemplo, en el artículo 9.5 LOPDH que dispone que las acciones protectoras de los derechos al honor, la intimidad y la propia imagen caducarán en el transcurso de cuatro años desde que el legitimado pudo ejercitarlas.

[925] Cfr. "El derecho a la autodeterminación informativa" en *Problemas actuales de la documentación y la informática jurídica*, (Pérez Luño ed.), Tecnos, Madrid, 1987.

[926] Desde el punto de vista procedimental, PÉREZ LUÑO se atreve a enumerar las condiciones mínimas necesarias para lograr una adecuada realización de los derechos fundamentales, lo que exige unas estructuras organizativas básicas que aseguren: "*a) el pluralismo político; b) el respeto de las minorías; c) la neutralidad o imparcialidad; d) la apertura de los procedimientos a las necesarias innovaciones*". Cfr. "Las generaciones de derechos humanos", en *Historia de los Derechos Fundamentales* ob. cit., p. 381.

Como se verá más adelante[927] sólo en el caso de que la petición del interesado, estando bien fundamentada y no incurriendo en ninguno de los supuestos excepcionales ni entrando en conflicto con otros derechos fundamentales, sea desatendida por el responsable del tratamiento de dichos datos personales, se producirá una violación de su derecho al olvido y, en consecuencia, podrá optarse a una indemnización por los daños y perjuicios sufridos, en base a la teoría de la responsabilidad civil.

Surge aquí nuevamente la cuestión de si las personas jurídicas pueden ser titulares del derecho al olvido y, en consecuencia, ejercitar las acciones correspondientes, a lo que ya se ha respondido afirmativamente en páginas anteriores. Si bien el Reglamento europeo no contempla expresamente esta posibilidad[928] al limitarse a regular la situación de las personas físicas, lo cierto es que tampoco lo prohíbe expresamente. Y, en concreto, en nuestro ordenamiento jurídico esta posibilidad se ha reconocido en algunos otros derechos de la personalidad, como el derecho al honor, por lo que, siguiendo la lógica jurisprudencial desarrollada y como ya se ha argumentado previamente, nada obstaría al reconocimiento del derecho al olvido respecto de las personas jurídicas privadas, excluyendo en todo caso, la posibilidad de aplicar dicho régimen a las personas jurídicas públicas, como igualmente se ha expuesto anteriormente[929].

Otra cuestión a plantearse es si puede ejercerse el derecho al olvido por una pluralidad de personas o por un colectivo, pues si bien es cierto que existen bienes generales o intereses difusos que por su propia naturaleza no pueden tutelarse bajo la óptica tradicional de la lesión individualizada, las características propias del derecho al olvido no parecen prestarse a ello, lo que se pretende aquí es dotar al individuo de un control sobre sus datos personales, tutelando en

[927] Vid. *infra* Cap. III.11.

[928] El considerando 14º del GDPR dispone: "*El presente Reglamento no regula el tratamiento de datos personales relativos a personas jurídicas y en particular a empresas constituidas como personas jurídicas, incluido el nombre y la forma de la persona jurídica y sus datos de contacto*".

[929] Sobre la posibilidad de que las personas jurídicas sean titulares de derechos fundamentales, STC 23/1989, de 2 de febrero. En cuanto al reconocimiento del derecho al honor de las personas jurídicas, STC 139/1995, de 26 de septiembre y Ley Orgánica 2/1984, de 12 de marzo, reguladora del derecho de rectificación cuyo artículo 1 así lo recoge expresamente.

conjunto su intimidad, honor, reputación y propia imagen, en base a la dignidad individual y el desarrollo de su personalidad.

Así pues, la posibilidad procesal de defender el derecho al olvido mediante *acción popular* no parece resultar idónea en este caso pues resulta difícil imaginar un supuesto en el que los intereses en juego superen al individuo e incidan en los ciudadanos en su conjunto, pues precisamente el derecho al olvido tutela una serie de bienes jurídicos personalísimos que difícilmente pueden afectar a una colectividad (no confundir aquí con una persona jurídica, cuya tutela del derecho al olvido ya se ha defendido anteriormente así como su capacidad para ostentar legitimación procesal pasiva) pues resultan privativos de una persona.

Sin embargo, el hecho de que el derecho al olvido no sea susceptible de la *acción popular* obedece a su peculiar naturaleza y no representa al conjunto de derechos de tercera –o cuarta, según le posición que se suscriba- generación entre los cuales se inserta pues, al ser la solidaridad el valor que los fundamenta, es común que su eficacia permita contemplar su titularidad de forma global, recayendo, real o potencialmente, en el conjunto de los seres humanos. Así, el derecho al medio ambiente sano, a la paz, al desarrollo sostenible sí que son predicables del conjunto de la ciudadanía dada la universalidad de sus aspiraciones pero ello no resulta predicable del derecho al olvido, pues resulta fácil diferenciar entre las características diferenciadoras de dichos derechos.

Íntimamente relacionado con ello, aunque se trata de una cuestión sensiblemente distinta, es el hecho de que el GDPR permita, en su artículo 80, la posibilidad de que los individuos deleguen la representación de ciertos aspectos de su derecho al olvido en entidades, organizaciones o asociaciones sin ánimo de lucro para que presenten, en su nombre, una reclamación ante una autoridad de control o, en su caso, un recurso ante los órganos jurisdiccionales.

b) La eficacia del derecho al olvido en las relaciones entre particulares

Examinando las características procesales del derecho al olvido, vuelve a suscitarse la cuestión acerca de los procedimientos idóneos para hacer valer los derechos fundamentales en

las relaciones jurídico-privadas. Si bien, en apartados anteriores ya se ha expuesto ampliamente el debate de fondo sobre la eficacia de los derechos fundamentales entre particulares, respondiendo afirmativamente a esta cuestión, procede a continuación desarrollar más detalladamente dicha argumentación.

En primer lugar, el artículo 53.2 CE antes mencionado, no parece imponer limitaciones a la eficacia jurídica de los derechos fundamentales entre los particulares, al no distinguir entre violaciones procedentes de poderes públicos o de personas individuales, sino que procede a dar cobertura a todas las pretensiones, cualquiera que sea su fundamento sustantivo, siempre que se basen en conculcación de derechos fundamentales.

Así pues, la legitimación procesal para el amparo judicial frente a una eventual vulneración del derecho al olvido se extiende tanto frente a las personas físicas como a las jurídicas, en la medida en que éstas sean titulares de derechos fundamentales, tal y como lo ha venido reconociendo la jurisprudencia.

En segundo lugar, y del mismo modo, cuando el artículo 7.1 de la LOPJ[930] dispone que "*los derechos y libertades reconocidos en el Capítulo 1º del Título I de la CE vinculan, en su integridad, a todos los jueces y tribunales y están garantizados bajo la tutela efectiva de los mismos*", por lo que no limita la protección de los derechos fundamentales a los actos de los poderes públicos, sino que la tutela que propugna tiene alcance general.

A mayor abundamiento, en su apartado segundo, dicho precepto dispone que "*en especial, los derechos enunciados en el artículo 53.2 de la Constitución se reconocerán, en todo caso, de conformidad con su contenido constitucionalmente declarado, sin que las resoluciones judiciales puedan restringir, menoscabar o inaplicar dicho contenido*". Así, si las resoluciones judiciales no pueden restringir, menoscabar o inaplicar este contenido, es que el mismo es efectivo cualquiera que sea su carácter, público o privado, del destinatario del mandato. Éste parece ser el criterio del Tribunal Constitucional que, en no pocas ocasiones, ha otorgado su amparo frente a violaciones de derechos fundamentales procedentes de

[930] Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial.

particulares[931], utilizando la vía indirecta al concederlo no directamente frente al acto en particular, sino frente a la resolución judicial que pone fin a la tutela solicitada ante la jurisdicción ordinaria[932].

Teniendo en cuenta toda la argumentación anterior, parece procedente concluir de nuevo que, el derecho al olvido tiene eficacia tanto en las relaciones jurídico públicos como en las relaciones entre particulares, permitiendo iguales cauces procesales para hacer efectivo dicho contenido pues, lo contrario, supondría negar la eficacia dogmática de la Constitución.

10.3. Protección penal de la esfera de privacidad del sujeto

Puesto que el reconocimiento del derecho al olvido es muy reciente, éste aún no se refleja en la legislación penal, sin embargo, por lo que respecta a la protección ofrecida desde el ámbito penal a los datos personales que forman parte de la esfera de privacidad del sujeto, debe partirse de una serie de cautelas, consustanciales al estudio del poder punitivo del Estado. En tanto que el Derecho penal representa el monopolio del *ius puniendi* por parte de las instituciones de control social formal, será necesario que la limitación de libertad que supone el recurso a la sanción penal se encuentre plenamente justificada. Para encontrar dicha justificación, debe partirse en primer lugar de la función de tutela de bienes jurídicos conferida a las normas penales. El concepto de bien jurídico se encuentra asociado a valores e intereses que son jurídicamente declarados como tales, bien de manera explícita, bien implícitamente a través de la correspondiente tutela penal. La intervención del poder punitivo se realiza precisamente para evitar comportamientos. En este sentido, el Derecho penal trata de impedir la realización de actos que vengan a negar los valores tenidos como tales por el Derecho que, a su

[931] STC 170/1987, de 30 de octubre, entre otras. De esta manera, el TC consigue, mediante la vía indirecta, salvar el escollo impuesto por la literalidad del artículo 41.2 de la Ley Orgánica 2/1979, de 3 de octubre, del Tribunal Constitucional, en base al cual el recurso de amparo protege frente a violaciones de derechos fundamentales "*originadas por disposiciones, actos jurídicos o simple vía de hecho de los poderes públicos del Estado, las Comunidades Autónomas y demás entes públicos de carácter territorial, corporativo o institucional, así como de sus funcionarios o agentes*", sin contemplar expresamente la posibilidad de recurrir en amparo frente a vulneraciones de derechos fundamentales imputables a personas privadas.

[932] Cfr. PÉREZ TREMPS. *Derecho constitucional. El ordenamiento constitucional. Derechos y deberes de los ciudadanos*, ob. cit., pp. 431 y 432.

vez, si es expresión de la voluntad general serán los más apreciados por la sociedad[933]. La forma de determinar estos valores parte de la relevancia constitucional de determinados derechos y libertades proclamados en la Constitucional. En este sentido, el Derecho penal desarrolla mediante su tutela estos valores, ofreciendo un marco de protección en los supuestos donde pueda apreciarse su transgresión. De acuerdo con esta primera consideración, la protección de la esfera de privacidad del sujeto desde el ámbito del Derecho penal partiría de la propia declaración constitucional contenida en el art. 18 de la Constitución española, en tanto que precepto donde se recogen los derechos fundamentales que protegen la privacidad de los ciudadanos.

En segundo lugar, se ha expuesto en los puntos anteriores la protección ofrecida a la esfera de privacidad del sujeto desde distintos ámbitos del ordenamiento jurídico, cerrando dicha enumeración con el presente punto sobre la protección penal de la privacidad. Esta estructura no es casual, dado que responde a la posición de *ultima ratio* conferida al Derecho penal. Sólo en los supuestos donde los sistemas de control jurídico y social previos hayan fracasado, será posible y estará justificado el recurso al Derecho penal. Esto es así, en tanto que el poder punitivo del Estado, como atribución de la violencia legitima que representa el *ius puniendi* estatal, supone el ámbito del ordenamiento jurídico de mayor aflictividad respecto de la libertad del sujeto. En este sentido, la sanción penal, siendo muestra paradigmática la pena privativa de libertad, sólo podría justificarse en los supuestos donde el resto de controles establecidos en el ordenamiento jurídico no sean suficientes para restituir el valor o interés constitucional dañado con el comportamiento. Esto se ha denominado como "carácter subsidiario" del Derecho penal, siendo una manifestación del principio de proporcionalidad. También como directriz derivada del principio de proporcionalidad, debe hacerse mención al "carácter fragmentario" del Derecho penal. La importancia del "carácter fragmentario" del Derecho penal, supone reconocer que no pueden castigarse las agresiones a cualquier valor o

[933] Cfr. CARBONELL MATEU, J.C. *Derecho penal: concepto y principios constitucionales*, Tirant lo Blanch, Valencia, 1999.

interés, sino que será necesario reservar la intervención punitiva a las conductas más gravosas contra los bienes de mayor valor.

Así las cosas, esta segunda cautela respecto de la protección penal de la esfera de privacidad del sujeto viene a establecer que sólo cuando hayan fracasado las vías de protección previas reconocidas en el ordenamiento jurídico, y siempre que la agresión sea de una gravedad que justifique el recurso al Derecho penal podrá pasarse a la protección dispensada por dicho sector del ordenamiento jurídico. Por lo tanto, la relevancia constitucional del bien jurídico protegido, así como la importancia de las notas derivadas del principio de proporcionalidad son cuestiones a tener en cuenta para determinar si cabe aplicar el Derecho penal para proteger la privacidad de la ciudadanía o si, en cambio, es más adecuado recurrir a otros controles jurídicos menos aflictivos desde el punto de vista de la libertad del sujeto.

Realizadas estas notas preliminares, se hará mención en este apartado a los distintos tipos penales recogidos en el Código penal español (CP) que tienen una relación directa con la protección penal de la esfera de privacidad del sujeto, o que pueden suscitar cuestiones relacionadas con la invocación del derecho al olvido. Estos serán los delitos contenidos en los arts. 197 ss., relativos al descubrimiento y revelación de secretos[934]:

> ***1.*** *El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.*
>
> ***2.*** *Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o*

[934] Por razones prácticas, sólo se cita en el texto el tipo genérico del delito recogido en el art. 197 CP, pudiendo consultarse los siguientes preceptos del Código penal en caso de interés para el estudio integral de estas conductas: 197 bis, 197 ter, 197 quater, 197 quinquies, 198, 199, 200 y 201.

telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

***3.** Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.*

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

Como puede apreciarse en este precepto, se establece un marco para la protección jurídico-penal de la intimidad, partiendo de la lesión al bien jurídico que representa el daño producido por un tercero a la intimidad o la privacidad del sujeto[935]. La modalidad genérica recogida en el art. 197.1 CP establece como requisitos del tipo objetivo el apoderamiento del medio donde puedan encontrarse los datos personales del sujeto pasivo, siendo necesario que este apoderamiento suponga un descubrimiento de secretos que vulnere la intimidad, descartando por tanto aquéllos datos personales que puedan estar expuestos al público. Como señala JAREÑO LEAL, "en el ámbito penal la lesión del bien jurídico protegido tendrá lugar cuando la captación o reproducción haya sido subrepticia y se dé en un contexto de intimidad. En este caso, la lesión existirá aunque haya actuaciones precedentes del sujeto pasivo haciendo públicos determinados aspectos de su intimidad mediante imágenes, puesto que se trata de un bien disponible"[936]. De acuerdo con lo expuesto, incluso en supuestos donde pueda existir una previa cesión de la privacidad por parte del sujeto, equiparable en términos cualitativos al apoderamiento que supone el delito, existirá el tipo porque lo que debe valorarse es la obtención sin consentimiento de los datos en que consista el delito. De este modo, la ausencia de consentimiento determina el tipo subjetivo de la conducta, en tanto que requiere un actuar

[935] Para un estudio amplio de la cuestión, véase: BOIX REIG, J./ JAREÑO LEAL, A. *La protección jurídica de la intimidad*, Iustel, Madrid, 2010.

[936] Cfr. "El derecho a la imagen como bien penal", *La protección jurídica de la intimidad*, ob. cit., p. 113.

doloso para que efectivamente se entienda cometido el delito, sin que sea posible la modalidad imprudente del delito.

Pasando al apartado segundo del art. 197 CP, reconoce como delictiva la conducta de quien se "*apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado*". Siguiendo con lo dispuesto en el número anterior, los requisitos del tipo objetivo exigen el apoderamiento, utilización o modificación de los datos de un tercero, siendo además necesaria la ausencia de consentimiento para que pueda apreciarse el actuar doloso desde la perspectiva del tipo subjetivo. Respecto de este apartado, resulta importante considerar la adecuación que podría suponer el desarrollo del derecho al olvido, en los supuestos de registros públicos o privados que acumulan datos masivos de los ciudadanos en soportes electrónicos o informáticos, en casos donde dicha información pueda no ser necesaria para la función realizada desde el punto de vista de la institución pública, o los sangrantes casos donde, pese a que una persona manifieste tácitamente su exclusión de un registro privado –piénsese, por ejemplo, en darse de baja de una compañía telefónica-, los datos se mantienen en dicho registro, facilitando de alguna manera la oportunidad criminal en el ciberespacio. En este sentido, la agravación contenida en el art. 197.3 CP, relativa a la pena imponible a los que difundan a terceros los datos o hechos descubiertos mediante la comisión del delito, muestra la importancia conferida a los supuesto, donde, además de reconocer la vulneración de la esfera de privacidad del sujeto por parte del autor de los hechos, se produce el descubrimiento efectivo de los datos por su revelación a terceros.

Una vez realizada la mención al delito de descubrimiento y revelación de secretos, puede hacerse una mínima referencia a otra de las categorías delictivas contenidas en el Código penal que tienen una relación con la protección de la esfera de privacidad del sujeto, además de con una posible aplicación del derecho al olvido. Esta sería la categoría de los delitos contra el honor, concretamente en lo relativo a los delitos de injurias y calumnias. La definición de ambos comportamientos se encuentran en los arts. 205 y 208 CP:

Art. 205 CP: "*Es calumnia la imputación de un delito hecha con conocimiento de su falsedad o temerario desprecio hacia la verdad*".

Art. 208 CP: "*Es injuria la acción o expresión que lesionan la dignidad de otra persona, menoscabando su fama o atentando contra su propia estimación*".

Desde el punto de vista de este trabajo, resulta interesante preguntarse acerca de los supuestos donde el sujeto pasivo de un delito de injurias o calumnias, donde se ha visto lesionado el honor como bien jurídico protegido, entendiendo éste como proyección pública del desarrollo de la libre personalidad, podría invocar el derecho al olvido en los supuestos donde el daño contra su honor haya sido realizado utilizando servicios accesibles en Internet. Sobre esta cuestión, seria necesario profundizar en medidas de tipo cautelar o reparador, en tanto que no tendría sentido que si se condena a una persona por realizar un comportamiento considerado como un delito contra el honor, el contenido sustantivo de la ofensa, el daño efectivo al desarrollo a la libre personalidad en que se concreta el delito, continúe accesible en el mismo espacio digital donde fue realizado en primera instancia, dado que esto sería absurdo, desde el punto de vista de la protección del sujeto pasivo, pero también atendiendo a la pena impuesta al sujeto por dicho comportamiento.

Para cerrar este comentario, puede hacerse una mínima referencia a la normativa penitenciaria que incide en la protección de la esfera de privacidad de los reclusos dentro del sistema penitenciario español. Sobre esta cuestión, resulta de especial interés el art. 6 del Real Decreto 190/1996, de 9 de febrero, por el que se aprueba el Reglamento Penitenciario (RP). Dicho precepto, relativo a la protección de los datos de carácter personal de los ficheros penitenciarios, regula la limitación del uso de la informática penitenciaria:

> ***1.*** *Ninguna decisión de la Administración penitenciaria que implique la apreciación del comportamiento humano de los reclusos podrá fundamentarse, exclusivamente, en un tratamiento automatizado de datos o informaciones que ofrezcan una definición del perfil o de la personalidad del interno.*

***2**. La recogida, tratamiento automatizado y cesión de los datos de carácter personal de los reclusos contenidos en los ficheros se efectuará de acuerdo con lo establecido en la legislación sobre protección de datos de carácter personal y sus normas de desarrollo.*

***3.** Las autoridades penitenciarias responsables de los ficheros informáticos penitenciarios adoptarán las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos de carácter personal en ellos contenidos, así como para evitar su alteración, pérdida, tratamiento o acceso no autorizado, y estarán obligadas, junto con quienes intervengan en cualquier fase del tratamiento automatizado de este tipo de datos, a guardar secreto profesional sobre los mismos, incluso después de que haya finalizado su relación con la Administración penitenciaria.*

***4**. La Administración penitenciaria podrá establecer ficheros de internos que tengan como finalidad garantizar la seguridad y el buen orden del establecimiento, así como la integridad de los internos. En ningún caso la inclusión en dicho fichero determinará por sí misma un régimen de vida distinto de aquél que reglamentariamente corresponda.*

En relación con este precepto, simplemente remarcar las limitaciones establecidas en el art. 6.1 RP respecto de la posibilidad de utilizar datos personales para la elaboración de perfiles delincuenciales basados en pronósticos de peligrosidad criminal fundamentados únicamente en la utilización de datos personales. Esto sería rechazable, en tanto que limitaría las posibilidades de reinserción a una cuestión meramente determinista, basada en el historial delictivo, social, económico o familiar de la persona reclusa. Como establecen los preceptos subsiguientes, todo el tratamiento de datos personales de los internos debe estar sometido a la normativa pertinente sobre protección de datos de carácter personal, pudiendo establecerse ficheros de control de los internos sólo en los supuestos donde sea necesario para garantizar la seguridad y el buen orden del establecimiento (6.4 RP). Una muestra de estas prácticas son los conocidos como Ficheros

de Internos de Especial Seguimiento (FIES), pese a las dudas que ha planteado la doctrina penal sobre su constitucionalidad y su difícil inclusión en el ordenamiento jurídico español[937].

10.4. La protección supranacional del derecho al olvido

Puesto que la vida social, económica, cultural y política de las últimas décadas ha sufrido un proceso de internacionalización, en lógica consonancia, el mismo fenómeno se ha producido frente a los derechos fundamentales que ven como su eficacia y garantía se extiende más allá de las fronteras nacionales.

El ordenamiento jurídico español está vinculado por los tratados sobre derechos humanos celebrados por el Estado español y, en consecuencia, hay previstos mecanismos de garantía para el caso de incumplimiento mediante los cuales, España –en cuanto a sujeto de derecho internacional- podría incurrir en responsabilidad internacional.

En este sentido, el artículo 10.2 CE dispone que "*Las normas relativas a los derechos fundamentales y a las libertades que la Constitución reconoce se interpretarán de conformidad con la Declaración Universal de Derechos Humanos y los tratados y acuerdos internacionales sobre las mismas materias ratificados por España*" y el Tribunal Constitucional ha venido entendiendo que los tratados internacionales sobre derechos humanos suscritos por el Estado español tienen carácter vinculante para la interpretación de los derechos fundamentales recogidos por la Constitución española[938]

Ello se complementa con el mandato del artículo 96.1 CE según el cual "*los tratados internacionales válidamente celebrados, una vez publicados oficialmente en España, formarán parte del ordenamiento interno. Sus disposiciones sólo podrán ser derogadas, modificadas o suspendidas en la forma prevista en los propios tratados o de acuerdo con las normas generales del Derecho internacional*".

---

[937] Cfr. RÍOS MARTÍN, J.C. *Los ficheros de internos de especial seguimiento. Análisis de la normativa reguladora, fundamentos de su ilegalidad y exclusión del ordenamiento jurídico*. Disponible en: http://www.derechopenitenciario.com/comun/fichero.asp?id=995

[938] Entre otras, STC 254/1993, de 20 de julio.

Así, y debido a la inclusión del Estado español en la Unión Europea, el ordenamiento jurídico español se ha visto directamente influenciado por las normas y disposiciones comunitarias y, como ya se ha visto en apartados anteriores[939], en materia de protección de datos son varios los instrumentos comunitarios reguladores de la materia con clara incidencia en el ámbito doméstico[940].

En primer lugar, y como no podía ser de otro modo, el Reglamento Europeo de Protección de datos personales cuyo artículo 17, como ya se ha comentado previamente, recoge por vez primera el derecho al olvido en un instrumento jurídico y de forma expresa, disponiendo que "*el interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales*" concurriendo circunstancias.

Este instrumento habilita a cualquier ciudadano español a interponer demanda bajo la jurisdicción española cuando el responsable o el encargado del tratamiento tenga en este territorio un establecimiento o bien cuándo el interesado resida en el Estado español[941]. Todo ello sin perjuicio de los recursos administrativos o extrajudiciales disponibles, incluido el derecho a presentar una reclamación ante la AEPD u otra autoridad de control en virtud del artículo 77 y 79 del GDPR. Asimismo, se prevé la posibilidad de interponer acciones para reclamar una indemnización por daños y perjuicios –artículo 82.6 GDPR-, así como la posibilidad de imponer multas administrativas –artículo 83.9 GDPR[942]-. Por último, el

[939] Vid. *supra* Cap. III. 3.1.

[940] Resulta interesante la perspectiva de DÍEZ-PICAZO GIMÉNEZ, según la cual "*los derechos fundamentales son también protegidos en el derecho de la Unión Europea. Éste, si bien hoy por hoy tiene su fundamento en una serie de tratados internacionales, es un ordenamiento jurídico diferenciado, resultado de un proceso de integración económica y política sin precedentes entre los Estados miembros de la Unión Europea*". Cfr. *Sistema de derechos Fundamentales*, ob. cit., p. 165.

[941] Artículo 79.2 GDPR: "*Las acciones contra un responsable o encargado del tratamiento deberán ejercitarse ante los tribunales del Estado miembro en el que el responsable o encargado tenga un establecimiento. Alternativamente, tales acciones podrán ejercitarse ante los tribunales del Estado miembro en que el interesado tenga su residencia habitual, a menos que el responsable o el encargado sea una autoridad pública de un Estado miembro que actúe en ejercicio de sus poderes públicos*".

[942] Artículo 83.9 GDPR: "*Cuando el ordenamiento jurídico de un Estado miembro no establezca multas administrativas, el presente artículo podrá aplicarse de tal modo que la incoación de la multa corresponda a la autoridad de control competente y su imposición a los tribunales nacionales competentes, garantizando al mismo tiempo que estas vías de*

Reglamento hace mención al derecho de toda persona física o jurídica a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna, que deberán ejercitarse ante los tribunales del Estado miembro en que esté establecida la misma –artículo 78-.

En segundo lugar, conviene hacer una breve mención sobre el Convenio Europeo de Derechos Humanos cuyo contenido, como se ha expuesto en páginas anteriores, ha producido importante jurisprudencia sobre el derecho a la privacidad, causando un impacto directo en los ordenamientos jurídicos internos. Dicho instrumento contempla también garantías jurisdiccionales, por lo que cualquier persona física, organización no gubernamental o grupo de particulares que se consideren víctima de una violación, por una de las Altas Partes Contratantes, de los derechos reconocidos en el CEDH o sus protocolos, podrá interponer demanda individual frente al Tribunal Europeo de Derechos Humanos[943] (TEDH) –artículo 34 CEDH-, siempre que haya agotado los posibles recursos internos contra la vulneración denunciada –artículo 35 CEDH-.

La legitimación pasiva en este tipo de demandas individuales corresponde siempre al Estado parte que no dio satisfacción a la previa petición de protección del derecho invocado en su jurisdicción. En consecuencia, la demanda individual dará lugar a una sentencia que, una vez firme o definitiva, será vinculante para el Estado parte que haya sido parte en el correspondiente litigio–artículo 46 CEDH-.

Así, en caso de una eventual condena al Estado parte por el TEDH, éste deberá poner fin a la violación del derecho y, en la medida de lo posible, reponer la situación al estado de cosas existente antes de que se produjera la violación. Y, cuando el ordenamiento interno sólo pueda reparar el daño de forma "imperfecta", el CEDH permite la posibilidad de conceder una

---

derecho sean efectivas y tengan un efecto equivalente a las multas administrativas impuestas por las autoridades de control. En cualquier caso, las multas impuestas serán efectivas, proporcionadas y disuasorias".

[943] El hecho de que la Unión Europea no se haya adherido aún al CEDH no ha impedido que el TEDH intervenga en asuntos pertenecientes a su ámbito al interpretar que los Estados parte en el CEDH están vinculados por éste incluso cuando actúan en cumplimiento de obligaciones contraídas en virtud de tratados internacionales o de su pertenencia a organizaciones internacionales.

satisfacción equitativa –artículo 41 CEDH- cuando así sea solicitada por la parte perjudicada, consistente en una condena pecuniaria que contemple tanto el daño material como el daño moral.

De este modo, en caso de considerarse vulnerado el derecho al olvido por parte de la actuación o inacción del Estado español, siempre que se den las circunstancias –como la legitimación procesal activa o haber agotado la vía interna- podrá acudirse al TEDH en aras de obtener una resolución condenatoria así como el cumplimiento efectivo del derecho al olvido y, en su caso, una reparación de los daños y perjuicios sufridos.

Procede recordar aquí que la labor del TEDH en la configuración legal del derecho a la privacidad ha sido muy relevante pues, a través del artículo 8 del CEDH, el Tribunal de Estrasburgo ha afirmado la existencia de un derecho a la protección de datos, a través de una interpretación evolutiva del mismo[944]. La interpretación extensiva de conceptos como vida privada o protección de datos por parte del TEDH ha sido condición indispensable para crear una cultura de protección de la esfera privada y de la información personal[945], presupuestos necesarios para lograr una configuración del derecho al olvido digital.

En tercer lugar, conviene hacer referencia a la Carta de Derechos Fundamentales de la Unión Europea del año 2000 (CDFUE) que establece, por vez primera, un catálogo de derechos específicos para la Unión Europea. Éste instrumento, incorpora nuevos derechos -como la protección de datos- que estaban ausentes, al menos de manera expresa, en el CEDH y les dota

[944] De hecho, el artículo 8 ha sido objeto de distintos exámenes, debates y amplias interpretaciones por parte del TEDH como puede derivarse de los informes periódicos que lleva a cabo el Tribunal de Estrasburgo a tal efecto y cuya última versión, actualizada a fecha de 2015, está disponible online. https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf

[945] Por razones de extensión, resultaría gravoso mencionar aquí todas las sentencias del TEDH con incidencia directa en la materia objeto de estudio aunque, a modo de muestra, pueden señalarse las siguientes: caso *Rotaru v. Romania*, de 4 de mayo de 2000; caso *Times Newspapers v. United Kingdom*, de 10 de marzo de 2009; caso *Mosley v. United Kingdom*, de 10 de mayo de 2011, caso *Ahmet Yildrim v. Turkey*, de 18 de diciembre de 2012, caso *Delfi AS v. Estonia*, de 10 de octubre de 2013.

del mismo valor jurídico que los Tratados, pese a que no se integra en el texto de los Tratados constitutivos ni se incorpora a los mismos como un protocolo anexo[946].

La Carta de Derechos Fundamentales no sólo tiene la fuerza de los Tratados sino que, además, se considera parámetro interpretativo de los propios derechos consagrados en la Constitución. De hecho, el propio Tribunal Constitucional ha acudido a la interpretación de la Carta hecha por el Tribunal de Justicia de la UE para interpretar la propia Constitución[947].

Por último, no puede dejar de contemplarse el Tribunal de Justicia de la Unión Europea (TJUE) dada la evidente importancia que dicho órgano ha tenido sobre el derecho al olvido. El TJUE es el órgano encargado de interpretar la legislación europea para garantizar que exista una interpretación idéntica en todos los países miembros y de resolver, en este contexto, los litigios ocasionados entre los gobiernos nacionales y las instituciones europeas. En algunas ocasiones, los particulares, empresas u organizaciones que crean vulnerados sus derechos por la acción u omisión de una institución de la UE también pueden acudir al TJUE para solicitar una indemnización por daños y perjuicios.

La función primordial del TJUE es interpretar la legislación de la UE para lograr una uniformidad en la aplicación e interpretación de una norma comunitaria por los tribunales domésticos para lo cual, habitualmente éstos recurren a la interposición de decisiones prejudiciales frente al TJUE cuando tiene dudas sobre la interpretación o validez de una norma europea. Fue en el marco de estos procesos, como ya se ha comentado en reiteradas ocasiones a lo largo de este trabajo, cuando el TJUE se pronunció sobre la existencia del derecho al olvido, a petición de la Audiencia Nacional en la STJUE de 13 de mayo de 2014[948].

Y, pese a ser ésta la sentencia del TJUE más importante para el estudio de la cuestión objeto de la presente disertación, no es la única, pues son numerosas las resoluciones de dicho

---

[946] Aún así, el artículo 6.1 del TUE dispone "*La Unión reconoce los derechos, libertades y principios enunciados en la Carta de los Derechos Fundamentales de la Unión Europea de 7 de diciembre de 2000, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados*".

[947] STC 26/2014, de 13 de febrero.

[948] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

órgano que han contribuido a perfilar el contenido del derecho a la protección de datos[949] y que demuestran como los mecanismos supranacionales de garantía de los derechos fundamentales resultan realmente efectivos.

11. Responsabilidad en caso de incumplimiento del derecho al olvido

Afirma REGLERO CAMPOS[950] que "la función primaria de todo sistema de responsabilidad civil es de naturaleza reparatoria o compensatoria: proporcionar a quien sufre un daño injusto los medios jurídicos necesarios para obtener una reparación o una compensación"[951]. Ello es también aplicable a los casos en que se vulnere el derecho al olvido de un determinado individuo pues, los daños y perjuicios que a éste le cause el almacenamiento, tratamiento, difusión o publicidad de una determinada información susceptible de ser protegida por el derecho al olvido, deben de compensarse por aquél que los haya causado, quien se convertirá en responsable del mismo.

DÍEZ PICAZO[952] sostiene que el moderno Derecho de daños aparece precisamente a causa de los avances tecnológicos, fundamentalmente por la necesidad de que los daños sean indemnizados en lugar de quedar impunes, así como por la "racionalización de los eventos y de sus causas". Y siguiendo la línea argumental defendida en este trabajo acerca de la falta de neutralidad de la tecnología, éste pone de relieve que como "entre las repercusiones más importantes que los modernos artilugios o ingenios técnicos producen en el campo jurídico, se

[949] Entre ellas, puede señalarse las sentencias del *caso Lindqvist* (de 6 de noviembre de 2003, petición de decisión prejudicial del Göta hovrätt –Suecia–, en proceso penal *Swedish Prosecutor's Office v. Bodil Lindqvist*, Asunto C-101/01), el *caso Promusicae* (de 29 de enero de 2008, *Productores de Música de España –Promusicae– v. Telefónica de España S.A.U*, Asunto C-275/06,*)*, el *caso Markkinapörssi-Satamedia* (de 16 de diciembre de 2008*, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, Asunto C-73/07), el *caso Rijkeboer* (de 7 de mayo de 2009, Petición de decisión prejudicial del Raad van State –Países Bajos–, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer*, Asunto C-553/07) o el *caso Digital Rights Ireland-Seitlinger y otros* (de 8 de abril de 2014, *Digital Rights Ireland Ltd v. Minister for Communications and Others; Kärntner Landesregierung v. Michael Seitlinger and Others,* Asuntos acumulados C-293/12 y C-594/12).

[950] Cfr. REGLERO CAMPOS, L.F/BUSTO LAGO, J.M. *Tratado de responsabilidad civil*, Aranzadi, Navarra, 2014, p. 81.

[951] No obstante, pese a que su finalidad principal sea la reparación del daño causado, cuando ésta se dificulta o es imposible de llevar a cabo, el perjudicado tendrá derecho a percibir una indemnización en resarcimiento por los daños y perjuicios causados. Por otra parte, no puede ignorarse la función reparatoria-compensatoria y la función preventivo-punitiva de la responsabilidad por daños en determinados supuestos.

[952] DÍEZ-PICAZO. *Derecho y masificación social. Tecnología y Derecho privado (dos esbozos)*, ob. cit., pp. 79 ss.

encuentra el caso de los derechos de la personalidad. Ha sido éste un terreno completamente desguarnecido de tratamiento jurídico". Defiende así el autor, que el Derecho de daños constituye el centro nervioso del Derecho privado, en tanto que deviene un mecanismo imprescindible para la protección de la persona frente a cualquier hecho a la que ésta pueda verse sometida.

Las lesiones a los derechos de la personalidad pueden producirse por cualquier persona con independencia de la relación existente o la ausencia de relación previa entre aquél que produce el daño y aquél que lo sufre[953]. Del mismo modo, el daño ocasionado puede ser tanto material como moral, pudiendo incluso una misma lesión dar lugar a ambos tipos de daño. Frente a la causación del daño o del perjuicio, el Derecho civil –junto a otros mecanismos jurídicos de distinto orden- reconoce al perjudicado el derecho a ser resarcido o compensado por el daño sufrido lo cuál puede llevarse a cabo, bien mediante la eliminación de la fuente que ocasiona el mismo, o bien a través de una compensación económica. En cualquier caso, las acciones de resarcimiento de los daños y perjuicios, constituyen para el sujeto afectado un auténtico derecho subjetivo, mediante el cual obtener la reparación del daño sufrido.

Sin embargo, la responsabilidad civil en el ámbito de Internet y su interacción con las nuevas tecnologías, plantean muchos problemas jurídicos y de determinación de responsabilidades pues, si bien parece evidente que el autor de los contenidos de una página Web así como de los datos transmitidos por una persona le convierten en responsable civil por los daños y perjuicios causados con dicha acción, la dificultad estriba en determinar "si el intermediario que le facilita un espacio, o que posibilita la comunicación y transmisión de datos con terceros es también responsable, frente a terceros, por los contenidos ajenos de los que no es autor, con base en que o bien ha mantenido cierta relación contractual con el autor de la

[953] DIEZ PICAZO/GULLÓN señalan que, el hecho de que se trate de derechos absolutos determina, además, que los beneficios obtenidos de una indebida invasión o lesión de derechos de la personalidad han de ser considerados como enriquecimiento injustificado y se debe al titular de los derechos la restitución del lucro. Cfr. *Sistema de Derecho Civil*, ob. cit., p. 339.

página Web al cederle un espacio propio, o bien facilita o hace posible la comisión de los ilícitos"[954].

Existen diferentes clases de satisfacción previstas en el ordenamiento jurídico para el supuesto de violación de un derecho fundamental lo que no cabe confundir, como ya se ha examinado anteriormente, con los procedimientos para obtener dichos remedios. DÍEZ-PICAZO GIMÉNEZ[955] sistematiza los tipos de reparación existentes frente a violaciones de derechos fundamentales en el ordenamiento jurídico español, de la siguiente manera: "A) Anulación de las disposiciones normativas (legales o reglamentarias) y de actos singulares (administrativos o jurisdiccionales) contrarios a un derecho fundamental. B) Mero reconocimiento declarativo de la titularidad del derecho fundamental objeto del litigio, o de la legitimidad de su ejercicio. C) Prohibición de conductas perturbadoras del ejercicio de derechos fundamentales. D) Restablecimiento de la situación jurídica subjetiva anterior a la violación del derecho fundamental, incluida la indemnización, en su caso, de los daños (materiales y morales) sufridos en los derechos fundamentales. E) Tutela provisional a través de las medidas cautelares". A lo que habría que añadir los remedios indirectos, consistentes en las sanciones penales so administrativas para conductas lesivas de derechos fundamentales.

11.1 Responsabilidad contractual y extracontractual

Debe considerarse, asimismo la distinción entre responsabilidad contractual y extracontractual o civil (derecho de daños, en un sentido estricto) pues la primera tiene lugar cuando existe una obligación previa entre el causante del daño y la víctima, mientras que la responsabilidad extracontractual se origina con independencia de la presencia de una obligación anterior entre dichos sujetos, pues ésta deriva del deber general de no ocasionar daño a los demás, *alterum non laedere*[956].

---

[954] PLAZA PENADÉS. "La responsabilidad civil de los intermediarios en Internet y otras redes" en *Contratación y comercio electrónico* (Orduña Moreno coord.), Tirant lo Blanch, València, 2003, p. 200.

[955] Cfr. *Sistema de derechos Fundamentales*, ob. cit., p. 94.

[956] No obstante, esta distinción es efectiva a efectos de su examen desde el punto de vista de la tradición jurídica continental pues su óptica diverge en muchos aspectos sustanciales respecto de la tradición anglosajona. Así, por ejemplo, mientras que en el *common law* la responsabilidad contractual es principalmente objetiva y, por el contrario, la responsabilidad

En líneas generales podría decirse que la responsabilidad contractual tiene su presupuesto en el incumplimiento (o en el cumplimiento inexacto o parcial) de las obligaciones derivadas de un contrato, por lo que los intereses protegidos ésta hacen referencia a los deberes asumidos entre las partes en el contrato (artículo 1.101 CC), ya sea explícitamente, o por aplicación de las fuentes de integración del mismo conforme al artículo 1.258, siempre dentro de los límites generales del artículo 1.255 CC. Sin embargo, la existencia de un contrato entre el causante del daño y la víctima del mismo no puede excluir por sí sola la responsabilidad extracontractual pues es perfectamente posible que unos mismos hechos constituyan el supuesto de hecho normativo de ambas responsabilidades[957]. Ello se debe a que ambas son instituciones pertenecientes a la misma categoría pese a que tienen importantes matices contrapuestos[958], principalmente en lo que se refiere a cuestiones de carácter procesal, lo que ocasiona no pocos problemas de cara a determinación de los ámbitos de responsabilidad[959].

Por otra parte, en la responsabilidad extracontractual, no existe vinculación previa alguna entre los sujetos intervinientes, sino que la obligación se genera *ex post*, a consecuencia del daño producido. Por ello, en el derecho de daños, la culpa o negligencia del sujeto que ha provocado el daño así como la relación de causalidad, tienen una posición predominante en la materia. La jurisprudencia del Tribunal Supremo[960] ha ayudado a configurar los requisitos de la responsabilidad extracontractual que pueden resumirse en la necesidad de probar la existencia de una acción u omisión que haya provocado un daño o un perjuicio, debido a un

---

extracontractual se deriva del comportamiento negligente; en nuestro ordenamiento jurídico, puede afirmarse que la responsabilidad contractual parte eminentemente del principio general de negligencia.

[957] CONCEPCIÓN RODRÍGUEZ. *Derecho de daños*, Bosch, Barcelona, 1999, pp. 28-29.

[958] "*Los artículos 1.101 y 1.902 CC, sancionadores, respectivamente, de la culpa contractual y de la extracontractual en el Código civil, responden a un principio común de derecho y a la misma finalidad indemnizatoria*", STS de 30 de diciembre (RJ 1980, 4815), considerando 2º.

[959] REGLERO CAMPOS sistematiza los casos problemáticos, a los que llama "supuestos transfronterizos entre ambos tipos de responsabilidad" en dos grupos, por una parte, los daños derivados de situaciones precontractuales, postcontractuales o paracontractuales y, por otra parte, aquellos que deriven de una situación en la que preexista una relación jurídica entre las partes, de naturaleza distinta a la contractual pero análoga a ella. Cfr. *Tratado de responsabilidad civil*, ob. cit., pp. 168-178.

[960] Por todas, STS 448/1998, de 18 de mayo.

comportamiento imprudente o negligente cuya causación resulta claramente atribuible a una determinada persona o entidad[961].

Respecto del derecho al olvido, el mecanismo jurídico para el resarcimiento de los daños y perjuicios que pueda ocasionar su vulneración se remite fundamentalmente al mecanismo de la responsabilidad extracontractual puesto que, entre el perjudicado y el causante del daño, no suele haber una vinculación contractual previa[962]. Piénsese, por ejemplo, en la interacción de los motores de búsqueda y su capacidad de lesión para el derecho al olvido de cualquier persona[963], como ya se evidenció en la sentencia del TJUE del caso *Google*, comentada en numerosas ocasiones a lo largo de este trabajo[964]. Ello no obsta la existencia de otros supuestos en los que, habiendo el interesado aceptado las condiciones generales de un determinado producto o servicio, quede éste contractualmente vinculado al causante del daño.

Los preceptos relativos a la responsabilidad civil vienen contemplados en el Capítulo II del Título XVI del Libro IV del Código civil, principiados por el artículo 1.902 que dispone "*el*

[961] Sin embargo, esta cuestión es discutida frecuentemente por la doctrina, una parte de la cual defiende que el esquema clásico ya no responde a la realidad del vigente Derecho de daños. En este sentido, afirma PEÑA LÓPEZ "De todos los presupuestos con los que se construía el concepto abstracto de ilícito extracontractual, sólo puede seguir manteniéndose que son elementos comunes del conjunto de regímenes que constituyen la responsabilidad civil extracontractual: el daño y la antijuricidad del daño (la determinación de los intereses protegidos por el sistema)". Afirma el autor pues, que el resto de los presupuestos de la cláusula general de responsabilidad del artículo 1.902 CC –la culpa, la acción u omisión y la relación de causalidad- no son elementos que necesariamente estén presentes en todos los regímenes de responsabilidad civil. Cfr. "De las obligaciones que nacen de culpa o negligencia" en *Comentarios al Código Civil* (Bercovitz Rodríguez-Cano Dir.), Tomo IX, Tirant lo Blanch, València, 2013, pp. 12962-12963.

[962] Así se entendió en la doctrina española desde un principio, como puede observarse en la ya citada SAP Barcelona 486/2013, Sección 14, mediante la cuál se produce el primer pronunciamiento jurisprudencial sobre el derecho al olvido en territorio español y que condenó al causante de la difusión de la información de los daños producidos a las personas perjudicadas en su derecho al honor, usando argumentos propios de la responsabilidad extracontractual.

[963] Íntimamente relacionado con ello, y siguiendo la línea argumental más moderna, REGLERO CAMPOS afirma que "el estrechamiento del campo de juego del tradicional criterio de imputación, junto con la revisión del elemento causal, permite afirmar que hoy sólo constituye presupuesto necesario de la responsabilidad civil la propia existencia del daño, por un lado, y su atribución a un determinado sujeto en virtud de un adecuado título de imputación, por otro". Cfr. *Tratado de responsabilidad civil*, ob. cit., p. 74.

[964] SIMÓN CASTELLANO afirma que el derecho al olvido se basa en el principio de responsabilidad por culpa y, para ello, se remonta hasta la jurisprudencia quebequesa que así lo estipuló –entendiendo el derecho al olvido como la difusión de una información que ha perdido la virtualidad pasado un tiempo, y que al volver a darle publicidad causa un daño a su protagonista- en una sentencia del siglo XIX (*Cour Supérieure du Quedeb, Goyette v. Rodier* (1889) 20 R.L. 108, 110) que dispuso el principio general, según el cuál todo el mundo tiene que respetar las normas de conducta con objeto de no causar daño a terceros. Cfr. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, ob. cit., p. 104.

que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado" y que, sencillamente, estipula la obligación (*ex post*) de toda persona que cause un daño ilegítimo a otra, de repararlo. Sin embargo, dada la escasa dedicación del Código Civil a dicha cuestión así como a la inmutabilidad de sus preceptos, la regulación de la responsabilidad civil ha sido ampliada, mediante la legislación especial[965] como podrá observarse a continuación, mediante el examen de las disposiciones del Reglamento europeo de protección de datos a tal efecto, así como de 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.

Tal y como se ha señalado anteriormente, la cuestión de la responsabilidad en el ámbito que nos ocupa la presente disertación, tiene algunas dificultades añadidas, principalmente, en términos de identificación del responsable y de las conductas susceptibles de causar daño, a lo que debe añadirse la ampliación exponencial del concepto de "jurisdicción" en el campo de Internet así como la idiosincrasia propia del campo del Big data y las nuevas tecnologías inteligentes. Ello plantea enormes dudas, también desde el punto de vista del derecho contractual, en base al empleo de cláusulas contractuales limitativas o exoneradoras de responsabilidad en los contratos de adhesión empleados en este ámbito, como también de las políticas de privacidad impuestas por las corporaciones del Big data en este contexto que, frecuentemente, contienen cláusulas abusivas, con las implicaciones innegables que de ello se desprenden con las relaciones de consumo. Teniendo esto en cuenta, así como las limitaciones de extensión y profundidad propias de este trabajo, se ha considerado oportuno no ahondar en demasía en cuestiones generales o de planteamiento, para centrar la investigación en la legislación especial propia del objeto de estudio.

11.2 Reglamento General de Protección de Datos

Como se ha descrito en apartados anteriores, son varias las vías que tiene una persona para ejercitar su derecho al olvido y obtener la tutela de su derecho a la protección de datos

[965] Así pues, incluso respecto de las cuestiones que se han tratado a lo largo de la disertación, hay que tener en cuenta diversas normas especiales que regulan aspectos relativos a la incidencia de Internet en los derechos y libertades, como la Ley de Propiedad Intelectual o la Ley General para la Defensa de los Consumidores y Usuarios.

personales como consecuencia de una infracción. Así, ya se ha explicado anteriormente como el GDPR prevé una doble vía de actuación para el interesado, pudiendo acudir alternativa o conjuntamente a una autoridad de control o a los órganos jurisdiccionales para la defensa de sus derechos.

En cuanto a la primera de las opciones, el artículo 77 GDPR dispone que todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control, ya sea la propia del Estado en la que éste tenga su residencia habitual, como la relativa en su lugar de trabajo, o la situada en el lugar de la infracción cometida, pudiendo asimismo –según entendemos- instar dicho procedimiento ante otra autoridad de control siempre y cuando se acrediten puntos de conexión suficientes[966].

En segundo lugar, el artículo 78 recoge la posibilidad de que toda persona física o jurídica, sin perjuicio de cualquier otro recurso administrativo o extrajudicial, pueda acudir a los órganos jurisdiccionales para obtener la tutela de su derecho a la protección de datos. De este modo, contra una decisión administrativa emitida por la autoridad de control, en base al procedimiento anterior, así como cuando ésta no curse dicha reclamación o no lo haga conforme a las garantías, procedimientos o plazos previstos -3 meses-, el interesado podrá dirigirse a los tribunales del Estado miembro donde se encuentre dicha autoridad de control para recabar su tutela.

En tercer lugar, y de forma no excluyente, el Reglamento prevé en su artículo 79 la posibilidad de que el interesado se dirija directamente frente al responsable o al encargado del tratamiento de sus datos personales, mediante la interposición de acciones bien, ante los tribunales del Estado miembro donde éste tenga su residencia habitual, bien ante los órganos jurisdiccionales donde el responsable o el encargado tengan su establecimiento, a su elección.

Como ya se ha comentado a lo largo de este trabajo, el artículo 80 GDPR permite que, para el ejercicio de los derechos anteriores, el interesado sea representado por una entidad,

[966] Ello se derivaría indirectamente del empleo de la expresión "en particular" de dicho precepto, que sugiere la posibilidad de extender la legitimación hacia otras autoridades de control, no especificadas en el art. 77 GDPR, cuando éstas guarden relación con el interesado o con el supuesto de hecho.

organización o asociación sin ánimo de lucro, legalmente constituida y cuyos objetivos estatutarios se inserten en el ámbito de la protección de datos, que ejerza en su nombre sus derechos. Lo que, en el terreno práctico, tiene indudablemente una gran repercusión, pues se dota a los ciudadanos de gran fuerza y capacidad de acción frente a posibles vulneraciones masivas de datos personales, facilitando la protección de los consumidores y usuarios del entorno digital gracias a su acción colectiva

a) Indemnización por daños y perjuicios

Otra cuestión es la relativa al ejercicio de acciones derivadas de la causación de un daño o perjuicio al interesado. El artículo 82 GDPR dispone que toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción de sus disposiciones, tendrá derecho a recibir del responsable o del encargado del tratamiento, según corresponda, una indemnización por los daños y perjuicios sufridos.

En cuanto al régimen de responsabilidad, ello exige algunas matizaciones. En primer lugar, respecto del contenido material de los daños y perjuicios indemnizables, la amplia configuración del Reglamento, permite incluir bajo su articulado, tanto perjuicios patrimoniales como los morales, siendo necesario que los órganos jurisdiccionales, en el procedimiento para su determinación y cuantificación, además de los daños materiales, tengan en cuenta aquéllos otros perjuicios indemnizables así como los intereses que se puedan desprender del desprestigio o menoscabo de la credibilidad personal o profesional[967]. En relación a dicha cuestión, debe acudirse a la jurisprudencia del Tribunal Supremo dictada sobre esta materia, como la STS 557/2015, de 18 de febrero, de la Sala de lo Civil que, en un supuesto de inclusión de los datos personales del interesado en un fichero automatizado que constituía un registro de morosos, se

[967] Otra cuestión distinta y más compleja es la relativa a la determinación de las cuantías objeto de indemnización pues los órganos jurisdiccionales, a la hora de valorar los daños y perjuicios causados y su cuantificación, deberán tener en cuenta no sólo la doctrina interna, sino también las interpretaciones que se deriven, en su caso, de la jurisprudencia del TJUE. Así lo dispone expresamente el considerando 146º del GDPR, según el cuál "*el concepto de daños y perjuicios debe interpretarse en sentido amplio a la luz de la jurisprudencia del Tribunal de Justicia, de tal modo que se respeten plenamente los objetivos del presente Reglamento*".

le concede una indemnización por daños y perjuicios al entender que se había vulnerado su derecho al honor.

El Tribunal Supremo, afirma que en este tipo de indemnizaciones debe incluirse "*el daño patrimonial, y en él, tanto los daños patrimoniales concretos, fácilmente verificables y cuantificables* […] *como los daños patrimoniales más difusos pero también reales e indemnizables, como son los derivados de la imposibilidad o dificultad para obtener crédito o contratar servicios* […] *y también los daños derivados del desprestigio y deterioro de la imagen de solvencia personal y profesional*" (FJ 4º). Asimismo, dispone el Alto Tribunal que la indemnización también debe resarcir el daño moral "*entendido como aquel que no afecta a los bienes materiales que integran el patrimonio de una persona, sino que supone un menoscabo de la persona en sí misma, de los bienes ligados a la personalidad, por cuanto que afectan a alguna de las características que integran el núcleo de la personalidad, como es en este caso la dignidad*" así como el quebranto y la angustia producida por "*las gestiones más o menos complicadas que haya tenido que realizar el afectado para lograr la rectificación o cancelación de los datos incorrectamente tratados*" (FJ 5º).

En segundo lugar, se establece un régimen distinto de responsabilidad según se trate del encargado de tratamiento o del responsable por lo que, mientras que un encargado sólo responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligación que el GDPR dispone específicamente a los encargados, o haya actuado al margen o en contra de las instrucciones legales del responsable, éste último responderá siempre que haya participado en la operación de tratamiento que no cumpla con lo dispuesto por el Reglamento. Se establece así, respecto del responsable, un régimen de responsabilidad objetiva, al contrario que respecto del encargado, que sólo responderá de los daños y perjuicios causados cuando pueda acreditarse que una operación de tratamiento no cumple con lo dispuesto por el GDPR por su culpa o negligencia (artículo 82.2). No obstante, el Reglamento prevé la posibilidad de que ambos actores queden exonerados de responsabilidad cuando consigan probar que no son de modo alguno responsables del hecho que haya causado los daños y perjuicios (artículo 82.3), lo que resulta un tanto contradictorio con lo anterior.

En tercer lugar, cuando sean varios los responsables o encargados del tratamiento o cuando un responsable y un encargado hayan participado en la misma operación de tratamiento del que resulten responsables de cualquier daño o perjuicio sufrido, con la finalidad de garantizar la indemnización efectiva del interesado, cada uno de ellos será considerado responsable de todos los daños y perjuicios (artículo 82.4). No obstante, cuando uno de ellos haya pagado solidariamente dichos daños y perjuicios, tendrá acción de repetición contra el resto de encargados y responsables que hubiesen participado en el tratamiento que dio lugar a los daños y perjuicios, la parte que les corresponda del pago de la indemnización (artículo 82.5).

El considerando 146 del Reglamento, sin embargo, prevé que cuando, acumulándose en una misma causa la indemnización, los obligados al pago puedan individualizar el daño, posibilitando el prorrateo de la indemnización en función de la responsabilidad de cada responsable o encargado por los daños y perjuicios causados por el tratamiento, siempre que se garantice la indemnización total y efectiva del interesado que sufrió los daños y perjuicios.

Por otra parte, procede destacar la posibilidad que abre el GDPR de acudir a la mediación o al arbitraje, como una vía extrajudicial de resolución de conflictos a la que acudir en un procedimiento de reclamación de indemnizaciones por daños y perjuicios[968]. Esta tercera vía puede reportar ventajas para los diversos sujetos que participen en ella, desde las empresas que sean responsables por los daños y perjuicios causados en el tratamiento, que podrán negociar las cantidades para la satisfacción de las indemnizaciones y evitaran la publicidad negativa que acarrea la imposición de una multa, hasta para los propios sujetos afectados, que recibirán personalmente las cuantías indemnizatorias, en lugar del Tesoro público.

Finalmente, y en cuanto al régimen de responsabilidad previsto en la legislación doméstica, la todavía vigente LOPD, recogiendo el mandato previsto por la derogada Directiva 95/46/CE de protección de datos, que contemplaba la posibilidad de obtener del responsable

[968] Artículos 40.2.k), 78 y 79 GDPR.

del tratamiento la reparación del perjuicio ocasionado[969], dispone en su artículo 19.1 que "*los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados*", instando a los afectados a ejercitar la acción ante los tribunales ordinarios en el caso de ficheros de titularidad privada, previendo reglas específicas respecto de los ficheros de titularidad pública[970].De este modo, la regulación prevista en el GDPR parece ampliar las vías de tutela para los afectados.

En el Proyecto de Ley Orgánica de Protección de Datos –en tramitación parlamentaria mientras se elabora este trabajo- su articulado se limita a mencionar el carácter solidario de la responsabilidad que, en cumplimiento del artículo 82 GDPR, pudiera imponerse por daños y perjuicios, respecto de los responsables, encargados y representantes de éstos, cuando no estén establecidos en la Unión Europea. Aunque sería deseable, una referencia expresa a las acciones de indemnización por daños y perjuicios, tanto desde el punto de vista de los ciudadanos afectados como por parte de los responsables y encargados del tratamiento, en la nueva regulación, que adolece de ciertas insuficiencias, sin embargo ello, en términos prácticos, no supone un menoscabo de los derechos de los interesados en tanto que, al ser el GDPR directamente aplicable, ello permite a los afectados obtener la indemnización por daños y perjuicios en los términos previstos en él.

b) Sanciones administrativas

Ante el incumplimiento de las disposiciones del Reglamento europeo de protección de datos, cada autoridad de control tiene facultades para imponer, de forma individual, multas administrativas efectivas, proporcionadas y disuasorias (considerando 150). El artículo 83, además, dispone las circunstancias que deben tenerse en cuenta para modular la imposición de

[969] Artículo 23 y considerando 55º. Éstos, asimismo, permitían la exención de la responsabilidad del responsable del tratamiento cuando pudiese demostrar la responsabilidad del interesado en la causación de dicho perjuicio, o la concurrencia de una causa de fuerza mayor.

[970] Artículo 19.2 LOPD: "*Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas*". Regulando, asimismo, los pormenores de los ficheros de titularidad pública en su Capítulo I, artículo 20 y ss.

multas y su cuantía: a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido; b) la intencionalidad o negligencia en la infracción; c) las medidas tomadas para paliar los daños y perjuicios sufridos por los interesados; d) el grado de responsabilidad del responsable o del encargado del tratamiento; e) las infracciones anteriores cometidas; f) el grado de cooperación con la autoridad de control para remediar la infracción y mitigar los efectos adversos de la infracción; g) la tipología de datos afectados por la infracción; h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida; i) la imposición previa de medidas correctivas; j) la adhesión a códigos de conducta o a mecanismos de certificación, y k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.

Las multas previstas en el GDPR oscilan en cuantía, en función de la tipología de infracción en la cual se incurra, de hasta 10.000.000 euros, según la tipificación de las conductas o hasta el 2% del volumen de negocio total anual global del ejercicio financiero anterior de una empresa; o hasta un máximo de 20.000.000 euros o hasta el 4% del volumen de negocio total anual global del ejercicio financiero anterior, según el tipo de incumplimientos que se lleve a cabo[971]. En cuanto a las administraciones públicas, el Reglamento delega en los

[971] Artículo 83.4 GDPR. "*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;

b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;

c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4".

Artículo 83.5 GDPR. "*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 %*

Estados miembros las facultades para que decidan las condiciones bajo las cuales, en su caso, se les podría sancionar (artículo 83.7).

En relación al régimen sancionador, procede señalar que numerosos preceptos del GDPR remiten su desarrollo a la legislación doméstica de los Estos miembros, entre los cuales se encuentran la regulación del estatuto de las autoridades de control, la determinación del régimen aplicable a los inspectores de un tercer Estado que lleven a cabo actividades conjuntas de investigación, o la designación de la autoridad que representará a cada Estado ante el Comité Europeo de Protección de Datos (artículos 83 y siguientes). Otros artículos del Reglamento, pese a no constituir remisiones expresas, exigen una adecuación del Derecho interno a las pautas marcadas por la legislación europea como, por ejemplo, en lo relativo a la determinación de los plazos de prescripción.

En cuanto al régimen sancionador en la legislación doméstica, pese a que la LOPD sigue estando en vigor mientras no se apruebe el Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal, su contenido correspondiente al régimen de infracciones y sanciones (artículos 43 y siguientes) ha sido derogado en su mayor parte por el *Real Decreto-ley 5/2018,*

---

como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;

b) los derechos de los interesados a tenor de los artículos 12 a 22;

c) las transferencias de datos personales a un destinatario en un tercer país o una organización internacional a tenor de los artículos 44 a 49;

d) toda obligación en virtud del Derecho de los Estados miembros que se adopte con arreglo al capítulo IX;

e) el incumplimiento de una resolución o de una limitación temporal o definitiva del tratamiento o la suspensión de los flujos de datos por parte de la autoridad de control con arreglo al artículo 58, apartado 2, o el no facilitar acceso en incumplimiento del artículo 58, apartado 1".

Artículo 83.6 GDPR. "*El incumplimiento de las resoluciones de la autoridad de control a tenor del artículo 58, apartado 2, se sancionará de acuerdo con el apartado 2 del presente artículo con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía*".

de 27 de julio, de medidas urgentes para la adaptación del decreto español a la normativa de la Unión Europea en materia de protección de datos[972].

En dicho instrumento -el cual inevitablemente pone en evidencia la dejación del legislador a la hora de cumplimentar el mandato del GDPR en el plazo establecido para ello- se dispone, entre otras cuestiones accesorias, el régimen sancionador resultante de los postulados del GDPR, en especial lo dispuesto en sus aparatados 4, 5 y 6 de su artículo 83, delimitando los sujetos que pudieran incurrir en la responsabilidad derivada de la aplicación del régimen sancionador[973], y determinando los plazos de prescripción de las infracciones[974] y sanciones[975]

---

[972] La promulgación de este Real Decreto-ley, por otra parte, es una decisión ciertamente cuestionable en términos de constitucionalidad, pues en él se contienen aspectos inherentes a un derecho fundamental y, en consecuencia, su regulación parece que debería estar sometida a una Ley Orgánica, no bastando el argumento de la urgencia ni de que en él se tratan cuestiones accesorias, para justificarlo.

[973] Artículo 3. Sujetos responsables.

1. "*Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y la normativa española de protección de datos:*

a) Los responsables de los tratamientos.

b) Los encargados de los tratamientos.

c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.

d) Las entidades de certificación.

e) Las entidades acreditadas de supervisión de los códigos de conducta.

2. No será de aplicación al delegado de protección de datos el régimen sancionador en esta materia".

[974] Artículo 5. Prescripción de las infracciones.

1. "*Las infracciones previstas en los apartados 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 prescribirán a los tres años.*

2. Las infracciones previstas en el artículo 83.4 Reglamento (UE) 2016/679 prescribirán a los dos años.

3. Interrumpirá la prescripción la iniciación, con conocimiento del interesado, del procedimiento sancionador, reiniciándose el plazo de prescripción si el expediente sancionador estuviere paralizado durante más de seis meses por causas no imputables al presunto infractor.

Cuando la Agencia Española de Protección de Datos ostente la condición de autoridad de control principal y deba seguirse el procedimiento previsto en el artículo 60 del Reglamento (UE) 2016/679 interrumpirá la prescripción el conocimiento formal por el interesado del proyecto de acuerdo de inicio que sea sometido a las autoridades de control interesadas".

[975] Artículo 6. Prescripción de las sanciones.

1. "*Las sanciones impuestas en aplicación del Reglamento (UE) 2016/679 prescriben en los siguientes plazos:*

a) Las sanciones por importe igual o inferior a 40.000 euros, prescriben en el plazo de un año.

b) Las sanciones por importe comprendido entre 40.001 y 300.000 euros prescriben a los dos años.

previstas en la norma europea pues, precisamente, uno de los objetivos claves del GDPR era, precisamente, unificar la normativa de los Estados miembros relativa a las sanciones así como sus cuantías (considerando 13, 129 y 150). Para ello, principalmente, se reproduce el contenido extractado del Proyecto de Ley Orgánica de Protección de Datos Personales, sometido actualmente a tramitación parlamentaria.

En dicho Real Decreto-ley, además, se regula el procedimiento en caso de plantearse una reclamación ante la AEPD (iniciación, duración, admisión a trámite, alcance territorial, actuaciones previas, medidas provisionales…) la cuál se designa como representante de España en el Comité Europeo de Protección de Datos, y se articula el sometimiento a sus resoluciones para el caso de que no se alcance un acuerdo entre autoridades de control en los tratamientos transfronterizos, en un contexto en el que, siendo el GDPR directamente aplicable, necesitaba algunas concreciones por la legislación doméstica.

De todo lo anterior puede concluirse que el régimen sancionador actual en materia de protección de datos, a resultas de las modificaciones introducidas por el Reglamento europeo así como debido a sus constantes remisiones a las legislaciones domésticas e inclusión de preceptos abiertos, junto con la amalgama normativa del ordenamiento español en dicha materia, éste reviste de una gran complejidad y está sujeto a múltiples interpretaciones sobre las cuales, además, no sólo incidirán los órganos jurisdiccionales, sino también la Agencia Española de Protección de Datos y el Delegado de Protección de datos correspondiente. Resulta urgente, en consecuencia, la promulgación de una legislación unitaria, entre otras muchas cuestiones, en dicha materia.

---

c) Las sanciones por un importe superior a 300.000 euros prescriben a los tres años.

2. 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.

3. La prescripción se interrumpirá por la iniciación, con conocimiento del interesado, del procedimiento de ejecución, volviendo a transcurrir el plazo si el mismo está paralizado durante más de seis meses por causa no imputable al infractor".

11.3 Servicios de la Sociedad de la Información y del comercio electrónico

Los servicios de la sociedad de información, como ha apuntado el Tribunal de Justicia de la Unión Europea, son aquellos "*servicios prestados a distancia, mediante equipos electrónicos de tratamiento y almacenamiento de datos, a petición individual de un destinatario de servicios y normalmente a cambio de una remuneración*"[976], también conocidos como "*online service providers* (OSPs)" o "*Internet service providers* (ISPs)".

Éstos, al actuar como intermediarios en la Sociedad de la Información, tienen una gran incidencia en el funcionamiento del mercado interior así como en cuestiones de competencia, por lo que, desde el ámbito europeo se estimó conveniente armonizar las normas de los Estados miembros en dicha materia para facilitar dirimir las responsabilidades civiles inherentes a la actuación de los prestadores de servicios[977].

Ello se llevó mediante la Directiva 2000/31/CE sobre el comercio electrónico[978], la cuál tiene por objeto, eliminar los obstáculos jurídicos que se oponen al desarrollo de los servicios de la información y al buen funcionamiento del mercado interior "*que hacen menos atractivo el ejercicio de la libertad de establecimiento y de la libre circulación de servicios*. *Dichos obstáculos tienen su origen en la disparidad de legislaciones, así como en la inseguridad jurídica de los regímenes nacionales aplicables a estos servicios; a falta de coordinación y ajuste de las legislaciones en los ámbitos en cuestión*"[979]. Sin embargo, conviene señalar que las fórmulas abiertas de sus preceptos así como las remisiones a las legislaciones domésticas

[976] STJUE (Gran Sala), de 23 de marzo de 2010, *Google France SARL y Google Inc. v. Louis Vuitton Malletier SA,* Asuntos acumulados C-236/08 y C-238/08, punto 110.

[977] Como señala DÍAZ FRAILE, la Directiva logró un difícil consenso entre países anglosajones y nórdicos, por un lado, y países centroeuropeos y mediterráneos por otro. La Directiva "integra elementos de Derecho continental con otros de Derecho anglosajón, del que procede fundamentalmente la inspiración en la redacción de los artículos relativos a los códigos de conducta y a la resolución extrajudicial de los conflictos, así como la idea de intervención legislativa mínima". Cfr. "Aspectos jurídicos más relevantes de la directiva y del proyecto de ley español de comercio electrónico" en *Contratación y comercio electrónico* (Orduña Moreno coord.), Tirant lo Blanch, València, 2003, pp. 79-80.

[978] Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado interior.

[979] Considerando 5º.

dejaron a los Estados miembro, en la práctica, un gran margen de discrecionalidad para su trasposición[980].

Dicha Directiva fue traspuesta en la legislación española mediante la *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico* (LSSICE en adelante), actualmente en vigor, que regula en el ámbito doméstico la responsabilidad civil de los prestadores de servicios de la sociedad de la información. Como señala PLAZA PENADÉS, la expansión de las redes de telecomunicaciones y, en especial de Internet, generaron unas incertidumbres jurídicas que también involucraron al ámbito de contratación electrónica así como de los ilícitos cometidos en la Red, por lo que, mediante la LSSICE, se establece un marco jurídico adecuado a dichas necesidades, con la finalidad principal de dotar de seguridad jurídica a todos los intervinientes y usuarios de este nuevo medio[981].

La Ley acoge un concepto amplio de "servicios de la sociedad de la información", incluyendo en él el suministro de información por vía electrónica –como los periódicos o revistas-, actividades de intermediación para la provisión de acceso a la Red, la transmisión de datos por redes de telecomunicación, la realización de copias temporales de páginas web, servicios, aplicaciones e instrumentos de búsqueda o de enlaces a otros sitios de Internet, así como otros servicios que se presten a petición individual de los usuarios cuando representen una actividad económica para el prestador[982]. En definitiva, como dispone el preámbulo de la LSSICE "*estos servicios son ofrecidos por los operadores de telecomunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades indicadas, incluido el comercio electrónico*".

[980] Así, por ejemplo, la Directiva dispone que la imputación de la responsabilidad civil se hará de conformidad con las normas propias de los distintos Derechos nacionales (considerando 22º).

[981] Cfr. "Los principales aspectos de la Ley de Servicios de la Sociedad de la Información y Comercio electrónico" en *Contratación y comercio electrónico* (Orduña Moreno coord.), Tirant lo Blanch, València, 2003, p. 32.

[982] Esto excluye expresamente la responsabilidad civil que pueda derivarse de los servicios prestados por medio de telefonía vocal o fax así como del intercambio de información mediante el empleo del correo electrónico u otro medio electrónico equivalente, cuando se lleve a cabo en un contexto no profesional, sin ninguna finalidad económica aparejada.

En cuanto a su objeto, el artículo 1 dispone que se trata de "*la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúan como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información*". No obstante, como especifica en el segundo apartado de dicho precepto, sus disposiciones se entenderán sin perjuicio de lo dispuesto en otras normas especiales, entre las cuales explicita la relativa a la protección de los datos personales.

En cuanto a lo que aquí interesa, la LSSICE establece las obligaciones y responsabilidades de los prestadores de servicios que lleven a cabo actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en Internet. Así, su artículo 13.1 dispone "los prestadores de servicios de la sociedad de la información están sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley". El anexo de la LSSICE recoge la definición de los servicios de intermediación disponiendo que "*son servicios de intermediación la provisión de servicios de acceso a Internet, la transmisión de datos por redes de telecomunicaciones, la realización de copia temporal de las páginas de Internet solicitadas por los usuarios, el alojamiento en los propios servidores de datos, aplicaciones o servicios suministrados por otros y la provisión de instrumentos de búsqueda, acceso y recopilación de datos o de enlaces a otros sitios de Internet*". Así las cosas, ello permite concluir que los motores de búsqueda son servicios de intermediación y, en consecuencia quedan sometidos a dicha legislación, con los derechos y responsabilidades que ello conlleva.

El artículo 2, por su parte, dispone la aplicación de dicha legislación a aquellos servicios que se presten efectivamente en territorio español, y lo hace en un sentido amplio[983], lo que ha

[983] Artículo 2. Prestadores de servicios establecidos en España.

permitido a los tribunales someter su articulado a las empresas que, pese a tener su establecimiento o residencia en otro Estado[984], tuviesen en España, de forma continuada o habitual, instalaciones o lugares de trabajo para realizar, cuanto menos, parte de su actividad[985].

Junto al régimen general del artículo 13, la LSSICE regula un régimen específico respecto de las responsabilidades de los operadores de redes y proveedores de acceso (artículo 14). Asimismo, el artículo 15 y siguientes regulan las causas por las que puede exonerarse de responsabilidad a los proveedores de servicios que realicen copia temporal de datos[986],

---

1. "*Esta Ley será de aplicación a los prestadores de servicios de la sociedad de la información establecidos en España y a los servicios prestados por ellos.*

Se entenderá que un prestador de servicios está establecido en España cuando su residencia o domicilio social se encuentren en territorio español, siempre que éstos coincidan con el lugar en que esté efectivamente centralizada la gestión administrativa y la dirección de sus negocios. En otro caso, se atenderá al lugar en que se realice dicha gestión o dirección.

2. Asimismo, esta Ley será de aplicación a los servicios de la sociedad de la información que los prestadores residentes o domiciliados en otro Estado ofrezcan a través de un establecimiento permanente situado en España.

Se considerará que un prestador opera mediante un establecimiento permanente situado en territorio español cuando disponga en el mismo, de forma continuada o habitual, de instalaciones o lugares de trabajo, en los que realice toda o parte de su actividad.

3. A los efectos previstos en este artículo, se presumirá que el prestador de servicios está establecido en España cuando el prestador o alguna de sus sucursales se haya inscrito en el Registro Mercantil o en otro registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

La utilización de medios tecnológicos situados en España, para la prestación o el acceso al servicio, no servirá como criterio para determinar, por sí solo, el establecimiento en España del prestador.

4. Los prestadores de servicios de la sociedad de la información establecidos en España estarán sujetos a las demás disposiciones del ordenamiento jurídico español que les sean de aplicación, en función de la actividad que desarrollen, con independencia de la utilización de medios electrónicos para su realización".

[984] Este podría ser el caso de un buscador -*Google* por ejemplo, por seguir con la misma ejemplificación a lo largo del trabajo- que pese a estar domiciliado en Estados Unidos, presta servicios en suelo español, con independencia de que la mayor parte de ellos provengan de su establecimiento y oficinas estadounidenses.

[985] Este precepto y el principio de extraterritorialidad que se desprende de él, parece avanzarse a lo que posteriormente dispondría el artículo 3 del GDPR que, sin necesidad de interpretaciones jurisprudenciales, dispone de forma expresa precisamente, la extensión de la legislación europea a empresas que, sin estar localizadas en suelo europeo, lleven a cabo en él cualquier operación de tratamiento de datos personales. De hecho, sobre la base de la LSSI , la AEPD mantuvo, en origen, la aplicación del derecho al olvido, en varias ocasiones.

[986] Artículo 15. Responsabilidad de los prestadores de servicios que realizan copia temporal de los datos solicitados por los usuarios.

"*Los prestadores de un servicio de intermediación que transmitan por una red de telecomunicaciones datos facilitados por un destinatario del servicio y, con la única finalidad de hacer más eficaz su transmisión ulterior a otros destinatarios que los soliciten, los almacenen en sus sistemas de forma automática, provisional y temporal, no serán responsables por el contenido de esos datos ni por la reproducción temporal de los mismos, si:*

alojamiento o almacenamiento de los mismos[987] o faciliten enlaces[988]. El concreto, merece destacar la fórmula "no tengan conocimiento efectivo" empleada simultáneamente en los

---

a) No modifican la información.

b) Permiten el acceso a ella sólo a los destinatarios que cumplan las condiciones impuestas a tal fin, por el destinatario cuya información se solicita.

c) Respetan las normas generalmente aceptadas y aplicadas por el sector para la actualización de la información.

d) No interfieren en la utilización lícita de tecnología generalmente aceptada y empleada por el sector, con el fin de obtener datos sobre la utilización de la información, y e) Retiran la información que hayan almacenado o hacen imposible el acceso a ella, en cuanto tengan conocimiento efectivo de:

1.º Que ha sido retirada del lugar de la red en que se encontraba inicialmente. 2.º Que se ha imposibilitado el acceso a ella, o 3.º Que un tribunal u órgano administrativo competente ha ordenado retirarla o impedir que se acceda a ella".

[987] Artículo 16. Responsabilidad de los prestadores de servicios de alojamiento o almacenamiento de datos.

1. "*Los prestadores de un servicio de intermediación consistente en albergar datos proporcionados por el destinatario de este servicio no serán responsables por la información almacenada a petición del destinatario, siempre que:*

a) No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

b) Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

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

2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control de su prestador".

[988] Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda.

1. "*Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:*

a) No tengan 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

b) Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

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

2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos".

artículos 16 y 17 de la LSSICE[989], que ha sido objeto de múltiples interpretaciones por los tribunales[990] en tanto que, según lo dispuesto en la normativa, permite exonerar de responsabilidad, respectivamente, a los prestadores de servicios de alojamiento o almacenamiento proporcionados por el destinatario de dicho servicio, o aquéllos que faciliten enlaces a contenidos o instrumentos de búsqueda respecto de contenidos ajenos, cuando no tengan conocimiento efectivo de que la actividad o la información almacenada o dirigida a sus usuarios es ilícita o lesiona bienes o derechos de un tercero susceptibles de indemnización; o si lo tienen, actúen con diligencia para suprimir dichos datos o hacer imposible su acceso a ellos.

Puede destacarse a tal efecto, la STS 559/2011, de 10 de febrero, que entiende que conocimiento efectivo es también "*aquel que se obtiene por el prestador del servicio a partir de hechos o circunstancias aptos para posibilitar, aunque mediatamente o por inferencias lógicas al alcance de cualquiera, una efectiva aprehensión de la realidad de que se trate*" (FJ 4º). De este modo, cuando los contenidos almacenados o enlazados mediante un buscador web, sean ilícitos de una forma patente y evidente por sí sola, no es precisa resolución judicial o administrativa que declare la ilicitud del contenido de las mismas, cosa que lleva a concluir la falta de la diligencia exigible al proveedor del servicio y, en consecuencia, su debida responsabilidad por los daños y perjuicios causados en el afectado[991].

---

[989] Señala BUSTO LAGO el carácter innovador del artículo 17 LSSICE que incorpora una regulación expresa de la responsabilidad civil de los prestadores de servicios que faciliten enlaces o contenidos o instrumentos de búsqueda, no exigida por la norma comunitaria que traspone. Cfr. BUSTO LAGO, J.M. "La responsabilidad civil de los prestadores de servicios de la Sociedad de la Información (ISPs)" en *Tratado de responsabilidad civil* (Reglero Campos y Busto Lago coord.), Aranzadi, Navarra, 2014, p. 601.

[990] Conforme a la LSSI, los buscadores de internet, en cuanto a servicios de intermediación que no ofertan contenidos propios sino ajenos, no tienen a priori responsabilidad por los contenidos que rastrean y difunden en Internet. El tratamiento automatizado que realizan los buscadores de Internet no genera responsabilidad *per se* hasta el momento en que la neutralidad que acompaña el automatismo cede al singular conocimiento, por lo que la responsabilidad del buscador emerge cuando concurren tres requisitos que deberán sucederse en el tiempo: en primer lugar, la ilicitud declarada de la información; en segundo lugar, su conocimiento efectivo y, por último, la falta de diligencia en su retirada. RALLO LLOMBARTE. "El derecho al olvido en el tiempo de Internet: la experiencia española" en *Percosi costituzionali. Libertà in Internet* (de Vergottini ed.), Jovene editore, nº 1, Napoli, 2014, pp. 179-180.

[991] Así lo reconoció también la STS 805/2013, de 7 de enero de 2014, la cual, mediante una interpretación amplia del artículo 16 LSSICE entendió que siempre que el prestador tenga medios para identificar y localizar al autor de unos contenidos que atenten contra los derechos fundamentales, debe adoptar las medidas necesarias al respecto y no esperar a que una resolución judicial o administrativa así lo verifique, pues ello viene exigido por el dinamismo propio del contexto de Internet.

Dicha cuestión también fue objeto de revisión por el TJUE en la STJUE de 23 de marzo de 2010[992] el cual dispuso, en relación a la interpretación del artículo 14 de la Directiva 2000/31/CE que se corresponde con dicho aspecto, "*el artículo 14 de la Directiva 2000/31 debe interpretarse en el sentido de que la norma que establece se aplica al prestador de un servicio de referenciación en Internet cuando no desempeñe un papel activo que pueda darle conocimiento o control de los datos almacenados. Si no desempeña un papel de este tipo, no puede considerarse responsable al prestador de los datos almacenados a petición del anunciante, a menos que, tras llegar a su conocimiento la ilicitud de estos datos o de las actividades del anunciante, no actúe con prontitud para retirar los datos o hacer que el acceso a ellos sea imposible*" (punto 120). En resumidas cuentas, para quedar excluido de la responsabilidad reconocida en la Directiva de comercio electrónico, la actividad del prestador de servicios debe ser puramente técnica, automática y pasiva, de forma que el prestador "*no tenga conocimiento ni control de la información transmitida o almacenada*" (punto 113).

Sin embargo, en el asunto del caso *Google*, el TJUE realiza una interpretación ciertamente clarificadora en este ámbito, tal y como se ha comentado en páginas anteriores, al considerar que los motores de búsqueda llevan a cabo tratamiento de datos y, en consecuencia, son responsables del mismo, "*el artículo 2, letras b) y d), de la Directiva 95/46 debe interpretarse en el sentido de que, por un lado, la actividad de un motor de búsqueda, que 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, debe calificarse de «tratamiento de datos personales», en el sentido de dicho artículo 2, letra b), 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 mencionado artículo 2, letra d)*" (punto 41). Incluso, estima el Tribunal, los buscadores llevan a cabo tratamiento de datos cuando

[992] STJUE (Gran Sala), de 23 de marzo de 2010, *Google France SARL y Google Inc. v. Louis Vuitton Malletier SA,* Asuntos acumulados C-236/08 y C-238/08.

meramente "*se refieran únicamente a información ya publicada tal cual en los medios de comunicación*" (punto 30).

La postura del Tribunal acerca de la responsabilidad de los motores de búsqueda, que afirma que éstos llevan a cabo tratamiento de datos personales incluso cuando se limitan a ser meros proveedores de contenido, desvirtúa el argumento de algunas pretensiones que, amparándose en la Directiva 2000/31/CE y la LSSICE e interpretando que los motores de búsqueda carecían de "conocimiento efectivo" sobre la información que ponían a disposición de los usuarios, eximían a los buscadores de toda responsabilidad. De este modo, se dispone el sometimiento de los motores de búsqueda a la legislación especial en materia de protección de datos, quedando sujetos a responsabilidad cuando dicho tratamiento sea contrario a la ley o cause daños y perjuicios.

Resulta curioso, no obstante, que la sentencia del TJUE en el *caso Google*[993], omita toda referencia a la Directiva 2000/31/CE sobre comercio electrónico, de hecho la propia Audiencia Nacional, cuando elevó las mencionadas cuestiones prejudiciales al TJUE que dieron lugar a dicha resolución, ni siquiera inquirió sobre la responsabilidad de los buscadores, en tanto que intermediarios de la sociedad de la información, en relación con lo dispuesto en la Directiva 2000/31/CE[994]. Dicha STJUE se limita a examinar la actividad de los buscadores en relación con la Directiva 95/46/CE de protección de datos –actualmente derogada por el GDPR- que, por ser anterior a la Directiva 2000/31/CE, no contiene mención alguna a los servicios de la sociedad de la información[995].

[993] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

[994] Sin embargo el abogado defensor de *Google Spain S.L.* sí que se refirió a esta cuestión a posteriori, interpretando que la STJUE del *caso Google* no implicaba la retirada de datos ni la imposibilidad de acceder a ellos en el futuro, pues eso supondría un deber general de supervisión, prohibido por el artículo 15 de la Directiva 2000/31/CE de comercio electrónico, sino que implicaba únicamente la reordenación de los resultados cuando la búsqueda se lleve a cabo específicamente introduciendo el nombre y los apellidos del interesado. Criterio, sin embargo, creemos equivocado tal y como ya se ha defendido en páginas anteriores.

[995] El vigente Reglamento europeo de protección de datos, por el contrario, sí que incorpora una breve mención a la Directiva 2000/31/CE en su considerando 21º y su artículo 2.4.

No obstante, por lo que respecta a la legislación doméstica, como se viene comentando en este apartado, la LSSICE traspuso al ordenamiento español los postulados de la Directiva 2000/31/CE, y llamativamente, sus preceptos fueron empleados por el Tribunal Supremo, como en su Sentencia de 4 de marzo de 2013[996], para exonerar de responsabilidad a los motores de búsqueda respecto de un supuesto de hecho en el que el interesado alegaba una vulneración del derecho al honor causada por las intromisiones ilegítimas de un buscador en su privacidad, frente a lo cuál sus pretensiones fueron rechazadas al entender el TS que los motores de búsqueda carecían de conocimiento efectivo sobre el contenido de los enlaces que proporcionan a los usuarios.

En cualquier caso, la STJUE del caso *Google*, disruptiva en materia de derecho al olvido, dispuso que los motores de búsqueda cuando realizan una actividad consistente en localizar información publicada o incluida en Internet por terceros relativa a personas físicas, indexarla de manera automática, almacenarla temporalmente y, por último, ponerla a disposición de los internautas según un orden de preferencia, efectúa un tratamiento de datos personales sometido a la normativa de protección de datos y, en consecuencia, deviene responsable del mismo (FJ 1º) con independencia de que el motor de búsqueda sea un intermediario de la sociedad de la información conforme a la Directiva 2000/31/CE. Del mismo modo, teniendo en cuenta la doctrina del TJUE, se extiende la responsabilidad de los motores de búsqueda en el tratamiento de datos, quienes podrían pasar a considerarse responsables en los términos del GDPR[997].

---

[996] "*Esta Sala coincide con la valoración fáctica y jurídica de la sentencia recurrida, sin que ninguna vulneración del artículo 17 de la LSSICE se haya producido, habiéndose realizado una aplicación correcta del mismo al excluir de responsabilidad a la entidad demandada por falta de conocimiento efectivo de la falsedad de la información*" STS 2245/2013, de 4 de marzo de 2013, FJ 5º.

[997] Artículo 4. 7): "*«responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros*".

En conclusión, puesto a que la aplicación de la legislación específica en materia de protección de datos[998] comprendería la responsabilidad de los motores de búsqueda en el tratamiento de los datos, las responsabilidades que, en su caso, se deriven de ello, se dirimirán conforme a la misma, no siendo aplicable lo dispuesto en la Directiva 2000/31/CE[999] cuyo objeto, principalmente, quedaría limitado a los supuestos de tratamiento ilícito de datos personales[1000]. Por el contrario, el derecho al olvido, dado su encaje en el campo de la protección de datos, comporta la eliminación de información lícita y veraz como regla general[1001].

11.4 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 último, y teniendo en cuenta la intrínseca relación existente entre el derecho al olvido y a la protección de datos personales y el derecho al honor, intimidad y a la propia

---

[998] Así lo dispone la propia Directiva 2000/31/CE que remite a la anterior 95/46/CE aquéllos aspectos relativos a la protección de datos "*La protección de las personas con respecto al tratamiento de datos de carácter personal se rige únicamente por la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (19) y la Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones (20), que son enteramente aplicables a los servicios de la sociedad de la información. Dichas Directivas establecen ya un marco jurídico comunitario en materia de datos personales y, por tanto, no es necesario abordar este aspecto en la presente Directiva para garantizar el correcto funcionamiento del mercado interior, en particular la libre circulación de datos personales entre Estados miembros. La aplicación y ejecución de la presente Directiva debe respetar plenamente los principios relativos a la protección de datos personales, en particular en lo que se refiere a las comunicaciones comerciales no solicitadas y a la responsabilidad de los intermediarios, la presente Directiva no puede evitar el uso anónimo de redes abiertas como Internet*" (considerando 14º), concibiéndose así la primera, como una norma general acerca de la Sociedad de la Información que integra aquellos aspectos no contemplados directamente por la legislación de protección de datos.

[999] ÁLVAREZ CARO se muestra contraria a esta perspectiva, al entender que resulta excesivo obligar a los proveedores de servicios de motores de búsqueda en Internet con las obligaciones del responsable del tratamiento, cuestionando incluso el fallo del TJUE en el *caso Google* en relación a esta cuestión. Añade la autora que ello supondría una ineficacia para el derecho al olvido, "descargar toda la ira en el buscador *Google* no es la mejor opción o, al menos, la más eficaz". Cfr. *Derecho al olvido en Internet: el nuevo paradigma de la privacidad en la era digital*, Reus, Madrid, 2015, pp. 116-117.

[1000] Esta argumentación fue la que empleó el Abogado General, el Sr. Nillo Jääskinen ante el TJUE en el *caso Google*, disponiendo que los procedimientos de detección y retirada contemplados a tenor de la Directiva 2000/31/CE, están relacionados con los contenidos ilegales, mientras que en el supuesto de hecho controvertido, la solicitud de supresión de los contenidos versaba sobre una información legítima y legal.

[1001] No obstante, ello puede resultar un tanto contradictorio con lo dispuesto en el artículo 2.4 del GDPR cuyo tenor literal, como mínimo, induce a la confusión: "*el presente Reglamento se entenderá sin perjuicio de la aplicación de la Directiva 2000/31/CE, en particular sus normas relativas a la responsabilidad de los prestadores de servicios intermediarios establecidas en sus artículos 12 a 15*".

imagen que, como se ha evidenciado en este mismo Capítulo, estos últimos tienen una incidencia notable en la configuración del objeto jurídico del derecho al olvido, por lo que resulta procedente hacer una mención breve a la legislación especial en dicha materia[1002].

Esta norma es importante a los efectos del examen del derecho al olvido en tanto que, en ocasiones, una vulneración del derecho de supresión puede conllevar, asimismo, una violación del derecho al honor, a la intimidad o a la propia imagen, en función de las circunstancias del caso concreto. Mientras que las consecuencias de la vulneración del derecho al olvido ya se han expuesto en páginas anteriores, cuando con ello se produzca una vulneración de alguno de los derechos recogidos en la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al honor, a la Intimidad Personal y Familiar y a la Propia Imagen (LOPDH, en adelante) los daños y perjuicios que de ello se deriven, se dirimirán por lo dispuesto en esta legislación especial[1003].

Someramente, procede recordar aquí como la Constitución española ha configurado los derechos objeto de la LOPDH, no sólo como derechos autónomos tal y como expresa el artículo 18 CE, epicentro de su regulación, sino también como límites de otros derechos fundamentales, como son la libertad de expresión e información recogidas en el artículo 20 CE. Ello comporta necesariamente una modulación del alcance de su protección en función de las circunstancias concretas del supuesto de hecho del que se trate lo que, como ya se ha visto, recurrentemente exige un juicio de ponderación respecto de los intereses jurídicos que, en el caso concreto, entren en colisión.

[1002] YZQUIERDO TOLSADA, sin embargo sostiene que la Ley Orgánica 1/1982 no constituye en puridad una ley especial en materia de responsabilidad civil en tanto que, frente a una intromisión ilegítima, ésta prevé, no sólo la posibilidad de indemnizar el daño moral, sino toda una serie de respuestas jurídicas, entre las que se encuentran las medidas cautelares, de cesación, de abstención… que, sin ser estrictamente objeto del Derecho de daños, guardan una estrecha relación con dicha materia. Cfr. "Daños a los derechos de la personalidad (Honor, Intimidad y Propia imagen)" en *Tratado de responsabilidad civil* (Reglero Campos y Busto Lago coord.), Aranzadi, Navarra, 2014, pp. 1366 y 1367.

[1003] Al igual que la prohibición de censura previa no excluye la eventual responsabilidad por las opiniones y noticias difundidas, pues el control a posteriori de publicaciones y grabaciones está reconocido constitucionalmente, pudiendo incluso retirar de la circulación contenidos difundidos que lesionen ilegítimamente derechos de terceros, en Internet, si bien no se puede controlar *a priori* lo que cada uno diga o comparta en la Red, ello no excluye que se esté sujeto al cumplimiento de los derechos y libertades reconocidos en el ordenamiento jurídico, ni implica que no deba responderse extracontractualmente, de los daños y perjuicios ocasionados así como, en su caso, penalmente.

Así, en la propia Exposición de Motivos de la LO 1/1982 se niega el carácter ilimitado de dichos derechos "*Además de la delimitación que pueda resultar de las leyes, se estima razonable admitir que en lo no previsto por ellas la esfera del honor, de la intimidad personal y familiar y del uso de la imagen esté determinada de manera decisiva por las ideas que prevalezcan en cada momento en la Sociedad y por el propio concepto que cada persona según sus actos propios mantenga al respecto y determine sus pautas de comportamiento. De esta forma la cuestión se resuelve en la ley en términos que permiten al juzgador la prudente determinación de la esfera de protección en función de datos variables según los tiempos y las personas*".

Respecto del contenido de la LOPDH, resulta ciertamente breve pues ésta viene configurada exclusivamente por nueve artículos, motivo que le ha valido numerosas críticas entre la doctrina[1004], y que ha requerido de abundante jurisprudencia del Tribunal Supremo para la configuración y el desarrollo de los preceptos que contiene. Someramente procede mencionar que dicha norma realiza una reglamentación conjunta de ambos derechos -lo cual resulta, cuanto menos sorprendente, dadas las significativas divergencias entre dichas figuras- cosa que ha ocasionado una regulación deficiente, precisamente, del derecho a la intimidad[1005] así como numerosas lagunas entorno a sus limitaciones con las libertades expresivas e informativas[1006].

En definitiva, como sostiene FAYOS GARDÓ, la LOPDH "omite prácticamente algún derecho, no habla para nada de la libertad de expresión, no tiene en cuenta la jurisprudencia

[1004] Destaca entre ellas, las críticas vertidas por SALVADOR CODERCH que llegó incluso a calificar esta legislación como una "ley muy mala". Cfr. *¿Qué es difamar? Libelo contra la Ley del Libelo*, ob. cit., p. 19.

[1005] Este extremo llevó a HERRERO TEJEDOR a reivindicar la inconstitucionalidad de dicha norma, al entender que el legislador había omitido la regulación de la figura de la intimidad casi por completo, pese a ser ésta un presupuesto indiscutible que motivó la creación de dicha Ley Orgánica. Cfr. *Honor, Intimidad y Propia Imagen*, Colex, Madrid, 1994, p. 202.

[1006] Al respecto, afirma YZQUIERDO TOLSADA que el legislador no se interesó lo más mínimo por los límites entre las libertades constitucionales de expresión y de información y los derechos al honor, intimidad e imagen, ni tampoco las implicaciones penales y procesales que de ello se derivaban. Cfr. "Daños a los derechos de la personalidad (Honor, Intimidad y Propia imagen)", ob. cit., p. 1366.

anterior, ni los criterios de derecho comparado, ni diferencia bien los tres derechos" [1007]. Sin embargo, con sus virtudes y sus defectos[1008], ésta es la legislación a la que debe acudirse para dirimirse las responsabilidades civiles que se deriven de la vulneración de tales derechos, como así establece su artículo 1 "*El derecho fundamental al honor, a la intimidad personal y familiar y a la propia imagen, garantizado en el artículo dieciocho de la Constitución, será protegido civilmente frente a todo género de intromisiones ilegítimas, de acuerdo con lo establecido en la presente Ley Orgánica*".

Dichos derechos, son configurados en la legislación especial como auténticos derechos subjetivos, en tanto que se trata de derechos fundamentales y garantizan un estatus jurídico, la libertad en un ámbito de la existencia, al mismo tiempo en que son "*elementos esenciales del ordenamiento objetivo de la comunidad",* propios del Estado social y democrático de Derecho[1009]. Asimismo, en cuanto a derechos de la personalidad, se les atribuye el carácter de derechos irrenunciables, inalienables e imprescriptibles (artículo 1.3).

El artículo 7 de la LOPDH, establece las conductas que tienen la consideración de intromisiones ilegítimas en los derechos fundamentales al honor, la intimidad personal y familiar y el derecho a la imagen:

> *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.*

[1007] Cfr. FAYOS GARDÓ. "Los derechos a la intimidad y a la propia imagen: un análisis de la jurisprudencial española, británica y del Tribunal Europeo de Derechos Humanos" en *InDret*, nº 4, 2007.

[1008] Muchos de ellos fueron subsanados por sucesivas reformas, la última de ellas acometida en 2010, mediante la Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

[1009] STC 25/1981, de 14 de julio.

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 octavo, dos.

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.

Sin embargo, no se trata de un *numerus clausus* como reiteradamente ha dispuesto la jurisprudencia del Tribunal Supremo[1010]. De hecho, por lo que respecta al derecho al olvido, éste no parece subsumible en ninguno de los apartados regulados expresamente en dicho

[1010] Por todas, STS de 28 de octubre de 1986 (RJ 1986, 6015).

precepto, pese a que mantenga ciertos paralelismos con la figura de la difamación[1011], pero su falta de regulación no puede ni debe impedir una reclamación fundada[1012].

Por su parte, el artículo noveno, regula las vías a través de las cuales los afectados podrán recabar la tutela judicial frente a las intromisiones ilegítimas en sus derechos al honor, intimidad o propia imagen, así como las medidas que podrán adoptarse a tenor de su reclamación para poner fin a la intromisión ilegítima de que se trate. Entre éstas, se encuentra el restablecimiento del perjudicado en el pleno disfrute de sus derechos, el cese inmediato de la intromisión y la reposición al estado anterior, así como el derecho de réplica y la acción para la difusión de la sentencia condenatoria en el caso de vulneración del derecho al honor, la indemnización de los daños y perjuicios causados y la apropiación por el perjudicado del lucro obtenido con la intromisión ilegítima en sus derechos.

Resulta destacable como, a la hora de determinar las indemnizaciones por daños y perjuicios, esta norma presupone siempre la existencia de perjuicio ante una intromisión ilegítima[1013]. Asimismo, contempla expresamente la inclusión del daño moral en la compensación pecuniaria -como una suerte de presunción- el cual se valorará atendiendo a las circunstancias del caso y a la gravedad del daño[1014], para lo que se tendrá en consideración el alcance de la difusión y la audiencia del medio a través del que se haya producido (artículo

[1011] Recordar que también constituyen difamación las informaciones veraces si éstas se acompañan de datos que afectan a la intimidad, aunque no constituyan insultos propiamente. A diferencia del derecho al honor, la *exceptio veritatis* no puede excluir la intromisión ilegítima de que se trate en la esfera de la privacidad, como estableció la STS 781/1995, de 26 de julio.

[1012] Cfr. YZQUIERDO TOLSADA. "Daños a los derechos de la personalidad (Honor, Intimidad y Propia imagen)", ob. cit., p. 1418.

[1013] Respecto de esta cuestión, la jurisprudencia del Alto Tribunal ha declarado numerosas veces que las indemnizaciones de carácter meramente simbólico no son admisibles: "*no es admisible que se fijen indemnizaciones de carácter simbólico, pues al tratarse de derechos protegidos por la CE como derechos reales y efectivos, con la indemnización solicitada se convierte la garantía jurisdiccional en un acto meramente ritual o simbólico incompatible con el contenido de los artículos 9.1, 1.1 y 53.2 CE y la correlativa exigencia de una reparación acorde con el relieve de los valores e intereses en juego*" , STS 696/2014, de 4 de diciembre, FJ 2º.

[1014] No obstante, pese a la presunción *iuris et de iure* de existencia de perjuicio indemnizable, el hecho de que la valoración del daño moral no pueda obtenerse de una prueba objetiva no excusa ni imposibilita legalmente a los tribunales para fijar su cuantificación, a cuyo efecto ha de tenerse en cuenta y ponderar las circunstancias concurrentes en casa caso, STS 312/2014, de 5 de junio.

9.3)[1015] que, en el caso de Internet, es enorme y potencialmente incluye a todos aquellos que tengan acceso a la Red.

Pese a que, en el contexto en el que se sitúa el derecho al olvido, dadas las características intrínsecas a su naturaleza y aparejadas al medio en el que se produce, la determinación de los daños morales pueda resultar harto difícil, incluso en ocasiones, llegando a ser imposible una valoración directa y exacta, ello no puede servir de pretexto para negar su indemnizabilidad. Como señala MARTÍN I CASALS "la tesis de la inestimabilidad no puede convertirse en una coartada para subvencionar la producción de daños, no hay ninguna buena razón para proponer un desarrollo judicial de nuestro Derecho de daños que no sólo no estimule a reducir razonablemente el sufrimiento humano sino que, negando toda indemnización, contribuya a incrementarlo. Semejante perversión es ajena a los fundamentos de nuestro sistema jurídico civil" [1016].

Esta misma postura es la que parece haber adoptado la jurisprudencia civil más reciente que, en relación con nuestro campo de estudio, ha resulto conceder indemnización por daños y perjuicios a los sujetos afectados por la vulneración del derecho a la protección de datos cuando además, con dicha conducta, se haya producido una intromisión ilegítima en el derecho al honor. Como ejemplo, la reciente sentencia de la Sala de lo Civil del Tribunal Supremo de 21 de junio[1017], la cual ha estimado que la inclusión del demandante en un fichero de morosos,

[1015] Respecto de dicha cuestión, SALVADOR CODERCH examina el criterio adoptado por la LOPDH frente al de la tradición jurídica anglosajona, lo que puede resultar clarificador teniendo en cuenta la perspectiva comparada de la presente disertación. Afirma así el autor que "el *common law* consideró tradicionalmente que la difamación escrita (*Libel*) daba lugar a acción sin necesidad de probar daños, pero que sólo las formas más graves de difamación oral (*Slander*) eran tratadas de igual manera, precisándose en los demás casos de la prueba de perjuicio ocasionado. El criterio del legislador español parece correcto pues no hay razón de peso para diferenciar tipos de difamación según la *forma* en que ésta se produzca: Tal y como se dijo en el primer epígrafe del apartado III, es el grado de *permanencia* y de difusión lo que ha de tenerse en cuenta, y no para apreciar la existencia o no de difamación, sino para determinar la cuantía del daño. Detenerse en la *forma* sería superficial. Del viejo derecho angloamericano cabe con todo retener su fondo de verdad: *scripta manent*, los escritos permanecen y por eso hacen normalmente más daño que las habladurías". Cfr. *¿Qué es difamar? Libelo contra la Ley del Libelo*, ob. cit., p. 19.

[1016] Cfr. MARTÍN I CASALS. "Indemnización de daños y otras medidas judiciales por intromisión ilegítima contra el derecho al honor" en *El mercado de las ideas* (Salvador Coderch dir.), Centro de Estudios Constitucionales, Madrid, 1990, p. 386.

[1017] STS 388/2018.

comporta una intromisión en el derecho al honor y, en consecuencia, da lugar a una indemnización por daños morales.

El supuesto en concreto, se trata de una persona que fue incluida durante un año en un fichero de morosos al que accedieron distintas entidades bancarias y de crédito, lo que motivó la denegación de un préstamo a la actora así como rebajó su índice de solvencia. El recurso de casación se interpone ante el Alto Tribunal, precisamente, en base a una supuesta infracción del artículo 9.3 de la LOPDH, en relación con el artículo 19 de la LOPD, concretamente, por la vulneración de las pautas que deben tenerse en cuenta para la valoración del daño moral. El Tribunal Supremo dispone, en primer lugar, que la inclusión de una persona en un registro de morosos sin cumplirse los requisitos establecidos en la LOPD, provoca una afectación a la dignidad, tanto en su aspecto interno como en su aspecto objetivo, por lo que resulta ciertamente indemnizable.

En segundo lugar, recuerda su doctrina en base a la cual, la inclusión ilegítima de una persona en un fichero de morosos supone una intromisión ilegítima en su derecho al honor de una trascendencia considerable, con independencia de que la cuantía supuestamente adeudada sea de pequeña entidad.

En tercer lugar, afirma el TS que la inclusión en dicho fichero no responde al principio de calidad de los datos según el cuál éstos deben der "exactos, adecuados, pertinentes y proporcionados a los fines para los que han sido recogidos y tratados", resolviendo que la inclusión del afectado en dicho registro le ha impedido acceder a créditos y a servicios. En consecuencia, el Tribunal sentencia estimar parcialmente el recurso de casación y conceder al perjudicado una indemnización por daños morales. En cuanto al *quantum* de la indemnización, si bien en primera instancia ésta fue fijada en 10.000€, posteriormente en apelación fue disminuida a 2.000€ y, en casación, ha sido establecida en 6.000€ por el Tribunal Supremo.

12. Cuestiones accesorias

En el siguiente apartado se va a proceder a distinguir el derecho al olvido con otras categorías jurídicas afines con las que ha mantenido o mantiene un núcleo común en cuanto a los bienes jurídicos protegidos o los mecanismos de garantía que integra.

12.1. El derecho de cancelación

El derecho de cancelación, se regula en la Ley Orgánica de Protección de Datos de Carácter personal. comentada páginas atrás, de manera conjunta con el derecho de rectificación:

> *Artículo 16. Derecho de rectificación y cancelación.*
>
> *1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.*
>
> *2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.*
>
> *3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas.*
>
> *Cumplido el citado plazo deberá procederse a la supresión.*
>
> *4. Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.*

5. *Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado*.

El artículo 5 RLOPD define el derecho de cancelación como el "*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*".

Poniendo los preceptos anteriores en relación con el artículo 4.5 LOPD, podríamos decir que el derecho de cancelación, en nuestra legislación, tiene lugar cuando determinados datos personales "*hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados*". De este modo, se impide que determinados datos personales sean conservados para que no se permita con ello la identificación del interesado, pasado un periodo de tiempo prudencial para llevar a cabo los fines para los cuales dichos datos fueron recabados o registrados, siempre y cuando no se incurra en alguna de las excepciones previstas[1018].

Este derecho de cancelación, se integra dentro de lo que se ha venido llamando los Derechos ARCO (esto es, acceso, rectificación, cancelación y oposición) cuya finalidad es garantizar el control de los datos personales de los interesados y cuya regulación se inserta dentro de la LOPD, comentada páginas atrás. Con este mismo objetivo se dicta el Reglamento europeo de protección de datos, cuyo articulado, por ser de directa aplicación en los Estados miembro, complementa la legislación anterior y la suple en aquéllos aspectos en que ambas sean incompatibles.

[1018] Atendidos los valores históricos, estadísticos o científicos puede permitirse, de acuerdo con la legislación específica, el mantenimiento íntegro de determinados datos.

En el marco europeo, si bien el derecho de rectificación se comprende en la misma sección 3 que el derecho de supresión, el GDPR hace una completa omisión del derecho de cancelación que, según se entiende, ha sido reemplazado por el nuevo derecho de supresión (artículo 17).

Como ya se ha visto en páginas anteriores, el GDPR amplía las garantías y prerrogativas de los interesados, incorporando nuevos derechos a los clásicos ARCO como el derecho a la limitación del tratamiento (artículo 18), al olvido o a la portabilidad de los datos (artículo 20), creando un marco más proteccionista para con la privacidad de los individuos.

El derecho de cancelación y el derecho al olvido tienen un contenido muy similar, de hecho, parece que, bajo la fórmula "derecho de supresión" se ha modernizado la figura clásica de la cancelación, adaptándola a las circunstancias actuales que exige el contexto del *Big data* y la interacción de Internet, sustituyendo mediante el denominado "derecho al olvido" a su antecesor derecho de cancelación. Eso explicaría la ausencia de toda mención al derecho de cancelación tanto en el vigente GDPR como en el Proyecto de Ley Orgánica de Protección de Datos –actualmente en tramitación parlamentaria- que vendría sustituido por el nuevo derecho de supresión.

Por consiguiente, en cuanto a su contenido, el objetivo de ambos derechos no difiere en absoluto, únicamente se produce una actualización del contexto y sus garantías mediante el nuevo derecho al olvido. Parece pues que, con el empleo de una denominación distinta, se ha querido resaltar la novedad y las virtudes de una figura jurídica que, sin embargo ya preexistía en nuestro entorno jurídico pero que, dadas las circunstancias del medio en el que debía de ejercitarse, había perdido cierta virtualidad.

Aunque, debemos esperar a la entrada en vigor de la nueva ley de protección de datos que derogará la vigente LOPD para poder constatar si, efectivamente, ha llegado el fin de la era de los derechos ARCO (por quedarse éstos reducidos a un ámbito mínimo de protección, entiéndase), en la actualidad se produce la peculiaridad de que ambos derechos, el de cancelación y el de supresión, conviven mutuamente en nuestro ordenamiento jurídico y son

susceptibles de aplicación. Teniendo ello en cuenta, y pese a la previsible fusión de ambas figuras, pueden distinguirse algunas diferencias.

En primer lugar, mientras que el derecho de cancelación, para hacerse efectivo, debe ejercitarse por el titular de los datos personales frente al responsable del fichero de la entidad que se trate, mediante un escrito dirigido al mismo, el derecho al olvido, por el contrario, puede ejercitarse indistintamente, tanto contra el responsable o gestor de una página o contenido web, como frente a un motor de búsqueda que indexe dicha información. Dicha pretensión, además, puede hacerse online (empleando el formulario específico que haya previsto tal responsable del tratamiento, o mediante cualquier escrito que acredite la información que se desea suprimir, las URL que la contemplen, y los caracteres empleados para la búsqueda, en caso de que se trate de un buscador web) o por escrito, e incluso cuando dicha empresa no tenga el domicilio social sito en España pero la actividad se esté produciendo en territorio español, ya sea por ella misma o por otra entidad de su mismo grupo empresarial).

En segundo lugar, el derecho de cancelación es personalísimo de forma que sólo puede ejercitarse por el afectado (art. 23 RLOPD) mientras que, en cierto modo podría decirse que el derecho al olvido puede ejercitarse por una entidad, organización o asociación sin ánimo de lucro que haya sido correctamente constituida en base al derecho doméstico, cuyos objetivos estatutarios sean de interés público y actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, pues puede presentar en nombre del interesado una reclamación, conforme al artículo 80 GDPR.

Por último, una vez ejercitado el derecho de cancelación, éste dará lugar a que se supriman los datos que resulten inadecuados o excesivos (artículo 31 RLOPD) o por causas contractuales o en cumplimiento de una obligación legal de confidencialidad (artículo 33 RLOPD), mientras que el derecho de supresión es prácticamente la regla general, negándose su eficacia únicamente en aquéllos casos en los que prevalga el derecho a la libertad de expresión e información, sea necesario para el cumplimiento de una obligación legal o por razones de interés público en el ámbito de la salud pública, o por fines de archivo o de investigación científica o histórica o fines estadísticos así como para la formulación, el ejercicio o la defensa

de reclamaciones. Los supuestos para los que se prevé su ejecución son tantos y tan amplios[1019] que, siempre que no se incurra en una de las excepciones anteriores, se procederá al borrado de la información personal, siendo indiferente que los datos personales sean adecuados, verdaderos o inciertos, numerosos o poco cuantiosos.

12.2. Derecho de oposición

Podría también señalarse la relación íntima del derecho al olvido con el derecho clásico de oposición, en tanto que éste último permite a su titular oponerse a que se lleve a cabo un determinado tratamiento de sus datos de carácter personal así como a solicitar que se cese en éste cuando concurra alguno de los siguientes supuestos: a) que no sea necesario su consentimiento para el tratamiento, en relación con un motivo legítimo y fundado, relativo a su concreta situación personal que lo justifique; b) que se trate de ficheros que tengan por finalidad la realización de actividades publicitarias y comerciales; o c) que el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal[1020].

[1019] Artículo 17.1 GDPR: "*El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando 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 de otro modo;

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".

[1020] Artículo 34, RLOPD.

De hecho, en el procedimiento ejercitado ante la Audiencia Nacional que dio lugar a la relativa cuestión prejudicial y, en consecuencia, se dictó la STJUE de 13 de mayo de 2014[1021], del ya comentado *caso Google*, el interesado ejercitó conjuntamente el derecho de oposición y el derecho de cancelación, para solicitar el borrado de sus datos personales en Internet, principalmente frente a los motores de búsqueda, cosa que, como ya se sabe, se concedió en base al derecho al olvido, cuya creación jurisprudencial tiene origen en dicho pronunciamiento.

Sin embargo, puede señalarse como rasgo diferenciador entre el derecho de oposición y el derecho al olvido, principalmente la extensión de su contenido pues, a diferencia del derecho de supresión, el derecho de oposición sólo se manifiesta como la potestad del sujeto de impedir una determinada finalidad del tratamiento de sus datos personales y no su borrado o desaparición total. Además, los supuestos por los que puede ejercitarse el derecho de oposición están tasados legalmente y otorgan al sujeto afectado la carga de la prueba acerca de la concurrencia de los requisitos por los que puede oponerse a un determinado tratamiento o retirar su consentimiento prestado en el pasado, para una finalidad concreta de tratamiento. Ello no ocurre en el derecho al olvido donde el sujeto que lo ejercite no debe probar de forma alguna que la permanencia de dichos datos le supone un daño o un perjuicio o la vulneración de cualquier derecho fundamental, bastando con demostrar que dicha información personal no es adecuado, correspondiéndole al responsable del tratamiento demostrar que se dan las circunstancias excepcionales para el mantenimiento de los mismos.

Ello está directamente relacionado con el principio del consentimiento del afectado, cuya importancia pivota sobre los tradicionales derechos ARCO, que se construyen en base a la teoría del consentimiento y su papel fundamental en el derecho a la protección de datos personales, mientras que en el marco actual éste ha dejado de tener tanta importancia, dada la interacción del tratamiento automatizado de decisiones así como la proliferación de algoritmos. Así, en la configuración del derecho al olvido, éste reside en otros presupuestos, como se puede observar en la extensión de la responsabilidad sobre los responsables y los encargados del

[1021] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

tratamiento así como en la introducción de elementos novedosos como el principio de privacidad desde el diseño.

A diferencia del derecho de cancelación del que no hace mención alguna el GDPR, el derecho de oposición sí que se ha mantenido y se contempla expresamente en su artículo 21:

> 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.

De este modo, parece más acertado vincular el derecho al olvido al clásico derecho de cancelación, además de por las razones anteriormente esgrimidas, porque ambos tienen por objeto poner fin a un determinado tratamiento en su conjunto, su cese o bloqueo, pese a que el derecho al olvido va un paso más allá y se configura como una extensión del derecho de cancelación, posibilitando el borrado total de dicha información personal.

12.3. El derecho de rectificación

Brevemente, puede definirse el derecho de rectificación como aquél que permite a su titular solicitar la corrección una información relativa a su persona, difundida a través de un medio de comunicación social cuando ésta no sea verídica y su divulgación le resulte perjudicial[1022].

En el ordenamiento jurídico español su regulación específica se encuentra en la Ley Orgánica 2/1984, de 26 de marzo, sobre el Derecho de Rectificación (LODR, a partir de ahora) la cual, en su artículo 1 dispone el objeto de su regulación: "*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. Podrán ejercitar el derecho de rectificación el perjudicado aludido o su representante y, si hubiese fallecido aquél, sus herederos o los representantes de éstos*".

Esta definición, enmarcada en un contexto social muy concreto, ha quedado obsoleta en la actualidad puesto que, como a continuación se expondrá, su articulado poco parece adaptarse al nuevo contexto jurídico que ha supuesto la irrupción de Internet.

Así, por ejemplo, los plazos previstos de siete días para la remisión del escrito y tres días para la publicación de la rectificación por el medio no parecen razonables ni pueden ser

[1022] El Tribunal Constitucional definió dicho derecho como "*la facultad otorgada a toda persona, natural o jurídica, de rectificar la información difundida, por cualquier medio de comunicación social, de hechos que le aludan, que considere inexactos y cuya divulgación pueda causarle perjuicio*". STC 168/1988, de 22 de diciembre, FJ 6º.

efectivos si tenemos en cuenta la fugacidad con la que aparecen las informaciones en Internet así como la instantaneidad de las comunicaciones actuales. De este modo, en la práctica, no se consigue equiparar los efectos y las condiciones del sujeto afectado y el medio de comunicación en tanto que difícilmente consigue revertir el impacto previo de la información falsa o inexacta de la que se trate, en relación con la rectificación que en su caso pueda llegar a hacerse.

De otra parte, en cuanto a la necesidad de probar el perjuicio ocasionado, ello resulta muy gravoso en el contexto de Internet, en el que la información está en cambio constante, siendo en muchas ocasiones anónima. Asimismo, la naturaleza propia de este medio dificulta enormemente la acción procesal en tanto que una noticia puede aparecer en un mismo medio en distintas posiciones y formatos, cambiando con el tiempo, y estando en muchos casos personalizada de acuerdo con las preferencias de cada usuario, lo que dificulta enormemente discernir su alcance real.

Claramente el derecho de rectificación se concibió básicamente para la prensa escrita como puede observarse en la necesidad de ejercitar el derecho de rectificación mediante "un escrito" cosa que hoy en día parece desfasado teniendo en cuenta el alcance de Internet, el cual no cuenta con un competidor directo pues en él se integran los medios de comunicación tradicionales, ampliando su difusión exponencialmente. Internet, además, tiene unas características propias como son la inmediatez y la continua mutabilidad, que requieren de nuevos instrumentos jurídicos para ejercitar el derecho de rectificación, más acordes con su naturaleza.

Por otro lado, el derecho de rectificación tiene unas raíces íntimamente relacionadas con el derecho al honor del artículo 18 CE[1023], así como con el derecho a la libertad de expresión e información del artículo 20.4 CE en tanto que en éstas últimas encuentra sus límites de

[1023] LIZARRAGA VIZCARRA. *El Derecho de Rectificación*, Aranzadi, Navarra, 2005, p. 20.

actuación y de ello se derivan ocasionalmente conflictos entre bienes jurídicos[1024], que exigen un ejercicio de ponderación por el Juzgador[1025].

Ello implica que dicha figura, siempre y cuando se produzca una vulneración del derecho al honor, ostentará la tutela civil ante los tribunales ordinarios conforme a lo dispuesto en la Ley Orgánica 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen; así como el procedimiento previsto en el artículo 53.2 CE y, en su caso, el recurso de amparo ante el Tribunal Constitucional por su conexión con otros derechos fundamentales[1026], aunque no como derecho autónomo[1027].

Sin embargo, el derecho de rectificación pertenece también a los denominados derechos ARCO, lo que inevitablemente supone un vínculo con el derecho a la protección de datos personales. De hecho, como ya se ha visto anteriormente, la propia LOPD contempla este derecho expresamente, el cuál regula en el artículo 16 junto con el derecho de cancelación[1028].

De este modo, se obliga al responsable del tratamiento de datos personales a hacer efectivo el derecho de cancelación cuando así se solicite por el interesado y dichos datos resulten inexactos o incompletos, así como cuando dicho tratamiento no se ajuste a lo dispuesto en la legislación reguladora.

[1024] Para un estudio en profundidad de la cuestión, Cfr. GUTIÉRREZ GOÑI. *Derecho de rectificación y libertad de información*, J. M. Bosch, Navarra, 2003.

[1025] Otro inconveniente que se produce aquí en relación con la libertad de expresión e información, y que ya ha sido señalado en páginas anteriores, es si debería o no redefinirse en el contexto de Internet quienes son informadores, en tanto que cualquiera puede ser sujeto de información, pudiendo extender, en su caso, las exigencias derivadas del rigor periodístico y, como contrapartida, las garantías de las libertades informativas cualificadas. En este sentido, FERNÁNDEZ SALMERÓN defiende la extensión de las garantías del periodismo profesional, al menos, a ciertos servicios que puedan resultar, aún sólo parcialmente, equivalentes a la prensa y los medios tradicionales. Cfr. "Rectificación y réplica. Reflexiones sobre su proyección en la Web" en *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías* (Cotino Hueso, ed.), Universitat de València, València, 2011, p. 373.

[1026] Por todas, STC 171/1990, de 12 de noviembre.

[1027] Conviene remarcar aquí que el derecho de rectificación no protege opiniones subjetivas sino sólo informaciones de hechos, por lo que la tutela acerca de las opiniones lesivas o incorrectas debe redirigirse mediante otros procedimientos como las arriba citado así como mecanismos penales.

[1028] Del mismo modo, y a diferencia del presumiblemente extinto derecho de cancelación, el proyecto de Ley Orgánica de Protección de Datos, contempla su pervivencia en su artículo 15.

Por su parte, el Reglamento europeo de protección de datos, contempla expresamente el derecho de rectificación en su Sección tercera, en la que se incluye también el derecho al olvido. Así, su artículo 16 reza: "E*l 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*".

Ello está íntimamente relacionado con el principio de exactitud de los datos personales, propugnado como principio inspirador a lo largo de la legislación europea de datos y contemplado expresamente en el apartado d) del artículo 5 del GDPR que dispone la exigencia de que los datos personales sean exactos "y, si fuese necesario, actualizados", en el sentido de que se adecúen a los fines para los que sean tratados. Con tal objetivo, deberán adoptarse todas las medidas razonables que permitan rectificar una información personal, completarla o, en su caso, suprimirla. Así, la necesidad de mantener una exactitud en el tratamiento recae sobre la responsabilidad del encargado del tratamiento que es quien, en última instancia, debe prever y accionar las herramientas necesarias para facilitar la rectificación de los datos inexactos.

En cuanto al procedimiento para su ejercicio, el perjudicado deberá de solicitar al responsable del tratamiento la rectificación de sus datos personales, por medios electrónicos o tradicionales y, en el plazo de un mes desde su recepción –plazo prorrogable hasta dos meses- el responsable deberá de informar al interesado sobre su resolución, frente a la cual se podrá interponer una reclamación ante una autoridad de control así como ante los órganos jurisdiccionales (artículo 12 GDPR). Sin embargo, en el entorno de Internet, dada la proliferación de intervenciones anónimas, ello hace muchas veces casi imposible determinar la autoría de determinadas informaciones, requiriendo de la colaboración de los sitios web para la

identificación de sus usuarios, lo que plantea problemas acerca de la legitimación pasiva del ejercicio del derecho de rectificación[1029].

Sin entrar en los pormenores regulatorios del derecho de rectificación en el GDPR, cabe mencionar que comparte muchas de las garantías procesales con el derecho al olvido así como, por ejemplo, la gratuidad del procedimiento o la posibilidad de que una autoridad de control ejerza un poder correctivo contra aquél encargado del tratamiento que no cumpla con las obligaciones derivadas del derecho de rectificación -artículo 58.2.g)-.

La coexistencia de ambas figuras jurídicas se debe a las divergentes finalidades para las que ambas han sido concebidas. Si bien el derecho de rectificación busca restablecer la exactitud o veracidad de una determinada información divulgada así como la reputación o el honor de una personal, el derecho al olvido persigue preservar la privacidad del interesado, con independencia –o a pesar- de que los datos publicados sean exactos o veraces, pues su objetivo es limitar la difusión universal e indiscriminadas de información personal.

Sin embargo, la exactitud de los datos sobre los cuales puede ejercitarse el derecho de rectificación deriva en última instancia de la licitud del tratamiento de los datos, lo que va ligado inexorablemente con el principio de tratamiento lícito, leal y transparente del GDPR (artículo 6 GDPR) el cuál es aplicable asimismo al derecho al olvido que puede determinar la ilicitud de un tratamiento en origen lícito, por diversas causas contextuales como un determinado transcurso de tiempo.

En relación con lo anterior, el derecho de rectificación se constituye como una garantía jurídica para preservar la veracidad de una determinada información, en plena correspondencia con la garantía de las libertades informativas[1030], mientras que la veracidad no ocupa ningún papel significativo a la hora de determinar la aplicación del derecho al olvido en tanto que los

---

[1029] Otro inconveniente que plantea esta cuestión y que, por razones de extensión no pasamos a comentar, es la relativa a la responsabilidad de los motores de búsqueda que si bien no contienen la información inexacta en origen, la difunden exponencialmente, mediante la indexación de los sitios web en los que ésta se encuentre.

[1030] BENITO GARCÍA. "El derecho de rectificación electrónica: una forma interactiva de participación", en *La ética y el derecho de la información en los tiempos del postperiodismo*, Fundación COSO de la Comunidad Valenciana para el Desarrollo de la Comunicación y la Sociedad, Valencia, 2007, p. 164.

datos personales se presuponen todos ellos verdaderos –pues, de otra forma, no permitirían identificar correctamente a una persona-, cuya finalidad es la salvaguarda de la privacidad de los individuos en consonancia con la protección de sus datos personales.

Por otra parte, y pese a que el GDPR no condiciona el ejercicio del derecho de rectificación a la existencia de un perjuicio por parte del interesado, sí lo exige así la legislación doméstica -LO 2/1984, de 26 de marzo- lo que supone una clara diferencia con respecto al derecho al olvido que puede accionarse simplemente cuando los datos personales no sean adecuados ni necesarios para la finalidad del tratamiento sin que se requiera probar la existencia de un daño o perjuicio.

Vincular la rectificación a la existencia de una lesión, supone de facto una limitación de la legitimación activa, que queda circunscrita a aquellas personas que se hayan sentido aludidas por la información y que además sean perjudicados por ésta, al contrario de lo que sucede con el derecho de supresión. En relación con dicha cuestión, parece oportuno recordar lo dispuesto en el artículo 80 del GDPR que permite la representación de los interesados por parte de una entidad, organización o asociación sin ánimo de lucro para que preste en su nombre una reclamación y ejerza algunos de sus derechos, entre los cuales se encuentra presentar una reclamación ante una autoridad de control cuando considere que el tratamiento de sus datos personales infringe la normativa europea (artículo 77 GDPR).

Por último, en cuanto a la aplicabilidad práctica de ambos derechos, si bien el derecho al olvido plantea algunas incertidumbres en cuanto a la efectividad de lograr un borrado íntegro de la información de que se trate, la rectificación "digital", en el contexto de Internet, parece plantear muchos más problemas en tanto que, el dinamismo y la mutabilidad inherentes al medio pueden suponer un límite en si mismos para lograr una rectificación idónea a falta de encontrar una estabilidad apropiada para ejercitar la rectificación en igualdad de condiciones que, en origen, tuvo la información inexacta[1031].

[1031] Piénsese, por ejemplo, en una información inexacta publicada en un medio online, en el que a lo largo de un día puede ocupar diversos titulares o posiciones dentro de un mismo portal –con distintas extensiones tipográficas y temporales-,así

Por otra parte, si los plazos de 7 y 3 días previstos en la legislación nacional no parecen convenientes para el ejercicio adecuado de la rectificación, debido a la propia naturaleza de Internet, la extensión de los plazos concedidos al responsable para el ejercicio de la rectificación en el GDPR hasta un máximo de dos meses, parecen definitivamente desafortunados. Si bien *a priori* no hay ningún inconveniente en ejercitar el derecho de rectificación en los nuevos medios de comunicación, su efectividad práctica sí que puede quedar condicionada debido a la propia lógica del funcionamiento de Internet.

Teniendo lo anterior en consideración, deben reformularse los instrumentos de garantía del derecho de rectificación, principalmente para adaptar sus presupuestos a los nuevos medios de interacción social y de comunicación, principalmente condicionados por las propiedades intrínsecas de Internet pues, según su configuración actual, no parece tener éste demasiada virtualidad, siendo necesario replantearse su vigencia. De hecho, su pervivencia en el GDPR sólo se explica por su aplicabilidad práctica en concretos y reducidos supuestos jurídicos, fundamentalmente asemejados con los que pueden identificarse en los medios de comunicación más tradicionales[1032].

En contraposición, y como se ha venido defendiendo a lo largo de este trabajo, se observa como el derecho al olvido obedece a las necesidades imperantes de la realidad social más actual, permitiendo dar respuestas jurídicas a los individuos, para la pervivencia de sus derechos fundamentales, partiendo de la consideración expresa del medio en el que éste de desarrolla, condicionado por la democratización de Internet, la masificación del *Big data* y el desarrollo de las nuevas tecnologías.

---

como los múltiples medios de reproducción de ésta en otras páginas web, especialmente en redes sociales, y las dificultades que ello comporta para un adecuado ejercicio del derecho de rectificación en los términos actualmente planteados.

[1032] Así lo estima BENITO GARCÍA que dispone que el derecho de rectificación debería circunscribirse a los sitios web que alberguen medios informativos y que pueda aplicárseles de forma análoga los presupuestos jurídicos previstos para los medios tradicionales, sin que pueda extenderse ello al resto de informaciones o comunicaciones vertidas en Internet. Cfr. "El derecho de rectificación electrónica: una forma interactiva de participación", ob. cit., p. 175.

13. Consideraciones críticas

Una vez se han desgranado los pormenores del derecho al olvido, en base a la estructura clásica de los derechos fundamentales, teniendo un conocimiento más amplio y polifacético de la cuestión, y más allá de las conclusiones finales que pueden extraerse, parece oportuno llevar a cabo algunas consideraciones críticas o aportaciones adicionales acerca del derecho al olvido, más allá de las cuestiones que se han ido comentando a lo largo del trabajo, así como del modelo jurídico de respuesta confeccionado en su conjunto.

Brevemente y con la intención de facilitar el examen y la discusión de los temas a tratar, a continuación se ofrece una categorización de las observaciones que se han considerado oportunas realizar en función de las temáticas sobre las cuales versan.

13.1 De la creación del derecho al olvido como solución idónea ante el nuevo contexto

En primer lugar, resulta inevitable cuestionar la idoneidad de la figura del derecho al olvido para hacer frente a la realidad imperante descrita en el primer Capítulo de esta disertación. Esta cuestión puede analizarse desde dos puntos de vista, en primer lugar, examinando si la creación del derecho al olvido queda justificada por la coyuntura social actual, cuestión sobre la cuál ya se ha respondido afirmativamente a lo largo del presente trabajo. Como parece claro, la democratización de las nuevas tecnologías, la masificación de internet así como la proliferación del *Big data*, son los elementos básicos que han conllevado al cambio de paradigma y que han acontecido el surgimiento de nuevas estrategias jurídicas, como el derecho al olvido, para preservar los derechos fundamentales[1033].

En segundo lugar, podría preguntarse si, como tal, la creación del derecho al olvido es la solución adecuada para los riesgos y amenazas aparejadas al nuevo cambio de paradigma,

[1033] Todos los sistemas jurídicos están condicionados por un determinado nivel de conocimientos científicos y de técnicas interpretativas que se ponen a prueba cuando un determinado cambio social requiere de una adecuada respuesta del ordenamiento jurídico, momento en el que se hace constar la flexibilidad del mismo para adaptarse a un nuevo contexto. Así, y de forma inevitable, las transformaciones técnicas y científicas tienen el correspondiente influjo en el ordenamiento jurídico que puede adaptarse a través de la interpretación extensiva de su articulado o promulgando nuevas regulaciones a tal efecto. En cualquier caso, debe haber una clara correlación entre el avance científico-técnico y el cambio jurídico que éste exige, pues la proyección social de ambos es indiscutible.

entendiendo que, de otro modo, no podía obtenerse la satisfacción de los bienes jurídicos mediante los mecanismos tradicionales. O, en otras palabras, si puede acusarse al derecho al olvido de ser un parche creado para paliar la incapacidad manifiesta o la falta de voluntad de regular la vulneración de los derechos fundamentales en el ámbito de Internet.

Sobre esta cuestión, PAZOS CASTRO dispone que con el derecho al olvido "podrá mantenerse que se ha otorgado un nuevo nombre a derechos ya conocidos como son los de oposición y cancelación, si bien este nuevo nombre se emplearía para una aplicación particular de los mismos"[1034].

Como ya se ha visto en páginas anteriores, existen ligámenes indiscutibles entre el derecho de oposición y cancelación con el derecho al olvido, pese a que este último difiere de los anteriores en cuanto a su alcance y limitaciones, de hecho, éste se concibió sobre la base de aquéllos, como se aprecia en la STJUE del caso *Google* en la que solicitaba el derecho de oposición y cancelación y por la que se obtuvo el derecho al olvido como una concreción del derecho de oposición y cancelación en un caso concreto, como es el tratamiento de los datos en Internet[1035].

Ciertamente, pese a que los derechos de oposición, pero sobre todo de cancelación, se aplicaban regularmente y de forma efectiva ante los supuestos clásicos de tratamiento de datos, en cuanto la coyuntura cambió y las nuevas tecnologías, aplicaciones y servicios empezaron a emplear datos masivamente así como se extendió Internet hacia todos los ámbitos de la sociedad, los derechos ARCO tradicionales dejaron se resultar óptimos, insuficientes en definitiva, para la protección de los derechos fundamentales ante las nuevas amenazas y lesiones[1036].

[1034] PAZOS CASTRO. "El mal llamado derecho al olvido en la era de Internet", Boletín del Ministerio de Justicia, nº 2183, 2015, p. 40.

[1035] STJUE de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González,* Asunto C-131/12.

[1036] Así lo señala SIMÓN CASTELLANO que describe el derecho al olvido como una forma poética de hacer referencia a algunos de los extremos que se deducen de los principios de calidad de los datos y del consentimiento, y que se concretan en las facultades subjetivas de cancelación y oposición, que se adaptan al nuevo reto hacer frente "a la perennidad de la información en la red y los efectos multiplicadores de los motores de búsqueda, tanto por lo que se refiere a la accesibilidad

Así, el derecho a la cancelación de los datos no llegaba a permitir, en la práctica, una efectiva cancelación de los mismos debido, entre otras cosas, "al brumoso alcance y significado de la condición requerida (agotarse las *finalidades* para las que se obtuvieron)"[1037] lo que condujo a la creación del derecho al olvido como método más idóneo para garantizar el borrado digital de los datos personales de los sujetos en este nuevo contexto.

Sin embargo, nada obstaba a la doctrina y a la jurisprudencia a configurar el derecho al olvido sobre las figuras preexistentes, revisitándolas, dotándolas de nuevo contenido y de mayores prerrogativas[1038]. En efecto, podría haberse extendido el derecho de cancelación, dotándolo de un contenido mayor y reformulando sus supuestos de aplicación, convirtiéndolo *de facto* en el derecho al olvido actual, sin embargo, se prefirió emplear una nueva figura, de forma alternativa, para solucionar los nuevos problemas jurídicos. Sin duda ello fue fruto de una decisión estratégica, política si se quiere, para con ello enfatizar el cambio de paradigma ante el que se enfrenta el Derecho y el poder de éste para, no sólo adaptarse, sino responder con contundencia ante la nueva realidad social[1039].

---

como por lo que se refiere a la gravedad potencial de los perjuicios ocasionados", sin que haya variabilidad alguna en los principios jurídicos a proteger. Cfr. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, ob. cit., p. 291.

[1037] RALLO LLOMBARTE. *El derecho al olvido en Internet. Google versus España*, ob. cit. p. 30.

[1038] Una norma del siglo XIX como el Código Civil, se puede aplicar y, de hecho se aplica, para dotar de solución jurídica a conflictos aún inimaginables en el momento de su creación. Los principios jurídicos que contiene, así como la interpretación analógica de sus preceptos, permiten dotar a la norma de cierta laxitud capaz de hacer frente nuevos desafíos jurídicos. Por otra parte, si bien la Constitución española, no goza de esa volubilidad, mediante la interpretación jurisprudencial del Tribunal Constitucional, sí que se perfila, e incluso en muchos casos se amplía, el contenido o los presupuestos de aplicación de la Carta Magna, como se ha observado con el derecho de protección de datos personales.

Estos dos supuestos ejemplifican como, a veces, normas preexistentes en nuestro ordenamiento jurídico, son capaces de otorgar cobertura a la mayoría de los conflictos que se plantean en la actualidad, sin estar inicialmente concebidos para ello, gracias a los principios y valores estructurales que permanecen en el tiempo y se adaptan a las circunstancias cambiantes.

[1039] Parece que su objetivo es eminentemente didáctico, pretendiendo poner de relieve el nuevo contexto en que se crea el derecho al olvido, dándole una mayor entidad. Sin embargo, podría también cuestionarse el oportunismo de algunas normas jurídicas que surgen como panacea de nuevas realidades sociales que quizás podrían obtener respuesta jurídica a través de los mecanismos tradicionales. Ciertamente, en el caso concreto, no puede ignorarse la existencia de ciertos *lobbys* interesados en dirigir el cursor hacia sus intereses políticos, comerciales y económicos con fuerza suficiente como para germinar normas jurídicas en este sentido, por lo que podríamos preguntarnos si, el GDPR no es una obra de arquitectura jurídica orientada hacia el interés público pero capaz de esconder otros propósitos más partidistas, encaminados hacia aspectos muy concretos e intereses de unos pocos.

En tercer lugar, e íntimamente relacionado con lo anterior, otra cuestión estriba en preguntarse si, con el derecho al olvido, se ha pretendido proporcionar una solución legal a un problema verdaderamente estructural, en tanto que, al fin de cuentas, no parece posible afirmar de forma rotunda la existencia de una posibilidad efectiva de olvidarse de todo, de borrar todo rastro personal de Internet.

Sobre la imposibilidad de desaparecer de la Red, DOMÍNGUEZ MEJÍAS distingue entre "derecho al olvido digital" y el "borrado de datos", señalando que en ningún caso puede emplearse como expresiones equivalentes dado que el derecho al olvido no posibilita de ningún modo la "desaparición digital de la persona"[1040].

Si a ello le añadimos la existencia de páginas web de repositorios que tienen como finalidad guardar todo aquello que alguna vez ha sido publicado en Internet, aunque haya desaparecido del contenido de su página web original[1041], así como el funcionamiento mismo de la arquitectura de Internet que parece imposibilitar, por si mismo, un verdadero derecho al olvido. No es que uno no pueda teóricamente desaparecer de Internet, si no del todo casi por completo, sino que en el estado actual de las cosas, ello parece una utopía. Tal y como se concibe actualmente la normativa de protección de datos, así como la reticencia de los Gobiernos a ejercitar una política claramente intervencionista en la materia así como su permisividad ante la autorregulación y hacia el comportamiento abusivo de las empresas privadas que mercadean con la privacidad, y el afán de mantener la supuesta "neutralidad" con la que fue concebido Internet, hacen de la situación actual una Distopía[1042].

[1040] DOMÍNGUEZ MEJÍAS. "Hacia la memoria selectiva en Internet. Honor, intimidad y propia imagen en la era digital a partir de la jurisprudencia española" en *Revista Iberoamericana de Ciencia, Tecnología y Sociedad*, nº 32, Vol. 11, 2016, p. 56.

[1041] Un ejemplo lo encontramos en *Hidden for Google* (http://sur.ly/i/hiddenfromgoogle.afaqtariq.com/), una página web dedicada a recolectar aquéllos enlaces sobre los que se ha ejercitado el derecho al olvido.

[1042] Sin embargo, ello no es más que el fruto de un conjunto de decisiones, eminentemente políticas, que podrían de otro modo permitir un completo y efectivo derecho al olvido –piénsese en Corea del Norte o en China, dónde Internet (incluyendo al mismo buscador *Google*) está capado y sometido a los criterios gubernamentales- no sin incurrir en numerosos riesgos y lesiones para la sociedad democrática.

13.2 Del rol activo del afectado para el ejercicio del derecho al olvido

Como ya se ha apuntado en paginas anteriores, en cuanto al rol del sujeto activo, no parece muy garantista el hecho de que se exhorte al sujeto interesado a mantener una preocupación, participación y ejercicio activo para conseguir la garantía de sus derechos fundamentales, pues ello le exige una serie de conocimientos técnicos así como una dedicación personal, poco deseable para la protección de un derecho fundamental en una democracia constitucional. Se consagra así una lógica radicalmente diferente a la habitual en materia de libertades expresivas, dejando un gran poder de iniciativa al ciudadano sobre sus datos y sobre su imagen[1043]. De hecho, el cumplimiento de la ley, siempre mediado por la cultura de protección de datos, ya no sólo atañe a los tradicionales responsables del tratamiento sino también a los ciudadanos particulares, que quedan asimismo sujetos a la prohibiciones y obligaciones legales –privacidad 2P2-[1044].

Dichas circunstancias ostentan una lógica aparentemente contrapuesta a la propia del Estado de Derecho, pues no parece oportuno transferir la responsabilidad de la protección de los derechos fundamentales a los propios usuarios, a quienes se le suministran productos que están preconfigurados de tal forma que, si no se modifican *a posteriori* por el propio interesado, pueden acabar empleándose para vulnerar sus derechos fundamentales así como otros propósitos ilícitos. Frente a ello, resultaría más conveniente que, de forma generalizada, las aplicaciones tecnológicas relacionadas con el *Big data* funcionasen de manera transparente, permitiendo a los ciudadanos un control completo sobre sus datos personales y asegurando la supervivencia de las libertades colectivas e individuales[1045].

[1043] BOIX PALOP se pregunta por qué el derecho al olvido no puede permitir pedir a *Google* la supresión de todas las fotografías de una persona, en tanto que constituyen un dato personal, cuando ésta no se sienta favorecida a pesar de que hayan sido tomadas en actos públicos e incluso a pesar de que esa persona sea un cargo público. En la medida en que ninguna de esas fotos en sí misma no aporte nada al debate púbico y dado que todas ellas suponen un tratamiento de un dato personal no autorizado por el titular. Cfr. "El equilibrio entre los derechos del artículo 18 de la Constitución, el 'derecho al olvido' y las libertades informativas tras la sentencia Google" ob. cit., p. 25.

[1044] MUÑOZ SORO/ OLIVER-LALANA. *Derecho y cultura de protección de datos. Un estudio sobre la privacidad en Aragón*, Dykinson, Madrid, 2012, p. 46.

[1045] Cfr. POULLET. "Hacia nuevos principios de protección de datos en un nuevo entorno TIC", en *Revista de Internet, Derecho y Política*, nº 5, 2007, pp. 41 ss.

No obstante, tampoco debe de entenderse el derecho al olvido como la panacea ante el asedio del *Big data*, sino como el último recurso a ejercitar ante una situación de vulneración de derechos fundamentales. Existen, sin embargo, otros mecanismos ejercitables antes de llegar a solicitar el borrado digital -pensemos en los tradicionales derechos ARCO, por ejemplo-, en relación a ello y en cuanto al conflicto entre los bienes de la personalidad y las libertades de información, hay quienes defienden la existencia de un "derecho de arrepentimiento digital"[1046], que facultaría a sus titulares para obtener al borrado de aquellos contenidos digitales que les involucren y que hayan sido publicados en Internet con su consentimiento, por el simple hecho de haber cambiado de opinión con el paso del tiempo, "se trata de un derecho que comparte base ideológica y espiritual con el olvido digital, la fe en la capacidad del ser humano de cambiar y mejorar"[1047] pero que difiere de él en cuanto al sujeto causante del conflicto de derechos.

La tutela administrativa y judicial del derecho al olvido, como bien se ha visto, tiene sus límites y no constituye el único recurso para salvaguardar la privacidad pues, en la práctica, los verdaderos garantes son los propios interesados que, aunque de forma precaria y con limitaciones, tienen una serie de derechos y facultades para "auto-protegerse". Sin embargo, el desarrollo y generalización de conductas de autoprotección presuponen un alto nivel de concienciación social en la materia, por lo que la cultura de protección de datos de los ciudadanos adquiere una dimensión esencial para reivindicar y obtener las garantías adecuadas en materia de derechos fundamentales[1048]. No obstante, sin entrar en el debate anterior relativo a la práctica de atribuir al sujeto la responsabilidad de hacer cumplir sus derechos[1049], si bien es

[1046] DOMÍNGUEZ MEJÍAS. "Hacia la memoria selectiva en Internet. Honor, intimidad y propia imagen en la era digital a partir de la jurisprudencia española" en *Revista Iberoamericana de Ciencia, Tecnología y Sociedad*, nº 32, Vol. 11, 2016, p. 62.

[1047] DE TEREWAGNE, "Privacidad en Internet y el derecho a ser olvidado", *Revista de Internet, Derecho y Política*, nº 13, 2012, p. 55. Señala el autor que, en los casos más extremos, los excesos del pasado conducen al internauta a lo que se ha llamado "suicidio digital" que responde al deseo de desaparecer voluntariamente y por completo de Internet, principalmente de las redes sociales.

[1048] MUÑOZ SORO,/ OLIVER-LALANA. *Derecho y cultura de protección de datos. Un estudio sobre la privacidad en Aragón*, Dykinson, Madrid, 2012, pp. 47-48.

[1049] Rechazamos el *status activus processualis* que defendieron, entre otros, DENNINGER, y que reclamaba una participación activa por parte del sujeto afectado en la reivindicación de sus derechos, asumiendo su propia responsabilidad

cierto que se necesita crear en los ciudadanos una conciencia crítica acerca de lo que supone la situación actual de la privacidad y del libre comercio de los datos personales[1050], ello no exime a los Estados de adaptar el ordenamiento jurídico para conseguir una protección eficaz de los derechos en juego.

En este sentido, PÉREZ LUÑO apunta la idea de la "responsabilidad tecnológica" como la necesidad de que se produzca una actitud reflexiva, critica y consciente de la nueva coyuntura social, tecnológica, económica y jurídica ante la que los ciudadanos no pueden permitirse el lujo de asistir pasivamente. Sobre la idea de que la teoría y práctica de la democracia no pueden resultar insensibles al nuevo escenario en que las innovaciones tecnológicas que han tenido someras repercusiones en los derechos humanos, poniendo en riesgo determinados derechos y libertades[1051].

13.3 De la privatización del juicio de ponderación. Propuesta de *lege ferenda*

Puesto que, del conjunto de la normativa en materia de protección de datos, no queda duda de que, en caso de conflicto de derechos –cosa que se produce casi siempre- debe hacerse una operación de ponderación entre los bienes jurídicos disputados y, dado que la regulación de los límites del derecho al olvido está llena de inconcreciones y lagunas, ello implica la transmisión de la responsabilidad de dicha decisión a dos sujetos intervinientes, ninguno de ellos apropiado.

Por una parte, se transfiere dicha responsabilidad a los motores de búsqueda que son quienes, en primer lugar, reciben las solicitudes de los interesados para la supresión de determinados datos personales, frente a las cuáles han de decidir si efectivamente desindexan

---

en los procedimientos en que sus libertades son afectadas. No se puede responsabilizar a los ciudadanos del cumplimiento de sus derechos fundamentales en la medida en que no depende de ellos, sino que debe existir una acción de los Estados que les otorgue de garantía suficiente. Cfr. "Government Assistance in the Exercise of Basic Rights" en *Critical Legal Thought: An American-German Debate* (Joerges/Trubek eds.), Nomos, Baden-baden, 1989.

[1050] NAVAS NAVARRO define este fenómeno bajo la denominación del "*mindfulness*", defendiendo cambiar la actual relación de los ciudadanos con Internet y las nuevas tecnologías, de modo que éstos actúen en el entorno digital bajo la conciencia plena de lo que ello significa así como de sus consecuencias, modificando la relación de los individuos con su información personal, pasando de "ser objeto observado a sujeto observador". Cfr. *Mercado digital. Principios y reglas jurídicas*, ob. cit., p. 276.

[1051] Cfr. *Los derechos humanos en la sociedad tecnológica*, Universitas, Madrid, 2012, p. 42.

dichos enlaces web o no. Sin embargo, parece inapropiado que el juicio de valor entre dos bienes jurídicos en colisión se deje en manos de una empresa privada –cuyo interés es meramente privado, la consecución de beneficios económicos, y que en nada incumbe al bien común[1052]- que usurpa las funciones propias de las autoridades nacionales de protección así como de los órganos jurisdiccionales, quienes son legalmente competentes para ello. Esta dejación de funciones puede ocasionar la adopción de decisiones que no conlleven un verdadero ejercicio de búsqueda del equilibrio de los intereses en juego o que respondan a objetivos viciados por la subjetividad propia del criterio del motor de búsqueda[1053].

En segundo lugar, frente a la negativa de dicho buscador web de suprimir determinados datos personales, el afectado podrá dirigirse a la AEPD y, en su caso como ya se ha explicado en páginas anteriores, interponer demanda ante los órganos jurisdiccionales. Respecto de la AEPD resulta inevitable cuestionar el gran poder que se concede a la Administración pública a la hora de mediar en conflictos privados -por mucho que ésta tenga como finalidad específica la protección de los datos personales- que, además, versan sobre el ejercicio de libertades expresivas fundamentales en una sociedad democrática, así como su viabilidad a tenor del artículo 20.2 CE y su prohibición de censura previa. Se produce un punto de inflexión –e incluso un cierto retroceso- respecto de las dinámicas propias de una sociedad pluralista así como del equilibrio tradicional entre derechos fundamentales basado en un control judicial *ex post* de las manifestaciones vertidas en pro de la libertad de expresión e información, que ahora quedan sometidas al control de los poderes públicos y sin unas reglas de juego claras[1054].

[1052] Como ejemplo, piénsese en el buscador *Google* que, si bien ha reiterado en numerosas ocasiones su oposición a la política garantista europea en materia de datos personales, reivindicando la sinrazón de extender sus estándares de protección más allá de su territorio y alegando una intromisión en su libertad de empresa; no le ha importado en absoluto someterse a las condiciones del régimen dictatorial chino –con una consecuente intervención en su actividad empresarial- a cambio de poder operar en su territorio. Si bien el análisis de esta cuestión requeriría de una reflexión mayor, que por razón de extensión no puede llevarse en este trabajo, puede apuntase a la doble moral de algunas de las empresas del *Big data*, cuya actuación, pese a que se enarbole el argumento de la "libertad" y "neutralidad", únicamente obedece a criterios económicos.

[1053] Cfr. MINERO ALEJANDRE. "A vueltas con el 'derecho al olvido'. Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital", Revista Jurídica de la Universidad Autónoma de Madrid, nº 30, 2014, p. 149.

[1054] Cfr. BOIX PALOP. "El equilibrio entre los derechos del artículo 18 de la Constitución, el 'derecho al olvido' y las libertades informativas tras la sentencia Google" en *Revista General de Derecho Administrativo* nº 38, 2015, p. 36.

Sobre el abuso del recurso a los tribunales, ya advirtió en su día DÍEZ-PICAZO que las proporciones titánicas de la burocratización del sistema judicial, lejos de mejorar, lo atascan, de forma que "*el asunto se transforma en expediente y los órganos de justicia en máquinas de resolver*"[1055]. El abarrotamiento de las instancias judiciales las lastra a una lentitud que no favorece en absoluto a la resolución de las demandas ciudadanas y, en asuntos como el aquí tratado, no puede quedarse en *stand-by* tanto tiempo, necesita de soluciones raudas.

Por otra parte, y a pesar de que dichos órganos están debidamente preparados para llevar a cabo tareas de este tipo, la cantidad ingente de conceptos jurídicos indeterminados de la única normativa en vigor acerca del derecho al olvido –el GDPR- así como sus constantes remisiones al desarrollo posterior por la legislación doméstica –que, en el caso del legislador español, no se ha llegado a efectuar aún- dificultan enormemente su tarea y añaden una mayor incertidumbre y discrecionalidad a la tutela administrativa y judicial del derecho al olvido.

Un ejemplo lo encontramos en las dificultades que entraña la determinación del tiempo que debe transcurrir para que una información deje de tener pertinencia, actualidad o vigencia pública, y las circunstancias en las que el regreso al anonimato de una persona que en su día pudo desempeñar un cargo o papel en la vida pública reduzca el interés público en disponer de esa información y haga prevalecer el derecho al olvido de dicha persona[1056]. El único elemento que aporta claridad en este sentido es la decisión del TJUE en el *caso Google*, lo que supondría aplicar el derecho al olvido en todos aquellos casos en que hubieran referencias análogas entre los supuestos de hecho.

Así, resulta excesivo el peso que se le otorga a la ponderación en el derecho al olvido, obligando a analizar caso por caso y a poner en valor no sólo hechos subjetivos, sino también intereses sociales e individuales[1057], tratando de llegar a un equilibrio cuando la falta de

[1055] Cfr. DÍEZ-PICAZO. *Derecho y masificación social. Tecnología y Derecho privado (dos esbozos)*, Civitas, Madrid, 1979, p. 79.

[1056] Cfr. MUÑOZ. "El llamado derecho al olvido en Internet y la responsabilidad de los buscadores", Diario la Ley, nº 8317, 2014, p. 6 ss.

[1057] A este respecto, recuerda CERNADA BADÍA que incluso respecto de valores esenciales como ocurre con la publicidad de las actuaciones judiciales, no existe un consenso acerca de qué interés debe prevalecer en una sociedad democrática, si el derecho a la privacidad o a la libertad informativa. Cfr. "El derecho al olvido judicial en la red" en *Libertad de Expresión e*

parámetros legales comporta excesivas lagunas y, en última instancia, provoca inseguridad jurídica[1058]. Frente a ello, no estaría demás una propuesta de *lege ferenda* capaz de articular los parámetros concretos que deben enmarcar todo análisis jurisprudencial del derecho al olvido, reduciendo el margen de discrecionalidad de los órganos jurisdiccionales y aumentando la seguridad jurídica de los intervinientes[1059]; así como disponer de forma expresa en el apartado cuarto del artículo 18 de la Constitución, tanto el derecho a la protección de datos como el derecho al olvido.

El derecho al olvido ha irrumpido en el escenario jurídico a base de pronunciamientos jurisprudenciales así como de la mano del Reglamento europeo de protección de datos, sin que el legislador español haya cumplido con los plazos establecidos en este último para la modificación de su normativa interna, ni haya aportado una regulación sustanciosa de la cuestión, como puede apreciarse en el Proyecto de Ley Orgánica de Protección de Datos personales que se limita a hacer una breve referencia al derecho de supresión en los mismos términos que dispone el GDPR. Se echa de menos así, una regulación específica y unitaria, que sea capaz de abordar el fenómeno desde un punto de vista global, acabando con la disparidad de procedimientos existentes hasta el momento, así como con la superposición de otras figuras como el derecho de cancelación o el derecho al honor, sobre el cual podría proveerse, por ejemplo, mecanismos agregados para la garantía de los derechos del afectado, en lugar de la actual intercalación entre normativas reguladoras específicas.

En este sentido, RALLO LLOMBARTE señala la necesidad de establecer un nuevo marco de protección de los ciudadanos en la era digital, lo que implicaría reconocer nuevos

---

información en Internet. Amenazas y protección de los derechos personales (Corredoira y Alfonso, y Cotino Hueso coord.), Centro de Estudios Políticos y Constitucionales, Madrid, 2013, pp. 521 ss.

[1058] Cfr. SIMÓN CASTELLANO. *El régimen constitucional del derecho al olvido digital*, ob. cit., p. 144.

[1059] Esta propuesta no está exenta de críticas por aquéllos que entienden que el Derecho no es una esfera libre de poder, sino un recurso de éste cuyo instrumento más importante es la prohibición y, por ende, cuanta más regulación, menos margen de libertad se deja a los individuos. Por todos, SOFSKY, W. quien defiende: "Las prohibiciones son órdenes y exigen pronta obediencia. Sea cual fuere la justificación que se invoca, el régimen de la prohibición tiende en última instancia a la supresión de la libertad por orden estatal. El Estado de derecho total debe dirigir la sociedad y educar a los súbditos. Reglas y preceptos incesantemente renovados se entrometen en la vida cotidiana". Cfr. *Defensa de lo privado*, Pre-textos, 2009, p. 33.

derechos digitales en el ámbito legal y en el constitucional, disponiendo que una hipotética reforma de la Carta Magna "debería incluir la actualización de la Constitución en la era digital y constitucionalizar una nueva generación de derechos digitales, de carácter sustantivo o prestacional, entre los que merecerían sobresalir los siguientes: a) el derecho de acceso a Internet independientemente de la condición económica; b) el derecho a la formación digital; c) el derecho a la neutralidad de la Red garantizando un internet libre, abierto, equitativo e innovador; d) el derecho al honor y a la propia imagen frente a agresiones específicas procedentes de la red; e) el derecho a la libertad de expresión y a la veracidad de las informaciones en la Red; f) el derecho de los trabajadores a su intimidad en la utilización de medios digitales y el derecho a la desconexión laboral; g) el derecho de acceso online a datos, innovaciones, creaciones y conocimiento generado con fondos públicos; h) el derecho a obtener reparación efectiva ante daños causados por conductas ilícitas en la Red; i) el derecho de los menores a su seguridad en la Red"[1060].

Con sólo algunas de las medidas esgrimidas anteriormente, se lograría dotar a los ciudadanos de una mayor seguridad jurídica, al mismo tiempo que limitaría el margen de discrecionalidad de los órganos jurisdiccionales en torno a la configuración del derecho al olvido, cumpliendo con los presupuestos generales del Estado social de Derecho. Por otra parte, acabaría con la disparidad normativa actual y la tendencia a la hiperregulación, que lejos de simplificar las cosas, dificulta la garantía jurídica de los derechos fundamentales. Se pretende así, simplificar los derechos y aunar los procedimientos, en lo que DÍEZ-PICAZO definió como la destrucción del ideal jacobino: "pocas leyes, claras y cortas", esencial para conseguir un sistema jurídico abarcable y comprensible[1061].

[1060] RALLO LLOMBARTE. "De la libertad informática a la constitucionalización de nuevos derechos digitales (1978-2018)", *ob. cit.*, pp. 665-667.

[1061] DÍEZ-PICAZO. *Derecho y masificación social. Tecnología y Derecho privado (dos esbozos)*, ob. cit., p. 79. El autor llegó a afirmar en su momento "Tras veinticinco o treinta años de estudios, me pregunto cuál puede ser la proporción del ordenamiento español que yo mismo conozco. Y con una buena dosis de optimismo, la conclusión a la que llego es que rondará entre un doce o un quince por ciento".

13.4 De la protección de la privacidad como principio general

Por otra parte, parece procedente cuestionarse si los cambios legislativos propuestos y las iniciativas públicas surgidas a tenor del nuevo paradigma, están directamente encaminadas a la protección de la privacidad de los ciudadanos, como una suerte de regla general. En relación con ello, y teniendo en cuenta todos los extremos expuestos en este trabajo, sería ingenuo pensar que los ciudadanos tienen a su disposición los mecanismos necesarios para hacer cumplir sus derechos y libertades en este campo, pues la legislación vigente en materia de protección de datos no tiene como fin exclusivo la garantía de los derechos de los ciudadanos y su privacidad sino que, al mismo tiempo, tiene como objetivo asegurar el libre flujo de datos entre los Estados parte, en un intento de acabar con la competencia desleal, lo que constituyen presupuestos aparentemente contrapuestos.

Buen ejemplo de ello, puede encontrarse en lo ocurrido con el *Safe Harbor* y la Sentencia del TJUE de 2015 en el *caso Schrems*[1062] que lo declaró inválido. En primer lugar, recordar que la regulación europea en materia de protección de datos anterior al GDPR, prohibió la transferencia internacional de datos personales de ciudadanos europeos a países que no contasen con ciertos estándares de protección, entre ellos Estados Unidos, territorio hacia el que se ha producido un éxodo masivo de empresas relacionadas con el *Big data* gracias a su laxa legislación, más permisiva con el mercadeo de la privacidad. Para lograr el intercambio comercial de datos entre la Unión Europea y los Estados Unidos entró en vigor el año 2000 el *Safe Harbor* (Puerto Seguro), una norma de adhesión voluntaria a la que se suscribieron empresas que operaban con datos a los dos lados del atlántico para garantizar así el tráfico de los mismo, a cambio de acatar el cumplimiento de ciertas normas de seguridad[1063].

A raíz de las filtraciones llevadas a cabo en 2013 por Edward Snowden, excontratista de la NSA y la CIA, se dejaron en evidencia las prácticas de espionaje masivo que se estaban

[1062] STJUE de 6 de octubre de 2015, asunto C-362/14.

[1063] Los requisitos que se exigían para formar parte del *Safe Harbor* eran de muy fácil cumplimiento,

mucho menos rígidos que los exigidos por la normativa europea en protección de datos, por lo que casi cualquier empresa estadounidense que lo solicitase entraba a formar parte de él. Se puede consultar la lista completa en: https://safeharbor.export.gov/list.aspx.

llevando a cabo por agencias de EEUU -en colaboración con otros países aliados- sobre la población mundial. Esto llevó al TJUE, a raíz de una demanda presentada por un ciudadano austríaco que arremetía contra *Facebook* por vulnerar su privacidad, a concluir que Estados Unidos no era un país seguro en materia de protección de datos, abriendo la puerta a los Estados europeos a que declarasen, si así lo estimaban, que el tratamiento de datos de sus ciudadanos por EEUU era ilegal.

Sin embargo, en contra de lo que dicta el sentido común, esto no significó el fin de las transferencias de datos personales desde la UE hasta los EEUU pues, aunque el vigente Reglamento de datos ha endurecido los estándares de seguridad, por otro lado, Estados Unidos y la Unión Europea llegaron a un nuevo acuerdo llamado *Privacy Shield*[1064] (Escudo de Privacidad) que, aunque impone mayores exigencias a las compañías estadounidenses[1065], les permite de facto, seguir especulando con los datos personales de los ciudadanos europeos con cierta impunidad[1066], sorteando los principios generales inherentes a la normativa europea de protección de datos[1067].

Así pues, la normativa en materia de protección de datos personales parece adquirir cada vez más un valor simbólico, como afirman MUÑOZ SORO y OLIVER-LALANA nuestro sistema de protección de datos "se articula alrededor de una aspiración ideal que se ha convertido en un mito: que en la sociedad actual cualquiera pueda mantener un control–al menos razonablemente- amplio sobre su información personal. Esto es, a grandes rasgos, lo que vienen a prometer las leyes, y lo que ratifican sus intérpretes privilegiados: las agencias y

[1064] Decisión de Ejecución (UE) 2016/1250 de la Comisión de 12 de julio de 2016.

[1065] El Departamento de Comercio de los Estados Unidos es el órgano encargado de velar por el cumplimiento de las normas acordadas por parte de las empresas que voluntariamente hayan firmado el acuerdo, bajo pena de sanciones. Se puede consultar online la lista completa de entidades adheridas en: https://www.privacyshield.gov/list

[1066] El GT29 declaró su falta de conformidad con dicho acuerdo por entender que se alejaba demasiado de los estándares de protección del GDPR. ARTICLE 29 DATA PROTECTION WORKING PARTY. *Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision*, 2016. Disponible online en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

[1067] Entre ellos, la excepcionalidad de las transferencias internacionales de datos que, en la práctica, se han convertido en la regla general y no en la excepción.

autoridades de protección. Pero o bien estamos ante una promesa que resulta inviable o bien entramos directamente en el terreno del engaño ideológico"[1068].

Aunque el avance en la materia ha sido notable en los últimos quince años, tanto jurisprudencialmente como a través de las nuevas medidas normativas, se observan muchas contradicciones en torno a las políticas públicas de protección de datos (como se observa en la adopción de acuerdos como el *Privacy Shield* o en la innegable dejación del legislador español que, más de dos años después de la entrada en vigor del GDPR no ha dictado la legislación doméstica preceptiva[1069]) mientras que las empresas privadas siguen traficando con datos personales sin apenas ninguna dificultad. Si a ello le sumamos revelaciones estremecedoras como las de *Snowden* o *WikiLeaks* o la sucesión de noticias relacionadas con la proliferación de *Fake News* y su injerencia en las democracias de nuestro entorno como el caso de *Cambridge Analytica*, resulta realmente difícil ser optimistas y constructivos en este marco.

Sin duda gobiernos y ciudadanos se encuentran cada vez más concienciados respecto de las amenazas que para los derechos fundamentales tiene las nuevas tecnologías por lo que, pese al clima descrito anteriormente, siempre podría corregirse –aunque ello parece poco probable- el actual rumbo de los acontecimientos y lograr un cambio de modelo para el paradigma actual. El derecho al olvido se encuentra en un estado relativamente incipiente por lo que quizás, con el transcurso del tiempo, la extensión y madurez de una cultura social de protección de datos así como la exigencia firme de políticas de privacidad por defecto y desde el diseño, en unos años el olvido digital se convierta en una realidad tangible y sin fisuras y los ciudadanos consigamos tener la privacidad que prometen nuestras leyes.

[1068] MUÑOZ SORO,/ OLIVER-LALANA. *Derecho y cultura de protección de datos. Un estudio sobre la privacidad en Aragón*, Dykinson, Madrid, 2012, p. 69.

[1069] Por otra parte, tampoco se explican actuaciones del legislador como las llevadas a cabo a través del Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos, publicado el pasado 30 de julio de 2018 en el Boletín Oficial del Estado (nº 182, p. 76249). Bajo el pretexto de la concurrencia de motivos de urgencia, se regulan aspectos relativos a la inspección y al régimen sancionador en materia de datos personales, así como concernientes a los procedimientos en caso de una eventual vulneración de la normativa de protección de datos, lo que plantea serias dudas de constitucionalidad en tanto que son aspectos inherentes a un derecho fundamental y que, por ende, su regulación debe estar sujeta a una Ley Orgánica, no pareciendo oportuno considerarlas cuestiones accesorias.

13.5 De la *privacy by design* y la *privacy by default* como alternativa

Relacionado con lo anterior así como con el objeto de encontrar un remedio para la incertidumbre jurídica de la que adolece el actual marco normativo, ello podría resolverse aplicando políticas de privacidad por defecto y desde el diseño, limitando la acción tecnológica para que apriorísticamente se protejan los derechos fundamentales de sus usuarios sin necesidad de interacción alguna por su parte.

Sobre estas medidas se pronuncia el GDPR, el cuál dedica el artículo 25 a dicha cuestión[1070] aunque, nuevamente su amplitud material y terminológica, hace de ello un principio inspirador y no un mandato real hacia las tecnológicas y corporaciones del *Big data*, lo cuál sería deseable para garantizar un claro marco regulador, pese a que ello significaría cambiar la estrategia actual de los gobiernos y apostar por un intervencionismo en la materia.

Estas medidas, que reciben en inglés la denominación de "*privacy by design*" y "*privacy by default*", están íntimamente relacionadas pues constituyen dos caras de la misma moneda -mientras que la primera es predicable respecto de la industria, la segunda viene referida a los usuarios- y no son de nueva creación por parte del GDPR sino que, en el ámbito europeo, tiene sus raíces en la opinión del Supervisor Europeo acerca de la modificación de la normativa europea en la materia[1071] así como en los informes del GT29[1072]. Éstas, se basan en la idea

---

[1070] Artículo 25 GDPR, 1."*Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados*".

2. "*El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines*

específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto,

los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

[1071] EUROPEAN DATA PROTECTION SUPERVISOR, "A comprehensive approach on personal data protection in the European Union", *Opinion of the European Data Protection Supervisor on the Communication from the Commision to the European Parliament*, 2011, p. 23. Disponible online en: https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf

general de integrar la privacidad en la arquitectura de todo sistema, aplicación o instrumento tecnológico así como en todo proceso que comporte tratamiento de datos personales, "*dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad*"[1073].

Se produce así una inversión del proceso de protección de la privacidad, que deja de operar como una reacción del interesado ante la vulneración de sus derechos fundamentales, para llevarse a cabo de manera proactiva y preventiva por parte de aquéllos que diseñan los productos o sistemas que pueden dar lugar a la vulneración de datos personales, protegiendo a los ciudadanos frente a eventuales intromisiones en su vida privada sin que sea necesario que éstos emprendan ningún tipo de acción[1074].

Y es que, como ya ha quedado probado en el primer Capítulo, los abusos acometidos por la informática y la telemática ni son fruto del azar ni son inevitables, sino que responden a decisiones conscientes de aquéllos que las crean o las emplean en el entorno del *Big data*. Así, en la actualidad se ha impuesto un modelo en el que la tecnología, que no es neutral, se ha inclinado por la comercialización de los datos personales, preconfigurando los dispositivos electrónicos inteligentes para monitorizar la actividad de los usuarios: sus contraseñas, sus rutinas de conexión, su localización, sus hábitos de consumo… convirtiendo información tradicionalmente privada en no tan privada y al servicio de la mercadotecnia.

Frente a ello, se propone operar, desde el momento del diseño inicial así como en el desarrollo de una tecnología, teniendo en cuenta el derecho a la protección de datos personales

---

[1072] ARTICLE 29 DATA PROTECTION WORKING PARTY. *Recomendation 01/99 on invisible and automatic processing of personal data on the Internet performed by software and hardware*, 1999, p. 3. Disponible online en: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp17_en.pdf

[1073] Considerando 78º GDPR.

[1074] Se prevé el uso de certificaciones para acreditar el cumplimiento de las obligaciones relativas a la privacidad desde el diseño y por defecto (artículo 17.3 GDPR).

como una variable más para su buen funcionamiento, respondiendo así a una visión de prevención y de reducción de riesgos que puede limitar cuantiosamente la vulneración de derechos fundamentales en este contexto. La protección por defecto de los datos personales se extiende durante todo su ciclo de vida ya que se aplica a la cantidad de datos recogidos, a la extensión del tratamiento en cuestión, pero igualmente a su plazo de conservación y de forma particular a la accesibilidad de los mismos, ya que no deben poder acceder a los mismos un número indeterminado de personas sin la intervención del interesado[1075].

En efecto, si se quiere proteger la privacidad y hacer que ésta opere como una regla general, es necesario contar la complicidad de la propia tecnología que, de forma predeterminada, desde su concepción inicial hasta su funcionamiento, debe responder a criterios compatibles con la protección de datos personales, en plena consonancia con la "*accountability*" -desde un sentido de responsabilidad- y la transparencia que propugna la normativa de datos personales. Y con ello, establecer unos parámetros por defecto que protejan lo máximo posible los datos personales, de forma que ningún titular de aquéllos pueda verse expuesto a diferentes riesgos que ignora o que no sabe valorar en su justa medida[1076].

Sin embargo dichas acciones de privacidad desde el diseño y por defecto, conforme al Reglamento europeo de protección de datos, se imponen directamente al responsable y encargado del tratamiento y no a las empresas tecnológicas y productoras de sistemas de tratamiento de datos sobre las que el GDPR sólo emite recomendaciones[1077] y quienes, por el contrario, tienen una gran responsabilidad en la materia, al ser éstas la que alumbran -diseñan, desarrollan, seleccionan y usan- los métodos informáticos –productos, servicios y aplicaciones- que posibilitaran, en el futuro y debido a un mal uso, un tratamiento de datos vulnerador de derechos fundamentales.

[1075] DUASO CALÉS. "Los principios de protección de datos desde el diseño y protección de datos por defecto" en *Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad* (Piñar Mañas dir.), Reus, Madrid, 2016, pp. 310 ss.

[1076] POULLET. "Pour une troisième génération de réglementations de protection des domnées", en *Jusletter*, nº 3, 2015, p. 12.

[1077] "*Ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones*", considerando 78º GDPR.

Ello está directamente relacionado con la exigencia de transparencia que se incluye en el propio GDPR y que se deriva asimismo, de las demandas sociales y la evolución misma del ordenamiento jurídico. Este principio, cuya aplicación es transversal, incide en múltiples aspectos de lo que se ha tratado en este trabajo, desde el requerimiento a las corporaciones del *Big data* para que descubran la lógica algorítmica empleada para el tratamiento de los datos personales, hasta la necesidad de lograr una claridad y sencillez en sus prácticas de contratación en masa y sus políticas de privacidad.

El principio de transparencia, como se ha señalado en páginas anteriores, supone un cambio de modelo a la hora de contratar de forma que, las cláusulas contractuales, además de los intereses particulares del predisponente, tengan en cuenta la realización de otros bienes o intereses generales del orden público, como son la protección o tutela de la parte contractual más débil y la calidad y competencia de la contratación bajo condiciones generales[1078]. Puesto que las cláusulas abusivas constituyen una vulneración frontal de los intereses generales, debe llevarse a cabo una transformación cualitativa de los esquemas teóricos del contrato por negociación, en tanto que "la transparencia, junto con el equilibrio de las prestaciones, se ha erigido como un principio jurídico del control social establecido" [1079].

Ello resulta especialmente predicable respecto de las prácticas de almacenamiento, tratamiento y difusión de los datos personales y de su gestión por los operadores, cualquiera que sea su naturaleza, así como de la regulación en su conjunto. De este modo, el principio de la transparencia debe concebirse como parte de un cambio cultural inherente a las exigencias del Estado social y democrático de Derecho, que consolida dicho valor como parte integrante de la razonabilidad moral y principio rector de las políticas públicas, vertebrando el conjunto del ordenamiento jurídico.

[1078] Ello se deriva de la STJUE de 21 de diciembre de 2016, asuntos acumulados C-154/15, C-307/15 y C-308/15, por la cuál se declara el carácter abusivo de las denominadas "cláusulas suelo" por falta de transparencia.

[1079] Cfr. ORDUÑA MORENO/SANCHEZ MARTÍN. *La transparencia como valor del cambio social: su alcance constitucional y normativo. Concreción técnica de la figura y doctrina jurisprudencial aplicable en el ámbito de la contratación*, ob. cit., p. 37.

13.6 De las paradojas de la privacidad

Podría decirse que en el momento actual se produce una de las mayores paradojas de la vida moderna y es que, si bien en el pasado se consideraba que el Estado era la mayor amenaza real y potencial de las libertades, frente al cuál surgió un numeroso catálogo de derechos y libertades capaces de defender a los ciudadanos de su propio Estado, en la actualidad se hace necesario contar con la tutela de los poderes públicos para la defensa de casi todas las libertades. Esta paradoja se ha descrito por DENNIGER en los siguientes términos "El mismo poder estatal para cuyo límite surgen los derechos fundamentales es, a la postre, el único que puede proteger eficazmente tales derechos"[1080].

Ello no implica, sin embargo, que no exista amenaza por parte del poder estatal, peusto que su posición de preeminencia refuerza su potencial lesivo también en la actualidad sin embargo, junto a él y en el campo que nos ocupa, ha surgido una industria privada cuyo poder para la vulneración de los derechos fundamentales se ha revelado como enorme, surgiéndole a los poderes públicos numerosos competidores en la limitación de las libertades públicas, especialmente respecto del derecho a la privacidad.

Existe una posición dominante por parte de las corporaciones del *Big data* y las empresas de Internet con una capacidad increíble de condicionamiento para los individuos, que han creado una economía de los datos personales, gracias en gran parte a la pasividad de los Estados, debe reconocerse. En este contexto, la exigencia al respeto de los derechos y libertades fundamentales de los ciudadanos requiere, en todo caso, el apoyo directo y explícito de los organismos públicos nacionales e internacionales.

Afirma PÉREZ LUÑO en este sentido "Los todopoderosos medios de comunicación se creen con derecho para invadir nuestra privacidad, para juzgarla y sentenciarla, en régimen de absoluta impunidad […] Hoy son los poderes públicos de las sociedades democráticas los

[1080] DENNINGER. *Menschenrechte und Grundgesetz. Zwei Essays*, Belt Athenäum, Weinheim, 1991, p. 11.

aliados necesarios de los ciudadanos en el esfuerzo por poner coto a las intromisiones abusivas de poderes privados en el ámbito de la intimidad individual"[1081].

Los pocos cambios que han llevado a cabo las empresas del *Big data* bajo el argumento de mejorar la transparencia de sus servicios se deben, de una parte a la normativa imperante en la materia, que va constriñendo su margen de actuación -hasta hace poco enorme, gracias a la autorregulación del sector-, y de otra a las demandas de los usuarios que exigen un mayor control sobre su privacidad, por lo que dichas corporaciones se han visto forzadas a recuperar o no perder la confianza que depositan en ellas millones de personas que utilizan sus servicios y en cuyos datos personales se basa su modelo de negocio. Así, estas empresas intentan que su política de transparencia haga más aceptable la realidad, pero no parece tanto que se recupere la privacidad como que las empresas buscan que se acepte como natural la situación previa[1082], como puede observarse en la inamovilidad de su estructura de negocio.

Esta inmutabilidad del modo de funcionar de las corporaciones del *Big data* para con la privacidad, viene sustentada por la actitud pasiva de sus usuarios que, si bien parecen estar preocupados por su privacidad y están cada vez más informados sobre sus derechos, se detecta una creencia muy extendida de que las amenazas a la privacidad resultan ya inevitables y que el rápido avance de las tecnologías de la comunicación hace imposible la adecuada garantía de nuestra esfera privada o la protección de la información personal. Como señalan MUÑOZ SORO y OLIVER-LALANA "La gente percibe la pérdida de privacidad como una consecuencia inevitable del progreso tecnológico, o como el precio que debemos de pagar si queremos evitar el aislamiento social. En una palabra, no sería ya viable oponerse al 'fin de la privacidad' que parece marcar el curso de los tiempos […] Sobre el trasfondo de esta especie de conformismo se explicaría, por ejemplo, que el gran aumento de la preocupación pública en abstracto coincida con la explosión social de fenómenos que comportan serios riesgos para la privacidad, tanto en un plano horizontal, entre los propios ciudadanos, como en el campo de los

[1081] PÉREZ LUÑO. "El derecho al honor y a la intimidad", ob. cit., p. 1075.

[1082] Cfr.HERNÁNDEZ MARTÍN. "La privacidad: una mirada desde la economía" en *En torno a la privacidad y la protección de datos en la sociedad de la información* (Aparicio Vaquero/Batuecas Caletrío coord.), Comares, Granada, 2015, p. 12.

'pequeños grandes hermanos', que ven crecer el uso de sus productos o servicios pese a sus (a veces) escandalosas practicas en materia de privacidad" [1083].

Esto constituye otra de las paradojas de la privacidad, que se ilustra en trabajos como el de MADDEN y RAINIE[1084] que recogen como, a pesar de las revelaciones recientes acerca de los programas de vigilancia de distintos gobiernos (caso *Snowden* o *WikiLeaks*, por ejemplo) o los ataques informáticos a ordenadores de compañías públicas y privadas (como el que se produjo en 2017 con el virus *WannaCry*) así como las prácticas abusivas de las empresas privadas (como el caso de *Cambridge Analytica*), el 91% de los ciudadanos no ha introducido recientemente ningún cambio en su comportamiento relacionado con el uso de Internet y las nuevas tecnologías por lo que la demanda de privacidad no se traduce en conductas efectivas para conseguirla con los medios disponibles. Conclusiones similares se extrajeron del último estudio publicado por la Comisión Europea[1085] y cuyos resultados respaldaron la elaboración del GDPR, en concreto, la instauración del principio general "*privacy by design*" y "*privacy by default*".

13.7 De los retos futuros, el *Blockchain* y el impacto de género del derecho al olvido

Por último, reconociendo el valor jurídico del derecho al olvido y una vez puestos de relieve algunos de sus puntos débiles, procede preguntarse si éste, junto con las medidas propuestas con el conjunto de la regulación de datos a la que viene aparejada, serán herramientas eficaces para hacer frente a los nuevos retos futuros más inmediatos[1086]. Como ya

[1083] MUÑOZ SORO/ OLIVER-LALANA. Derecho y cultura de protección de datos. Un estudio sobre la privacidad en Aragón, Dykinson, Madrid, 2012, p. 39.

[1084] MADDEN / RAINIE. "Americans' attitudes about privacy, security and surveillance", en *Pew Research Center*, 2015. Disponible online en: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

[1085] EUROPEAN COMISSION. "Public Opinion on Future Innovations, Science and Technology", en *Eurobarometer Qualitative Study*, 2015. Disponible online en: http://ec.europa.eu/commfrontoffice/publicopinion/archives/quali/ql_futureofscience_en.pdf

[1086] Así, por ejemplo, el escenario descrito en este trabajo parece tener inevitables consecuencias desde el punto de vista del derecho a la competencia, en el cuál podría preguntarse si, a raíz de la irrupción del mercado digital deben establecerse pautas nuevas o repensar los objetivos tradicionales de las leyes *antitrust* de los mercados tradicionales. Así, podría proponerse, por ejemplo, reevaluar el nivel de eficiencia perjudicial, lo que conllevaría a una política activa de intervención en los mercados contra los abusos de dominación en relación con los macrodatos. Del mismo modo, podría reconsiderarse

se ha visto, la tecnología puede consistir en si misma una limitación para el cumplimiento efectivo de determinados derechos y, a ello, debe añadírsele su carácter evolutivo constante, lo que puede ocasionar una fugacidad en la efectividad de las medidas jurídicas adoptadas.

Este es el caso que parece plantear la tecnología del *Blockchain*, fundamentada sobre una base de datos distribuida y cifrada, construida a partir de cadenas de datos diseñadas para eludir su modificación y el contenido de las cuales es visible para todos, cuyo éxito se basa en carencia de intermediarios que certifiquen la autenticidad de los datos contenidos y las transacciones que puedan llevarse a cabo a partir de éstos.

Las transacciones llevadas a cabo a través de esta tecnología se almacenan en un registro de datos que no puede ser modificado posteriormente, pues cada dato introducido en el bloque se vuelve único, irrepetible e inmutable. Se necesita el consenso de todas las partes implicadas para actualizar dichas cadenas de datos de forma que una transacción posterior pueda enmendar o cambiar la anterior, pero sobre su base en forma de concatenación, por lo que nunca llega a desaparecer la información introducida en la cadena de datos. Cada operación se une a la cadena de bloques, en relación con la transacción anterior y la posterior, con una serie de algoritmos criptográficos que aseguran su integridad.

Mediante su funcionamiento, se construyen registros inquebrantables, imposibles de modificar sin dejar huellas, motivo por el cual esta tecnología está transformando los procesos de negocios en general y de la banca y las aseguradoras en particular, pues su aplicación se ha extendido en los servicios financieros, popularizándose en el uso de *Bitcoins* -los usos corporativos más comunes están asociados a las criptomenadas- y expandiéndose hacia otros sectores, principalmente a través de los *smarts contracts*, como las telecomunicaciones o a industria de la salud.

El conflicto pues, se produce cuando una información registrada en uno de tantos bloques de datos contenga información personal y un individuo decida ejercitar su derecho al

---

cuáles son los criterios que deben determinar la posición dominante en los mercados digitales, especialmente en conexión con el uso de los datos personales y la discriminación de los competidores.

olvido frente a dichos datos, pues la publicidad de sus registros es inherente a la lógica de su funcionamiento[1087]. La característica básica de la tecnología del *Blockchain* es su inmutabilidad pues ciertamente, es esta inalterabilidad la que dota de confianza y veracidad a todo el sistema.

El GDPR resulta perfectamente extensible al *Blockchain*, pues sus postulados son aplicables con independencia de la forma en que se almacenen los datos, del mismo modo en que la información que contienen las cadenas de datos, pese a no identificar a sus titulares directamente, pues se trata de una sucesión de caracteres, sí que los hace identificables a través del rastreo de las operaciones, lo que deriva asimismo en una materia sometida al influjo del Reglamento de datos.

Sin embargo el *Blockchain* parece del todo incompatible con el GDPR pues la eliminación de cualquier dato integrante en la enorme cadena que forman los distintos bloques, es directamente contraria a la idiosincrasia propia de dicha tecnología, pues parece descartable la posibilidad de reconstruir una cadena de datos después de haberse suprimido determinados datos que la integraban. Además de ello, la propia tecnología supone una limitación para el ejercicio del derecho al olvido, pues una vez la información se inserta dentro de los bloques y las cadenas de datos, ésta ya no puede suprimirse.

Así las cosas, debe de buscarse con la mayor prontitud una solución jurídica que permita resolver una eventual petición de derecho al olvido ante una cadena de datos, así como establecer previsiones ante posibles colisiones de intereses. Podrían adoptarse distintas soluciones en este sentido, en función de los intereses políticos o jurídicos que se quieran preponderar, desde limitar el alcance del derecho al olvido por parte de las legislaciones nacionales en los sistemas *Blockchain* en base a las previsiones del artículo 23 GDPR, hasta obligar al encriptado de la información personal que haga identificable al sujeto, antes de incluirla en el sistema *Blockchain* de modo que eliminar la clave de descifrado equivaldría a destruir los datos, o al menos su acceso publico.

[1087] Ello también plantea numerosos problemas jurídicos desde el punto de vista de los consumidores y usuarios si se piensa, por ejemplo, en cómo puede llevarse a cabo el ejercicio del derecho de desistimiento en el *Blockchain*.

Una tercera opción sería rediseñar los software y trasladar la información almacenada mediante *Blockchain* a bases de datos tradicionales que, permitan sin duda identificar a los sujetos y, al mismo tiempo, garantizar el borrado de los datos personales cuando así se solicite, sin embargo, ello supondría acabar con los beneficios del *Blockchain*. Ciertamente, el conflicto creado a tenor del *Blockchain* resulta cuanto menos paradójico, pues su finalidad es dotar a los sujetos de un verdadero control sobre sus datos, dada la transparencia que facilita y la imposibilidad de que se produzcan cambios aleatorios o fraudulentos, logrando así llevar a cabo transacciones sin intermediarios que puedan influenciar en dicho proceso, los bancos por ejemplo, lo que supone una incontestable autonomía para los sujetos.

Pasando a otra de las cuestiones determinantes que deben ser abordadas como retos a asumir en el desarrollo del derecho al olvido como derecho fundamental, puede mencionarse la necesidad de incluir en su evolución normativa las reflexiones pertinentes para incluir el impacto de género en su desarrollo legislativo. Sobre esta cuestión, es necesario determinar en primera instancia qué se entiende por el concepto de género, para así considerar la razón que justifique un desarrollo legislativo orientado por los estudios sobre el impacto de género.

Siguiendo los postulados de BUTLER, autora postmoderna que redefine el concepto de género, abandonando el mero tratamiento biológico para darle una nueva dimensión, el género puede considerse como un constructo cultural, esto es, un significado que desborda la propia categorización binaria hombre v. mujer, adentrándose en el proceso de contrucción política, social y cultura de la identidad de la persona. Este proceso vendría a manifestarse en el cuerpo como campo donde se manifiesta el género, sin que éste pueda determinar desde la perspectiva biologicista clásica la opción escogida, en tanto que como se ha dicho lo importante es la construcción cultural de dicha identidad. Esto es lo que lleva a BUTLER a afirmar el carácter performativo del género como parte integrante de la teoría *queer*, mediante la cual se reconoce

la importancia de la subjetividad, de las formas en que la persona se representa y adapta en el medio social, para así respetar el libre desarrollo de su identidad[1088].

La postura de esta autora viene a reforzar una idea clave para el desarrollo del derecho al olvido, *leitmotiv* de la investigación presentada en esta tesis doctoral, que no es otra que la necesaria respuesta que el ordenamiento jurídico debe ofrecer a los cambios propios del medio social. Por esta razón, centrándonos en la necesidad de integrar los estudios de impacto de genero en el desarrollo de la legislación, ésta sería una exigencia derivada de las nuevas corrientes de pensamiento que han venido a resignificar el concepto de género, adoptando una postura mucho más permeable al respeto a las distintas identidades culturales que se derivan de éste. Así las cosas, el propio ideal democrático al que responde el derecho al olvido como derecho fundamental, que no es otro que respetar la libertad de la ciudadanía a partir de la protección de la privacidad en el contexto del *Big data*, inspira también la necesidad de que la evolución del marco legal del derecho al olvido incluya estudios de impacto de género, donde se incorpore un entendimiento del género alejado de la mera categorización en términos binarios, siendo por ello recomendable considerar la teoría *queer* desarrollada por Judith Butler.

Partiendo de estos fundamentos, puede considerarse de qué manera, pese a la importancia de esta cuestión en un Estado democrático de Derecho, la necesaria adecuación del impacto de género en la legislación no ha sido reflejado en el GDPR, dado que sólo se realizan menciones en cuanto a la orientación sexual, en lo relativo a las decisiones automatizadas, o en lo que respecta a los datos sobre la vida sexual cuando se incluye dentro de la denominada categoría especial dentro del tratamiento de datos personales.

Sobre esta cuestión, debe tenerse en cuenta cómo el género supone un contenido con una mayor incidencia en términos cualitativos, dado que responde a sensibilidades mucho más profundas dentro de la esfera personal del sujeto, por lo que se echa en falta un mayor

[1088] Dado que la bibliografía de BUTLER sobre esta cuestión es muy extensa, simplemente se consideran una serie de aportes básicos para entender su pensamiento: *Deshacer el género*, Paidos, D.L., Barcelona, 2006; *El género en disputa: el feminismo y la subversión de la identidad*, Paidos, México, 2001.

tratamiento personalizado de la cuestión en el GDPR, especialmente si consideramos lo novedoso de este cuerpo legal. En este sentido, sorprende la falta de compromiso del Reglamento con el vinculante y complejo principio del *gender mainstreaming*, asumido por la IV Conferencia Mundial sobre la Mujer, dependiente de la Asamble General de Naciones Unidas, celebrada en Beijing en 1995[1089]. Este principio supone integrar la perspectiva de género como corriente principal en las legislaciones, en las políticas y programas de proyectos públicos, con la finalidad de ofrecer un criterio orientador para el desarrollo legislativo de acuerdo con la protección de la igualdad en las políticas públicas. De acuerdo con BARRÈRE, este compromiso supone asumir por las autoridades nacionales la tarea de "apoyar como corriente principal a escala gubernamental una perspectiva de género en todas las políticas y promover una política activa y visible que eleve a corriente principal la perspectiva de género en todas las políticas y programas"[1090].

Así las cosas, la necesidad de incluir el impacto de género en el desarrollo legislativo del derecho al olvido responde a que el género, en sus múltiples facetas, deviene un dato de carácter personal, de contenido altamente sensible, el cual hace identificable a una persona. Sobre esta premisa, y teniendo en cuenta que éste es susceptible de sufrir modificaciones, cabe concluir que ello sería permeable a la acción del derecho al olvido.

Como se ha dicho, la consideración del género como construcción cultural puede ser susceptible de adoptar cambios, por lo que, pudiendo ser parte de la propia identidad de la persona, y en consecuencia de su esfera de privacidad, si el género sufre una variación, los datos relativos al género anterior dejarían inmediatamente de ser exactos y, en base a las potestades de dicha persona, podrá ejercitarse lícitamente el derecho al olvido.

Ello sin embargo, puede presentar numerosos problemas prácticos a la hora de demostrar algunos extremos, como puede ser el hecho de que se haya producido efectivamente un cambio

[1089] Cfr. GIL RUIZ. "Nuevos instrumentos vinculantes para una ciencia de la legislación renovada: impacto normativo y género", *Anales de la Cátedra Francisco Suárez*, 47, 2013, p. 18.

[1090] Cfr. BARRÈRE. "La interseccionalidad como desafío al *mainstreaming* de género en las políticas públicas", *Revista Vasca de Administración Pública*, nº 87-88, 2010, pp. 40-41.

de género, cuando ello puede no conllevar ninguna exteriorización verificable a tal efecto, o que la referencia al mismo permita identificar a dicha persona, así como en relación al interés público que acarreara dicha cuestión o el transcurso del tiempo que pudiera exigirse en su caso.

Pretende evidenciarse con ello como el derecho al olvido tendrá en el futuro múltiples aplicaciones así como conflictos y problemas jurídicos que ahora no son ni siquiera imaginables. La falta de una regulación específica sobre la materia, ocasiona incertidumbre y problemas prácticos en cuanto a la definición de conceptos, la concreción de supuestos de hecho y la precisión de responsabilidades, cuya conflictividad será creciente en tanto que no se dispongan unas pautas mínimas de actuación, al menos, orientadas a facilitar las tareas de los órganos jurisdiccionales. Por ello, consideramos necesario que de cara al futuro el desarrollo legislativo del derecho al olvido incorpore los requeridos estudios sobre el impacto de género, considerando en todo caso éste desde la perspectiva sociocultural presentada en este punto.

14. Recapitulación

I. La realidad social vigente, con los cambios económicos y culturales que en ella han provocado la masificación de Internet y las nuevas tecnologías de la información y la comunicación, ha propiciado la aparición del derecho al olvido como mecanismo de reacción jurídico, debido a la exigencia del Estado social y democrático de Derecho de adecuar sus presupuestos estructurales y su ordenamiento jurídico al cambio de paradigma que ha supuesto la revolución digital y, en especial, el *Big data*.

El derecho al olvido como derecho fundamental, se construye a partir de una *refundamentación* de la privacidad capaz de representar una esfera personal del sujeto libre de injerencias de terceros, mucho más amplia que el tradicional concepto de intimidad y como presupuesto indispensable para el ejercicio de la libertad individual, en tanto que deviene una garantía esencial para la protección de la dignidad y el libre desarrollo de la personalidad, de plena adecuación al nuevo contexto de "modernidad líquida".

Si bien los orígenes remotos del derecho al olvido pueden suscitar discrepancias entre la doctrina, lo cierto es que inevitablemente éstos toman causa en el "*right to be let alone*"

acuñado por la doctrina clásica anglosajona y en el "*right to privacy*" cuya base se adecua a la *refundamentación* presentada en esta disertación. No obstante, la doctrina clásica civilista de la tradición jurídica continental, contiene asimismo principios y derechos que permiten legitimar el derecho al olvido, como la responsabilidad civil por culpa o la prescripción.

La gran proliferación de datos personales ocasionada por las tecnologías del *Big data* así como la memoria virtual y permanente que supone Internet, han propiciado el surgimiento del derecho al olvido frente a las demandas de los ciudadanos ante las distintas prácticas de almacenamiento, procesamiento y transferencia masiva de información personal que han conllevado, en ocasiones, una vulneración del derecho de privacidad. Combatiendo dicha problemática, el derecho al olvido digital permite a los interesados el cifrado y borrado online de sus datos personales cuando éstos sean perjudiciales para sus derechos fundamentales.

II. El derecho al olvido, como la mayoría de derechos fundamentales, tiene su origen en la creación jurisprudencial, concretamente en la sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014, conocido popularmente como *caso Google*, que se ha erigido como el *leading case* en la materia dado que constituye el primer pronunciamiento jurídico acerca del derecho al olvido. A través de dicha resolución, el TJUE reconoció la existencia de un derecho al olvido por vez primera, afirmando como principio general la prevalencia de los derechos fundamentales frente a la tecnología.

También en nuestro sistema jurídico recientemente, han abundado los pronunciamientos jurisprudenciales en torno al derecho al olvido, encontrando sentencias tanto de las Audiencias Provinciales, como de la Audiencia Nacional, el Tribunal Supremo y, más recientemente, el Tribunal Constitucional. Este último, en su sentencia de 4 de junio (STC 58/2018), hace un reconocimiento expreso del derecho al olvido y le atribuye un carácter fundamental y autónomo sobre la base del derecho a la protección de datos personales, la intimidad y el honor, con todas las implicaciones que ello comporta.

No es hasta la publicación del Reglamento europeo de protección de datos personales que el derecho al olvido deja de ser un derecho de creación jurisprudencial para quedar

reconocido expresamente en un instrumento jurídico, el único en vigor hasta la fecha, siendo rebautizado como "derecho de supresión" (artículo 17).

De hecho, su denominación no es pacífica así como tampoco lo es su concepto, pues, por una parte, el único texto jurídico que lo regula hasta la fecha ofrece una concepción relativamente abierta y, de otra, su carácter novedoso lo sitúa como un concepto todavía en evolución. Sin embargo, en la presente tesis doctoral se propone una definición del derecho al olvido como el derecho al borrado digital de hechos pasados que tiene toda persona que se haya sentido vulnerada en su derecho a la privacidad, debido a causas justificadas o porque con el paso del tiempo sus datos personales han perdido su virtualidad, con independencia del perjuicio efectivamente causado o de si éstos son exactos o ciertos.

III. Pese a que el soporte jurídico del derecho al olvido es relativamente reciente y en la actualidad tiene una virtualidad propia, su origen y pretexto se sitúa en el derecho fundamental a la protección de datos personales cuyo reconocimiento es más amplio y sirve de base para el derecho al olvido.

Así, en el ámbito doméstico, el derecho a la protección de datos se inserta en el artículo 18.4 CE tal y como ha confirmado reiteradamente la jurisprudencia constitucional, pese a no estar reconocido expresamente. Del mismo modo, viene desarrollado en la Ley Orgánica de Protección de Datos de Carácter Personal, cuyo proyecto de reforma, actualmente en tramitación parlamentaria, hace expresa mención al derecho al olvido, lo que supondría su primer reconocimiento en un texto legislativo nacional.

Igualmente son múltiples los instrumentos jurídicos supraestatales dedicados a la protección de los datos personales y la privacidad, que devienen vinculantes para nuestros órganos jurisdiccionales en base al artículo 10.2 de la Constitución, destacando entre ellos, la Declaración Universal de los Derechos Humanos, el Convenio Europeo de Derechos Humanos, el Convenio 108 del Consejo de Europa y los distintos Tratados de la UE.

IV. En cuanto a su naturaleza jurídica, un examen en profundidad permite categorizar el derecho al olvido dentro de las cuatro posiciones clásicas que sistematizan los derechos dentro

de la doctrina pues, ciertamente, puede concluirse que se trata de un derecho humano, fundamental, subjetivo y de la personalidad. Así, se configura dentro de los derechos humanos de última generación, en tanto que se construye sobre las necesidades e intereses del ser humano como un todo, dentro del contexto actual, reconfigurando los derechos y libertades de las anteriores generaciones para hacer frente a la "contaminación de las libertades".

El derecho al olvido también es un derecho fundamental en tanto que así lo ha determinado el Tribunal Constitucional y, fundamentalmente, porque al configurarse como garantía de la privacidad, protege en última instancia el libre desarrollo de la personalidad. Partiendo de la base de que las violaciones de la privacidad suponen en último término una vulneración de la libertad, el ordenamiento jurídico exige que los presupuestos legales de la libertad sean desarrollados por la vía de los derechos fundamentales.

El derecho al olvido es, asimismo, un derecho subjetivo dado que viene integrado por una doble garantía, en primer lugar, dotando a su titular de un contenido prestacional para su ejercicio, permitiéndole obtener el borrado digital de sus datos personales cuando se den las circunstancias para ello y, en segundo lugar, porque garantiza a su titular una esfera libre de injerencias en su privacidad. Este contenido subjetivo se puede predicar frente a los poderes públicos así como frente a las relaciones jurídico-privadas, dada la eficacia horizontal del derecho al olvido, originada por la situación privilegiada de oligopolio de las corporaciones de Internet y su capacidad de condicionamiento en las personas, en base a la doctrina *vis expansiva de los derechos*.

Finalmente, siguiendo la doctrina civilista clásica, puede sostenerse que el derecho al olvido es un derecho de la personalidad pues su finalidad última es la protección de la integridad personal del ser humano y de su propia identidad pese a que, por su peculiar naturaleza, no puede afirmarse con total rotundidad su estatus como límite a la autonomía de la voluntad ni su carácter indisponible, pues goza en cierto modo de un contenido patrimonial.

V. En cuanto a la titularidad activa del derecho al olvido, ello no plantea ninguna duda respecto de las personas individuales, pues a diferencia de las condiciones para su ejercicio o la

extensión de su contenido, el derecho de supresión es predicable respecto de todas las personas físicas por igual. En cuanto a las personas jurídicas, se ha desarrollado una construcción jurídica que permite defender la titularidad del derecho al olvido por éstos, principalmente en base a su conexión con otros derechos como el honor, derivándose así de la jurisprudencia del Tribunal Constitucional, quedando en todo caso excluidas las personas jurídico-públicas.

También se ha discutido la aplicabilidad del derecho al olvido sobre las personas fallecidas afirmando que, contrariamente al principio civilista por el cual la muerte del sujeto de derecho extingue los derechos de la personalidad, esta posibilidad resulta predicable respecto del derecho al olvido, permitiendo que los herederos puedan solicitar la supresión de los datos del fallecido sin más limitaciones que las establecidas por ley o cuando el difunto lo hubiere prohibido expresamente.

En cuanto al sujeto pasivo del derecho al olvido, se reafirma nuevamente la capacidad de ejercitarlo frente a las personas jurídico-privadas, ya se trate de los propietarios y administradores de una App o dominio web, o de un motor de búsqueda, los cuales tienen una legitimación procesal pasiva reconocida tanto por la jurisprudencia del TJUE como por el GDPR, pese a que se haya dictado jurisprudencia contradictoria por el Tribunal Supremo.

VI. El objeto del derecho al olvido tiene un carácter poliédrico, siendo integrado por un conglomerado de derechos fundamentales que interaccionan entre sí, colisionando en ocasiones entre ellos. Así, si bien la privacidad es el bien jurídico protegido por éste, se insertan también en él, el derecho al honor, a la propia imagen, a la intimidad, a la protección de datos personales, así como a la dignidad y al libre desarrollo de la personalidad.

Así, el derecho al honor encuentra su vínculo con el derecho de supresión en tanto que permite al sujeto preservar su fama o reputación, del mismo modo que puede afectar a la intimidad cuando un determinado dato personal incida en el ámbito más resguardado de una persona, o al derecho a la propia imagen en tanto que ésta constituye un elemento personal que permite identificar a un individuo. Indudablemente el derecho a la protección de datos fundamenta de forma directa el derecho de supresión en tanto que este último se acciona para el

borrado digital de una determinada información personal. Por último, el derecho al olvido protege en última instancia la dignidad personal y el libre desarrollo de la personalidad de su titular dado que, de un lado, permite al sujeto configurar libremente su privacidad y, de otro, dichos derechos actúan como pilar ontológico para la existencia del resto de libertades.

Finalmente, el derecho al olvido está íntimamente relacionado con la libertad de expresión y comunicación, las cuales operan fundamentalmente como limitación a su contenido.

VII. El derecho al olvido no permite a los sujetos configurar un pasado a su medida ni alterar libremente su identidad digital, sino que dota a su titular de un poder de control sobre sus datos personales, permitiéndole salvaguardar su privacidad. Se le reconoce así un contenido tanto objetivo como subjetivo dado que permite a su titular salvaguardar una esfera libre de injerencias y, asimismo, otorga a su titular de un control sobe sus datos (*habeas data*).

En cuanto al alcance del derecho al olvido, frente a lo que dispuso la jurisprudencia en un origen, se sostiene su efecto multidireccional, permitiendo tanto la desindexación de los enlaces por parte de los motores de búsqueda en relación con los resultados obtenidos a partir de la introducción de los nombres y apellidos de una persona, como el borrado de los datos personales accionado directamente frente a las webmaster fuente, de acuerdo con el *principio de responsabilidad proactiva* del GDPR.

VIII. Aunque se configura como una suerte de regla general, el derecho al olvido no es absoluto, sino que para salvaguardar la garantía y la coherencia de todo el ordenamiento jurídico, es susceptible de delimitaciones e intromisiones. Se contemplan expresamente limitaciones al derecho de supresión en base a un tratamiento de datos personales que sea necesario para ejercer el derecho a la libertad de expresión e información, para el cumplimiento de una obligación legal o en aras del interés público, con fines de investigación científica, histórica o estadística, así como para la formulación, ejercicio o defensa de reclamaciones.

Se ha tratado en profundidad la eventual colisión entre el derecho al olvido y la libertad de expresión e información, la cual debe de resolverse mediante a un ejercicio de ponderación

entre ambos intereses jurídicos, cuyo resultado variará en función de las circunstancias concretas de cada caso. Respecto de los factores que deben tenerse en cuenta para llevar a cabo dicho ejercicio hermenéutico destacan, la naturaleza privada o pública del sujeto en cuestión, el carácter público o privado de la información así como el interés público para la opinión general en una sociedad democrática, el tiempo transcurrido desde la publicación de una determinada información, el interés legítimo del responsable del tratamiento, la tecnología disponible y el coste de su aplicación.

Así, la doctrina constitucional en torno a las limitaciones del derecho a la libertad de expresión e información, pese a que presenta ciertos paralelismos con la situación aquí examinada, ha quedado obsoleta por la nueva coyuntura digital, principalmente debido a la invalidación de la veracidad como elemento de ponderación y a la incorporación del factor tiempo como ingrediente esencial de dicho examen hermenéutico.

Por último y como regla general, el principio de buena fe y la prohibición del abuso del derecho, comprendidos en el artículo 7 del Código Civil, actúan asimismo como límites del derecho al olvido en tanto que tienen un alcance general sobre el ordenamiento jurídico.

IX. La protección del derecho de supresión, puede dar lugar a distintas reacciones jurídicas, esto es, a una tutela constitucional, penal, civil o contencioso-administrativa. Sobre la construcción anterior del carácter fundamental del derecho al olvido, se sostiene la posibilidad de recurrir en amparo ante el Tribunal Constitucional así como se afirma su directa aplicación y su tutela en base a un procedimiento basado en los principios de preferencia y sumariedad.

En cuanto al procedimiento habitual para la tutela del derecho al olvido, éste puede ejercitarse por el titular o una entidad, organización o asociación constituida a tal efecto, directamente frente al editor del contenido web de origen o frente al motor de búsqueda, empleando sus propios formularios o solicitando por escrito y de manera motivada, los datos que desean suprimirse. Transcurrido el plazo previsto sin obtener respuesta o siendo ésta negativa, el interesado podrá interponer una reclamación ante la autoridad de control que dictaminará su decisión, a su vez, susceptible de recurso ante los Tribunales.

Asimismo, el GDPR parece facultar a los sujetos para que directamente, mediante demanda civil, soliciten el borrado de determinados datos personales ante los órganos jurisdiccionales. Así las cosas, se echa en falta una ley de desarrollo que contemple detalladamente el proceso a seguir para el ejercicio del derecho al olvido así como que proporcione una regulación unitaria del mismo, acabando con la pluralidad procedimental actual.

En cuanto a la protección penal del derecho al olvido, ello no se refleja expresamente en su legislación que, sin embargo, sí que tutela la esfera de privacidad de los sujetos en base a determinados tipos delictivos contenidos en los artículos 197 y siguientes del Código Penal relativos al descubrimiento y revelación de secretos, así como los artículos 205 y 208 CP referentes al delito de calumnias y de injurias, para la protección del derecho al honor.

El derecho al olvido, aunque no siempre de forma expresa, tiene reconocido también un ámbito supranacional de garantía en cuanto a la esfera de privacidad del sujeto se refiere, cuya protección viene sustentada por el Reglamento europeo de protección de datos así como por el Convenio Europeo de Derechos Humanos, la Carta de Derechos Fundamentales de la Unión Europea y demás tratados y acuerdos internacionales sobre la materia.

X. Por lo que respecta a la responsabilidad en caso de vulneración del derecho al olvido, los daños y perjuicios que se causen mediante el almacenamiento, tratamiento, difusión o publicidad de unos determinados datos susceptibles de ser protegidos por el derecho al olvido, deben de compensarse al afectado por quien los haya causado. Las lesiones que eventualmente puedan producirse serán resarcidas con independencia de la relación existente o la ausencia de vínculo previo entre aquél que produce el daño y aquél que lo sufre. Igualmente se compensará tanto el daño material como el moral.

La responsabilidad civil en el ámbito de Internet y su interacción con las nuevas tecnologías, plantean muchos problemas jurídicos y de determinación de responsabilidades. Asimismo, ésta puede tener su origen en una responsabilidad contractual (cuando, por ejemplo, el afectado haya aceptado las condiciones generales de un determinado producto o servicio) o

en una responsabilidad extracontractual (derecho de daños en un sentido estricto) la cuál tiene lugar con independencia de la presencia de una obligación anterior entre dichos sujetos, pues deriva del deber general de no ocasionar daño a los demás. Respecto del derecho al olvido, el mecanismo jurídico para el resarcimiento de los daños y perjuicios que pueda ocasionar su vulneración se remite fundamentalmente al mecanismo de la responsabilidad extracontractual puesto que, entre el perjudicado y el causante del daño, no suele haber una vinculación contractual previa, como ocurre con las vulneraciones del derecho al olvido llevadas a cabo por los motores de búsqueda.

XI. El Código Civil dispone con carácter general el régimen de responsabilidad civil aunque éste ha sido ampliado notoriamente mediante la legislación especial, entre ellos, el Reglamento europeo de protección de datos. El GDPR regula varias vías a través de las cuales una persona puede obtener la tutela de su derecho al olvido a consecuencia de una infracción, principalmente pueden distinguirse dos, pudiendo el interesado acudir alternativa o conjuntamente a una autoridad de control o a los órganos jurisdiccionales para la defensa de sus derechos, o dirigiéndose éste directamente frente al responsable o al encargado del tratamiento. El Reglamento, también permite que el interesado sea representado por una entidad, organización o asociación sin ánimo de lucro, para el ejercicio de algunos de sus derechos.

Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción de sus disposiciones, tendrá derecho a recibir del responsable o del encargado del tratamiento, según corresponda, una indemnización por los daños y perjuicios sufridos, incluyendo tanto los perjuicios patrimoniales como los morales. El GDPR dispone respecto del responsable, un régimen de responsabilidad objetiva, mientras que el encargado sólo responderá de los daños y perjuicios causados cuando intervenga culpa o negligencia.

Ante el incumplimiento de las disposiciones del Reglamento, cada autoridad de control tiene facultades para imponer, de forma individual, multas administrativas efectivas, proporcionadas y disuasorias, cuya cuantía oscila en función de las circunstancias concretas,

pudiendo llegar hasta un máximo de 20.000.000 euros o hasta el 4% del volumen de negocio total anual.

XII. En segundo lugar, se ha examinado la normativa reguladora de los servicios de la sociedad de la información y de comercio electrónico, esto es, la Directiva 2000/31/CE y la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE) en tanto que establecen las obligaciones y responsabilidades de los prestadores de servicios que lleven a cabo actividades de intermediación como las de transmisión, copia, alojamiento y localización de datos en Internet, incluyendo bajo su normativa a los motores de búsqueda.

Los supuestos de exoneración de responsabilidad a los proveedores de servicios que realicen copias temporales de datos, alojen o almacenen éstos, ha sido objeto de múltiples interpretaciones jurisprudenciales, debido a que la falta de un conocimiento efectivo acerca de la ilicitud o lesión de la actividad o la información de tratamiento de datos, permite eludir responsabilidades. A tenor de la STJUE del caso *Google*, en la que se afirmó que los motores de búsqueda efectúan un tratamiento de datos y, en consecuencia, les resulta aplicable la legislación relativa a la protección de datos personales, se ha pasado a considerar a éstos como sujetos responsables del tratamiento, no siendo aplicable lo dispuesto en la normativa reguladora de los servicios de la sociedad de la información cuyo objeto, principalmente, quedaría limitado a los supuestos de tratamiento ilícito de datos personales.

XIII. En tercer lugar, la responsabilidad civil también viene comprendida en 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. Su examen se ha tenido en consideración en tanto que, en ocasiones, una vulneración del derecho al olvido puede conllevar igualmente una violación del derecho al honor, a la intimidad o a la propia imagen, debido a la intrínseca relación existente entre dichas figuras por lo que, los daños y perjuicios que de ello se deriven, se dirimirán por lo dispuesto en dicha norma.

Entre las vías que dicha ley establece para que los afectados puedan recabar la tutela judicial frente a las intromisiones ilegítimas en sus derechos al honor, intimidad o propia imagen, se encuentra la indemnización de los daños y perjuicios causados y la apropiación por el perjudicado del lucro obtenido con la intromisión ilegítima en sus derechos.

A la hora de determinar las indemnizaciones por daños y perjuicios, la LOPDH presupone siempre la existencia de perjuicio ante una intromisión ilegítima. Asimismo, contempla expresamente la inclusión del daño moral en la compensación pecuniaria.

XIV. Debe distinguirse el derecho al olvido de aquéllas otras categorías jurídicas afines con las que mantiene un nexo común debido a los bienes jurídicos que protegen o a los mecanismos de garantía que incorporan. Entre ellos se encuentra el derecho de cancelación, cuya finalidad es garantizar el control de los datos personales de los interesados y cuya regulación se inserta dentro de la LOPD. Sin embargo, en el GDPR, se hace una completa omisión del derecho de cancelación que, según se entiende, ha sido reemplazado por el derecho de supresión.

El derecho de cancelación y el derecho al olvido tienen un contenido muy similar, de hecho, parece que, bajo la fórmula "derecho de supresión" se ha modernizado la figura clásica de la cancelación, adaptándola a las circunstancias actuales que exige el contexto del *Big data* y la interacción de Internet. Esto explicaría la ausencia del derecho de cancelación en el Proyecto de Ley Orgánica de Protección de Datos, que vendría sustituido por el derecho de supresión. Así, parece que con el empleo de una denominación distinta, se ha querido resaltar la novedad y las virtudes de una figura jurídica que, sin embargo, ya preexistía en nuestro entorno jurídico pero que, dadas las circunstancias del medio en el que debía ejercitarse, había perdido cierta virtualidad.

Por el momento, ambas figuras coexisten en la legislación doméstica pudiendo, no obstante, resaltarse algunas diferencias entre éstas. Así, mientras que el derecho de cancelación debe ejercitarse frente al responsable del fichero de la entidad que se trate, el derecho al olvido permite dirigirse indistintamente, frente al responsable o gestor de una página o contenido web,

o frente a un motor de búsqueda que indexe dicha información. Por otra parte, mientras que el derecho al olvido se erige como una regla general, negándose su eficacia sólo en casos excepcionales en los que prevalece un interés superior, el derecho de cancelación sólo puede accionarse cuando concurran los supuestos tasados.

XV. El derecho al olvido también encuentra puntos de conexión con el derecho de oposición, pese a que pueden apreciarse notables diferencias entre ambas figuras jurídicas, principalmente en relación a la extensión de su contenido pues, a diferencia del derecho de supresión, el derecho de oposición sólo permite al sujeto impedir una determinada finalidad del tratamiento de sus datos personales y no su borrado o desaparición total.

Asimismo, los supuestos por los que puede ejercitarse el derecho de oposición están tasados legalmente y otorgan al sujeto afectado la carga de la prueba acerca de la concurrencia de los requisitos exigidos, a diferencia del derecho al olvido, que no está condicionado a la existencia de daños o vulneraciones de derechos, correspondiéndole al responsable del tratamiento probar la necesidad de que unos datos no deben ser borrados.

Las diferencias existentes entre ambas figuras hacen de ellas dos herramientas jurídicas para preservar el derecho a la protección de datos personales, lo que explica su coexistencia en el GDPR que ha mantenido el derecho de oposición en su artículo 21.

XVI. Se aprecia asimismo una relación entre el derecho al olvido y el derecho de rectificación, cuya regulación específica se encuentra en la Ley Orgánica 2/1984, de 26 de marzo, sobre el Derecho de Rectificación (LODR).

El GDPR contempla asimismo el derecho de rectificación digital pero su configuración no parece adaptarse a las circunstancias del contexto del *Big data* e Internet, lo que plantea muchos problemas dado que la idiosincrasia del propio medio supone un límite en si mismo para lograr una efectiva rectificación. Así, su pervivencia en el Reglamento sólo se explica por su aplicabilidad práctica en concretos y reducidos supuestos jurídicos, fundamentalmente asemejados con los que pueden identificarse en los medios de comunicación más tradicionales.

La coexistencia de ambas figuras jurídicas se debe a las divergentes finalidades para las que ambas han sido concebidas. Si bien el derecho de rectificación busca restablecer la exactitud o veracidad de una determinada información divulgada así como la reputación o el honor de una persona, el derecho al olvido persigue preservar la privacidad del interesado, pese a que los datos publicados sean exactos o veraces, pues su objetivo es limitar la difusión universal e indiscriminadas de información personal.

XVII. En este último Capítulo, se ha creído oportuno llevar a cabo algunas consideraciones críticas acerca del derecho al olvido, así como realizar algunas aportaciones adicionales a la investigación. Principalmente, se ha querido reflexionar acerca de la creación del derecho al olvido como solución idónea frente al contexto presentado, debatiendo la estrategia adoptada por el GDPR que, en lugar de extender el contenido y garantía del derecho de cancelación, ha preferido crear una nueva figura jurídica, suponemos, como estategia para enfatizar el cambio de paradigma al cual se enfrenta el Derecho.

Asimismo, se ha razonado acerca de la capacidad del derecho al olvido de proporcionar una solución legal al problema subyacente de la cuestión, eminentemente de tipo estructural. La arquitectura propia de Internet junto con la reticencia de los gobiernos de adoptar una política claramente intervencionista en la materia y la permisividad de ciertos comportamientos abusivos de las empresas privadas del *Big data* que mercadean con la privacidad, impiden afirmar de forma rotunda la posibilidad efectiva de borrar todo rastro personal de Internet.

XVIII. En cuanto al rol activo exigido al sujeto afectado para el ejercicio del derecho al olvido, no parece muy garantista el hecho de que se le exhorte a mantener una preocupación, participación y ejercicio activo para conseguir la garantía de sus derechos fundamentales, pues ello requiere de una serie de conocimientos técnicos así como una dedicación personal, poco deseables para la protección de un derecho fundamental en un Estado de Derecho. No parece oportuno trasferir la responsabilidad de la protección del derecho al olvido a los propios usuarios sino que, por el contrario, las aplicaciones y los instrumentos tecnológicos del contexto *Big data* deberían funcionar de manera transparente, permitiendo a los ciudadanos un

control completo sobre sus datos personales y asegurando por defecto la garantía de las libertades colectivas e individuales.

De lo contrario, en tanto que los verdaderos garantes de la privacidad son los propios interesados, quienes deben de llevar a cabo conductas de autoprotección, ello requiere asimismo de un alto nivel de concienciación social en la materia, por lo que la cultura de protección de datos exige una dimensión fundamental para reivindicar y obtener las garantías adecuadas en materia de derechos fundamentales en lo que se ha denominado "responsabilidad tecnológica".

XIX. Como se ha visto, la ponderación entre bienes jurídicos en conflicto resulta recurrente en materia de derecho al olvido. Sin embargo, se cuestiona la transmisión de la responsabilidad de dicha decisión, en primera instancia, a los motores de búsqueda, cuyo criterio puede ocasionar la adopción de decisiones que no conlleven un verdadero ejercicio de búsqueda del equilibrio de los bienes en juego, en tanto que se trata de empresas privadas cuyos intereses son eminentemente particulares, por lo que las decisiones que tomen pueden fácilmente responder a objetivos viciados por su subjetividad propia.

Las críticas acerca del juicio de ponderación se extienden, asimismo, a los órganos jurisdiccionales en tanto que se considera excesivo el peso que se le otorga a la ponderación en el derecho al olvido, obligando a analizar caso por caso y a poner en valor no sólo hechos subjetivos, sino también intereses sociales e individuales. Las inconcreciones y lagunas del GDPR en esta materia, el abuso de conceptos jurídicos indeterminados así como sus constantes remisiones al desarrollo posterior de las legislaciones domésticas, dificultan las tareas de los tribunales y ocasionan inseguridad jurídica.

Se requiere una propuesta de *lege ferenda* capaz de articular los parámetros concretos que deben enmarcar todo análisis jurisprudencial del derecho al olvido así como la inclusión expresa de éste en el artículo 18 de la Constitución (así como del derecho a la protección de datos), reduciendo el margen de discrecionalidad de los órganos jurisdiccionales en torno a la

configuración del derecho al olvido y cumpliendo con los presupuestos generales del Estado social de Derecho.

XX. Se ha debatido también acerca de la motivación de los cambios legislativos propuestos a raíz del nuevo paradigma así como de las iniciativas públicas al respecto. Se concluye que dichas actuaciones no tienen como fin exclusivo la garantía de la privacidad de los ciudadanos ni la protección de sus derechos sino que, junto a ello, tienen como objetivo asegurar el libre flujo de datos entre los Estados, en un intento de acabar con la competencia desleal.

Ello parece asentarse sobre presupuestos aparentemente contrapuestos y, aunque es innegable que la legislación en materia de protección de datos ha supuesto una ampliación de la garantía de los derechos y libertades de los ciudadanos, cuyo incremento ha sido exponencial en los últimos quince años, se observan muchas contradicciones en torno a las políticas públicas, como acreditan instrumentos como el *Privacy Shield*, lo que hace cuestionarse si la normativa de protección de datos personales está adquiriendo paulatinamente un valor simbólico.

XXI. Se propone la adopción de políticas de privacidad por defecto y desde el diseño, limitando la acción tecnológica para que apriorísticamente se protejan los derechos fundamentales de los ciudadanos sin necesidad de interacción alguna por su parte. Dichas medidas, contempladas expresamente en el GDPR, producen una inversión del proceso de protección de la privacidad, que deja de operar como una reacción del interesado ante la vulneración de sus derechos fundamentales, para llevarse a cabo de manera proactiva y preventiva por quienes diseñan los productos o sistemas que pueden dar lugar a la vulneración de datos personales.

Ello está directamente relacionado con la "*accountability*" y la exigencia de transparencia, previstas asimismo en el GDPR, y que derivan de las demandas sociales y la propia evolución del ordenamiento jurídico. El principio de transparencia, cuya aplicación es transversal, incide en múltiples aspectos tratados en este trabajo, desde el requerimiento a las

corporaciones del *Big data* para que descubran la lógica algorítmica empleada para el tratamiento de los datos personales, hasta la necesidad de lograr una claridad y sencillez en sus prácticas de contratación en masa, así como en sus políticas de privacidad.

XXII. Una de las mayores paradojas de *posmodernidad* se produce respecto de la privacidad en tanto que, si bien en el pasado se consideraba al Estado como la mayor amenaza para la salvaguarda de las libertades, frente al cuál surgieron numerosos derechos y libertades capaces de defender a los ciudadanos frente a la injerencia de los poderes públicos, en la actualidad se hace necesario contar con la tutela del Estado para la defensa de prácticamente todas las libertades.

Debido a la posición dominante de las corporaciones del *Big data* y las empresas de Internet así como su capacidad de condicionamiento respecto de los ciudadanos, la exigencia del respeto sus derechos y libertades fundamentales requiere, en todo caso, el apoyo directo y explícito de los poderes públicos.

XXIII. Reflexionando sobre la aptitud de la regulación actual respecto del derecho al olvido para adaptarse a los retos futuros más inmediatos, se interroga acerca de la durabilidad de sus medidas frente a la constante evolución y aparición de nuevas herramientas y aplicaciones tecnológicas. La tecnología del *Blockchain*, fundamentada sobre una base de datos cifrada, construida a partir de cadenas de datos diseñadas para eludir su modificación y el contenido de las cuales es visible para todos, se presenta como un obstáculo a corto plazo. El conflicto se produce cuando una información registrada en uno de tantos bloques de datos contenga información personal y un individuo decida ejercitar su derecho al olvido frente a dichos datos, pues la publicidad de sus registros es inherente a la lógica de su funcionamiento.

Pese a que el GDPR resulta perfectamente extensible al *Blockchain*, ambos fenómenos parecen del todo incompatibles, pues la eliminación de cualquier dato integrante en la enorme cadena que forman los distintos bloques, es directamente contraria a la idiosincrasia propia de su funcionamiento. Incluso la propia tecnología supone una limitación para el ejercicio del

derecho al olvido en este supuesto, pues una vez la información se inserta dentro de los bloques y las cadenas de datos, ésta ya no puede suprimirse.

Otra de las cuestiones que se ha destacado es la omisión en el GDPR del impacto de género en su legislación. Además de otras consideraciones políticas y democráticas, la necesidad de incluir el impacto de género en el desarrollo legislativo del derecho al olvido responde a que éste, en sus múltiples facetas, deviene un dato de carácter personal, de contenido altamente sensible, el cual hace identificable a una persona. Sobre esta premisa, y teniendo en cuenta que el género es susceptible de sufrir modificaciones en tanto que se trata de una construcción cultural, se afirma la posibilidad de ejercitar lícitamente el derecho al olvido puesto que configura la identidad de la persona y, en consecuencia, afecta a su esfera de privacidad.

XXIV. El derecho al olvido tendrá en el futuro múltiples aplicaciones así como conflictos y problemas jurídicos que ahora no son ni siquiera imaginables. La falta de una regulación específica y unitaria en la materia comporta serios problemas de inseguridad jurídica, así como numerosas dificultades prácticas, muchas de ellas en aspectos tan esenciales como definiciones de conceptos, concreción de los supuestos de hecho así como la precisión de las responsabilidades que de su incumplimiento se derivan.

Esta conflictividad no cesará, sino todo lo contrario, mientras no se dispongan unas reglas sólidas para el ejercicio del derecho al olvido así como que se unifiquen criterios, al menos respecto de las pautas de actuación de los órganos jurisdiccionales. El desarrollo del derecho al olvido exige contemplar como mínimo los aspectos fundamentales en torno a éste y que han sido abordados a lo largo de la presente disertación, siendo deseable además, que se dispongan mecanismos que permitan afrontar escenarios futuros.

CONCLUSIONES FINALES

A lo largo de los capítulos que componen esta tesis doctoral se han expuesto, de forma particularizada y con la mayor exhaustividad posible, tratando de establecer las conexiones pertinentes, las conclusiones obtenidas a partir de la discusión presentada en el desarrollo de la investigación. Ahora, en este apartado de conclusiones finales, serán puestos de relevancia los insumos cosechados por este estudio en su conjunto.

I. Vivimos en una época de continua expansión tecnológica, donde la revolución digital ha producido un cambio sustancial en las pautas de comportamiento de la ciudadanía. En este estado de cambio constante, la técnica no se detiene, y el conocimiento deviene vanguardia o anacronismo de forma acelerada. En lo que se ha denominado como "modernidad líquida", se produce un cambio radical en la cohabitación humana, en el condicionamiento social de las políticas de vida.

En este contexto, cada uno de los movimientos en la Red genera información que se digitaliza en código binario y se almacena masivamente para, con técnicas de lo más complejas, analizarlos y extraer nuevas referencias que en el futuro puedan aplicarse a la transformación del mundo real. Este proceder supone un uso y tratamiento masivo de datos destinados a inferir, a partir de su análisis, nuevas percepciones o indicadores, los cuales tienen una dimensión valorativa o axiológica que puede servir como fundamento para la transformación de los mercados, organizaciones o entes, e incluso la propia forma de relacionarse entre el Estado y la ciudadanía.

II. Así las cosas, llamamos *Big data* al almacenamiento, tratamiento y transferencia de datos a gran escala a través de las tecnologías de Internet. En la globalización del siglo XXI, las innovaciones tecnológicas junto con el nuevo modelo económico y social, han hecho proliferar enormes cantidades de bases de datos relativos a realidades tangibles (datos físicos) o intangibles *a priori* pero convertidos mediante algoritmos en información digital. Entre los unos y los otros hay un número muy elevado de datos de carácter personal. La relevancia de

estos datos masivos no sólo afecta a cuestiones directa e indirectamente vinculadas a nuestra privacidad, sino que tiene una trascendencia que abarca la propia configuración del tejido social.

III. En este sentido, el *Big data* no sólo trata de acumular datos, sino de interrelacionarlos entre sí para lograr aumentar exponencialmente la información a obtener y sacarle así un mayor rendimiento. Este proceso ha sido denominado como *agregación*: conformar el perfil de una persona a través de la triangulación y organización de la información que se ha obtenido sobre ella, obteniendo así nuevos datos sobre un individuo. La filtración de los datos (*data mining*) permite cruzarlos atendiendo a los parámetros que para su finalidad concreta resulte interesante y la información obtenida vuelve a almacenarse de nuevo en otras bases de datos, compartimentadas según los criterios empleados y a las que llamamos bancos de datos. Posteriormente, se completa el proceso con el denominado *reality mining*, esto es, la técnica consistente en procesar datos masivos procedentes de dispositivos móviles para extraer inferencias y predicciones sobre el comportamiento humano.

IV. En las prácticas del *Big data* como fenómeno de transformación social, es indudable la posición de preeminencia asumida por el cálculo algorítmico. Sobre esta cuestión, la utilización del algoritmo ha sido defendida desde la neutralidad asignada al pensamiento científico, en tanto que lenguaje perfectamente codificado mediante el uso de las matemáticas como vehículo, cuando, en realidad, está impulsado por la posición dominante adoptada por la hegemonía del pensamiento neoliberal en las sociedades capitalistas o por el interés de control de determinados aparatos de Estado. En este sentido, no puede considerarse el *Big data*, ni tampoco su desarrollo mediante el cálculo algorítmico, como una realidad social neutra, en tanto que pese a su carácter científico-técnico, la forma de orientar esta evolución, por ejemplo respecto al valor monetario atribuido a los datos masivos, muestra una opción ideológica concreta. Este propósito de desnaturalizar una posición ideológica no es más que una demostración de que todo proceso social se encuentra orientado por un marco de referencia ideológico concreto.

V. Por mucho que los algoritmos puedan responder a razonamientos matemáticos, consecuencia de una lógica científica, esto no obsta para que puedan tener determinados sesgos o limitaciones cuando traspasan el ámbito del *deber ser ideal* propio del pensamiento científico, para aplicarse en el *ser conflictivo* de los procesos sociales. Sobre esta cuestión, se ha discutido la posibilidad de establecer variables relacionadas, por ejemplo, con el nivel económico o la procedencia social de los sujetos destinatarios del cálculo algorítmico. Aunque este planteamiento pueda presentarse como un criterio técnico, sin ningún ánimo discriminatorio respecto de sus destinatarios, resultan innegables los riesgos de que este tipo de prácticas puedan terminar en un simplificador y reduccionista proceso de etiquetaje de la ciudadanía y de la persona en función de su acceso a los recursos. En consecuencia, existirá el peligro de que se produzca un proceso de catalogación respecto de determinados colectivos, a partir de prácticas discriminatorias de tipo social o económico, que puedan dar lugar a una segregación o exclusión de los grupos afectados. En definitiva, la creación de lo que se ha dado en llamar una *sociedad de clases digital*.

VI. Así las cosas, impera la necesidad de impugnar aquellas formas de pensamiento que, amparadas en la técnica o la neutralidad, suponen una limitación de la capacidad crítica al asentarse en valores que se presentan como inmutables y que, por tanto, deben ser aceptados con una confianza que se torna ciega. En este estado de cosas, se hace del todo necesaria una verdadera discusión pública sobre los límites de esta vida basada en el algoritmo, no buscando el rechazo completo del modelo, sino de aquellas cuestiones que puedan cercenar el libre desarrollo de la personalidad del individuo y de sus expresiones sociales.

De acuerdo con lo expuesto, esta posibilidad sería especialmente asfixiante en el ámbito de las ciencias jurídicas. No únicamente por la propia dinámica de reforma del ordenamiento jurídico en base a las necesidades sociales, sino también en la propia aplicación práctica de las normas legales por los órganos jurisdiccionales. En este sentido, si consideráramos como irrefutable cualquier predicción desarrollada de acuerdo con el cálculo algorítmico, existirían dudas sobre la posibilidad de afirmar el libre albedrio como característica inherente del ser humano.

VII. Sobre esta cuestión, ha sido criticada la posibilidad de normalizar, a partir de los postulados del *Big data*, una nueva cultura de la vigilancia de acuerdo con lo que se ha denominado como *Dataveillance*.

A partir del concepto de *panóptico digital*, siguiendo las sucesivas aportaciones en materia de filosofía del control social de BENTHAM, FOUCAULT y HAN, se ha rechazado la posibilidad de establecer nuevos espacios de control y vigilancia basados en la sensación de *control permanente* propia de lo que se ha denominado como *sociedad de la transparencia* o *sociedad de la exposición*. En el nuevo contexto propio de la revolución digital, especialmente si consideramos el papel de preeminencia de las redes sociales, aparece una nueva forma de vigilancia donde destaca la ausencia de poder coactivo sobre el supervisado, en tanto que son los vigilados quienes aceptan de forma *voluntaria* dicho papel (por desconocimiento, por indiferencia o por condicionamiento extorsionador para el acceso *gratuito* –o incluso oneroso– a bienes o servicios). Esto ocurre como consecuencia del tratamiento masivo de datos personales, cedidos voluntariamente por la ciudadanía para el acceso a determinadas aplicaciones, o por el propio fetichismo digital de las redes sociales.

VIII. De acuerdo con lo expuesto, será del todo necesaria la construcción de herramientas jurídicas que permitan que este nuevo hábitat de vigilancia pueda, al menos, atender a un estándar mínimo de protección de la privacidad. Cuando los pasos que damos en el mundo digital pueden suponer una observación perpetua, es necesario dotarse de instrumentos para proteger los derechos de los ciudadanos que, obligados por las propias dinámicas sociales, se prestan *voluntariamente* para ser parte de este *panóptico digital*. Por esta razón, el desarrollo del derecho al olvido como derecho fundamental supone una necesidad imperante en el avance de la ciencia jurídica, en tanto que ésta requiere de una adaptación al contexto expuesto, para así garantizar la seguridad jurídica y la protección de los derechos y libertades de la ciudadanía.

IX. Por lo que respecta a la mercantilización de los datos personales en el contexto *Big data*, puede hablarse de una expropiación de la privacidad sin precedentes. Los datos personales se han convertido en un activo patrimonial de gran valor económico en el Mercado, el petróleo del siglo presente, ellos orientan el desarrollo y uso de nuevos productos y servicios.

La obtención de información personal cuenta con dos grandes aliados, de una parte las nuevas herramientas tecnológicas y, de otra, la fragmentación legislativa o incluso la desregulación, lo que da rienda suelta al mercadeo de datos personales sin demasiados problemas.

Estos dos factores han convertido a la privacidad en el producto estrella a comercializar por las grandes corporaciones del *Big data*. El negocio resulta más que rentable: los usuarios ceden gratuitamente sus datos personales a empresas que se dedican a almacenarlos, venderlos a terceros o procesarlos para un tratamiento posterior, generalmente con objetivos de marketing. En este punto, puede destacarse la actividad de los *data brokers*, empresas que se encargan directamente de hacer negocio con la privacidad, son vendedores de información que se dedican a recolectar datos de los consumidores (la mayoría de veces sin su consentimiento) y vendérselos a un tercero.

X. Así las cosas, las corporaciones de Internet y los operadores de telecomunicaciones tienen una capacidad de condicionamiento sobre los usuarios sin precedentes que, colateralmente, se traduce en una supresión progresiva de la privacidad por medio de la entrega de servicios falsamente gratuitos que imponen unilateralmente cláusulas abusivas respecto de los datos personales de sus usuarios. En consecuencia, los usuarios de estos servicios ya no son consumidores pasivos sino que, a través de una pérdida considerable de la privacidad, se convierten en parte del producto cuya ganancia, sin embargo, no perciben. Sin ser del todo conscientes se ha evolucionado del Internet de las cosas al Internet de las corporaciones, donde las cosas son las personas y en el que los datos personales son el nuevo producto a comercializar. A ello se le une la disposición, a veces ineludible, de los ciudadanos para entregar sus datos personales a distintas corporaciones, sean éstas comerciales, aplicaciones gratuitas o redes sociales. En este escenario, se ha considerado indispensable repensar el concepto de privacidad para adecuarlo a la necesaria protección de la esfera personal del sujeto.

XI. Para la *refundamentación* del concepto de privacidad propuesta en esta trabajo, se ha partido de la confrontación entre las nociones de intimidad y vida privada, que se torna en complementariedad a partir de la comprensión dialéctica de ambos conceptos. Esta confrontación comprensiva permite *refundamentar* la privacidad en unos términos que sean

asumibles para establecerla como presupuesto metodológico en orden al desarrollo del derecho al olvido digital. En este apartado de las conclusiones se pretende desarrollar cómo se ha articulado esta comprensión entre ambos conceptos.

Por un lado, la intimidad se circunscribe al ámbito más personal del individuo, al reducto de cada ser humano libre de toda injerencia externa y en que se fraguan las decisiones más particulares e intransferibles, desarrollándose la propia personalidad en toda su extensión. La privacidad, por su parte, aunque también integra un ámbito de protección del individuo libre de injerencias externas, comprende una esfera de protección mucho mayor en tanto que supera el perímetro circunscrito de lo estrictamente íntimo para abarcar otras conductas y facetas cotidianas y personales sujetas al control de la soberanía individual. A diferencia de la intimidad, el ámbito de protección de la privacidad es flexible y está sujeto a cambios pues depende del contexto, de las pautas de comportamiento e interacción respecto de un lugar, de unas costumbres o de unas necesidades individuales y sociales.

Así, la intimidad es el ámbito en el que el individuo ejerce plenamente su autonomía personal, el confín último de la personalidad, donde uno es plenamente soberano para decidir sus formas de comportamiento social, privado o público. Y la privacidad puede presentar diversas características según la naturaleza de las relaciones interpersonales que se desenvuelvan en dicho ámbito –así, cuanto más connotaciones públicas adquiera el papel que un individuo desempeñe en la sociedad, menor será la esfera de su vida privada–, constituyéndose por reglas de convivencia que tienden a preservar la intimidad personal y se erigen como barreras a la invasión de lo público.

Podría decirse que, mientras que el derecho a la intimidad se relaciona con el poder que cada individuo tiene para controlar la injerencia externa en su esfera más íntima, el derecho a la privacidad permite controlar el acceso, el alcance y la difusión de los demás a ese dominio íntimo. Igualmente, mientras que la intimidad es necesaria para salvaguardar la autonomía personal y el libre desarrollo de la personalidad, la privacidad abarca una dimensión mayor en el contexto de las relaciones interpersonales, proporcionando un espacio libre para llevar a cabo una multiplicidad de actos entre los que se incluye el intercambio de información personal. De

este modo, intimidad y privacidad son realidades distintas aunque relacionadas y tienen un objetivo común: la ausencia de difusión -resguardarse de la publicidad no deseada-, reservando al individuo una parcela libre de toda injerencia.

Así las cosas, se ha desarrollado un concepto de privacidad encuadrado en la propia realidad social derivada del *Big data*. En este sentido, se ha reconocido de qué manera la revolución digital y tecnológica ocasiona riesgos para la protección de la esfera personal del sujeto que, sin penetrar necesariamente en su estricta intimidad, sí inciden en su ámbito de privacidad. De acuerdo con lo expuesto, entendemos la privacidad como aquella esfera personal, integrada por informaciones y comportamientos no íntimos, que el individuo desea que sólo sean conocidos por él o por determinadas personas con las que voluntariamente quiera compartirlos, sustrayendo su conocimiento a grupos más amplios de la sociedad.

XII. En el contexto del *Big data*, la privacidad viene referida a la esfera de libertad que todo ser humano tiene respecto de sus datos de carácter personal, información que, si bien no en todas las ocasiones puede lesionar su intimidad, afecta a otra esfera menos restringida pero igualmente protegida por el Derecho. En consecuencia, debe abandonarse la concepción tradicional de la vida privada como un *status* negativo, pues la protección de la privacidad sin duda es un derecho activo de control, de defensa si se prefiere, que permite a cada individuo controlar el ámbito de privacidad deseado, concediéndole asimismo herramientas efectivas para reaccionar frente a cualquier intrusión.

De este modo, la estrecha conexión que liga el derecho a la autodeterminación informativa con el derecho a la intimidad no tiene por qué traducirse en una concepción individualista de ésta, en la medida en que la propia intimidad ha dejado de ser un privilegio del hombre aislado para devenir en un valor constitucional de la vida comunitaria. Lo que se pretende es reconocer la pluralidad de manifestaciones que tiene la esfera privada, concediendo a todas ellas protección jurídica, cuyo contenido no obstante, variará de mayor a menor, en función de la cercanía al núcleo más íntimo de la personalidad.

Las circunstancias sociales, culturales e históricas aconsejan ampliar el concepto y la garantía de lo privado desde la "intimidad" hacia la "privacidad", en una concepción unitaria y global. De acuerdo con lo expuesto, la *refundamentación* propuesta en este trabajo supone emplear el término "privacidad", de forma consciente y en contraposición al concepto de "intimidad", pues se entienden integradas sus garantías dentro del entendimiento ofrecido a la privacidad.

Sería ésta la delimitación conceptual sobre la que se establecen los presupuestos metodológicos de este trabajo, siendo la *refundamentación* de la privacidad propuesta en esta tesis doctoral la que se enuncia y caracteriza en los términos expresados en el apartado siguiente de estas conclusiones finales, donde se establece la exigibilidad de su contenido como una demanda necesaria para la protección del libre desarrollo de la personalidad en un Estado social y democrático de Derecho.

XIII. El concepto de privacidad propuesto en este trabajo se integra dentro de una realidad social compleja, como lo es la "modernidad líquida" y la mutabilidad que conlleva, en tanto que origina en la sociedad una sensación permanente de volatilidad, lo que verdaderamente supone incertidumbre y claro está, inseguridad jurídica. En este ámbito, el *Big data* ha supuesto un cambio de paradigma en la protección de la esfera personal del sujeto, siendo por tanto necesario desarrollar un propuesta doctrinal coherente que armonice la protección de los derechos y libertades de la ciudadanía con este nuevo estado de cosas. Reconociendo ésta como una de las muchas realidades conflictivas resultantes de la *posmodernidad*, la postura adoptada no supone negar el uso de los datos masivos, pues este escenario, además de ser irreversible, puede ser beneficioso para la ciudadanía, siempre que su desarrollo se encuentre inspirado por los presupuestos estructurales de un Estado social y democrático de Derecho.

Se trata de un nivel de exigencia definitorio de la *refundamentación* de la privacidad presentada en esta tesis doctoral: para que pueda efectivamente respetarse la esfera personal del sujeto, es necesario el desarrollo de un estándar de garantía desde la protección de los derechos y libertades públicas. Sobre esta cuestión, debe recordarse de qué manera los derechos

fundamentales no responden a valores inmutables, sino que han surgido como respuesta a necesidades sociales de protección en momentos de conflicto social respecto de valores e intereses, como lo es en la actualidad el contexto *Big data*.

En efecto, los derechos fundamentales emergen como respuesta a dichos conflictos, para así garantizar en última instancia el respeto a la dignidad de la persona, a su propia capacidad para desarrollarse de acuerdo con el principio general de libertad. No puede obviarse la necesidad de asegurar el respeto a las condiciones materiales que permiten el disfrute de esta libertad de forma plena, o dicho de otro modo, no es lo mismo el reconocimiento formal de una libertad que la posibilidad real de ejercerla. Difícilmente una persona podrá actuar libremente si no se respeta su capacidad de autodeterminarse en una esfera de actuación o pensamiento, representada por el concepto de privacidad desarrollado en este trabajo.

Ante el conflicto que representa el *Big data* para la protección de la privacidad, se propone la construcción desde los derechos fundamentales de un modelo garantista de derecho al olvido que permita, sin renunciar al disfrute de los avances tecnológicos, proteger dicha esfera de privacidad, libertad en última instancia, de la ciudadanía. Puede decirse que el derecho al olvido como derecho fundamental, es una exigencia derivada del espacio de previsibilidad objetiva que el Estado debe ofrecer a la ciudadanía para conocer los límites en el ejercicio de sus derechos y libertades, pero también las restricciones establecidas ante las posibles injerencias de terceros, como de hecho ocurre en la esfera de la privacidad.

XIV. En el ámbito jurídico del *common law*, concretamente en el ordenamiento jurídico británico, mediante la utilización de la fórmula *right to privacy* se da cobijo a una serie de valores o intereses jurídicos donde quedan recogidas la intimidad y la vida privada, pero también otras cuestiones relacionadas como el derecho al honor o la propia imagen. Asimismo, a partir del *right to privacy* se desarrolla la normativa relativa a la protección de datos personales.

Se trata, sin duda, de un ordenamiento jurídico de referencia que justifica la atención de esta tesis doctoral. En primer lugar se esboza una aproximación a la evolución del llamado

right to privacy, por su idoneidad respecto de los presupuestos metodológicos de este trabajo, dada su cercanía a la *refundamentación* de la privacidad propuesta. En segundo lugar, porque resulta interesante para reforzar el alcance *iuscomparativo* de esta investigación, dado que se ofrece la visión de un ordenamiento propio de la cultura legal anglosajona, tradicionalmente desatendido por la doctrina continental, pese a formar parte del ámbito europeo.

Asimismo, el caso británico permite ejemplificar el carácter evolutivo, no sólo del ordenamiento jurídico, sino del sistema legal en su conjunto, cuando así lo requieren las circunstancias sociales, políticas, económicas e incluso culturales, de cada momento.

XV. El desarrollo del *right to privacy* se encuentra influido por los rasgos inherentes al ámbito jurídico del *common law*. Su evolución se ha enfrentado a la dicotomía de un ordenamiento jurídico propio de la cultura legal anglosajona que da preeminencia al precedente judicial, y a la influencia cada vez mayor del positivismo jurídico como consecuencia de la integración en su orden legal de la normativa comunitaria.

A ello se le añade el hecho de que el Reino Unido no cuente con una Constitución escrita, sino con lo que se ha llamado "*unwritten constitution*", basada en la fuerza vinculante del *common law*, las disposiciones normativas de origen parlamentario y los tratados internacionales. Pero, además, todas estas cuestiones se ven condicionadas por la máxima *rule of law*, el principio de legalidad a partir del cual debe desplegarse un estándar de garantía para la protección y promoción de los derechos y libertades de la ciudadanía.

Este particular orden constitucional permite la mutabilidad de su contenido, la adaptación de sus proposiciones a las cambiantes circunstancias de cada momento histórico. Dicha variabilidad impregna el ejercicio de los derechos y libertades de la ciudadanía, como muestra la evolución del modelo británico de protección de la privacidad.

XVI. El desarrollo del *right to privacy* experimenta una constante evolución en el ordenamiento jurídico británico. Así, puede hacerse mención a la promulgación de la *Data Protection Act 1984*, a consecuencia del Convenio del Consejo de Europa de 1981 relativo a la protección de datos personales. Uno de los aspectos clave de esta Ley fue el establecimiento de

los principios fundamentales en los que se debía cimentar toda actuación relacionada con los datos personales, concretados en ocho puntos de contenido muy general. En cuanto a las garantías, consagró por vez primera derechos de información, acceso, rectificación y borrado de datos personales, obligó a aquellos que almacenaban datos personales a inscribirse en un registro específico, creó una autoridad de control independiente para su supervisión (*The Office of the Data Protection Registrar*) e implantó unos órganos jurisdiccionales especiales para tratar asuntos en materia de protección de datos (el *Information Rights Tribunal*), entre otras.

La *Data Protection Act 1984* fue ampliada por la *Data Protecion Act 1998*, donde se incorporaban las exigencias comunitarias de la Directiva 95/46/CE. Ésta última reconoce el derecho a la protección de datos personales como rasgo inherente de la protección jurídica de la intimidad y la vida privada. De igual modo, introduce un sistema adecuado para su garantía, proporcionando herramientas jurídicas a los tribunales que, hasta el momento, sólo concedían exigua protección a la privacidad a través de algunas figuras tradicionales del *common law* como la *breach of confidence*, la *defamation* o la *nuisance*. Si bien reproduce el marco normativo de 1984, incorpora nuevos derechos subjetivos relativos a la protección de la esfera de privacidad del sujeto, como el de acceso y a ser informado respecto de las decisiones automatizadas. Finalmente, establece como regla general la prohibición de exportar datos a terceros países.

XVII. De forma complementaria al desarrollo de las distintas versiones de la *Data Protection Act*, debe hacerse mención a la importancia de la aprobación de la *Human Rights Act 1998*, mediante la cual se incorpora al ordenamiento jurídico británico la declaración de derechos y libertades contenida en el Convenio Europeo de Derechos Humanos. La *Human Rights Act 1998* viene a paliar la ausencia de una *Bill of Rights* en el Reino Unido, convirtiendo en vinculante el contenido del CEDH. En relación con la protección del *right to privacy*, el artículo 8 de la *Human Rights Act 1998* reconoce la protección jurídica de la vida privada y la intimidad.

En este sentido, la HRA establece como prescriptivo que la interpretación de la legislación británica sea realizada conforme a los derechos y libertades reconocidos en el

Convenio, además de la obligatoriedad de los tribunales británicos de interpretar el *right to privacy* de acuerdo con el *case law* del Tribunal Europeo de Derechos Humanos. De este modo, establece un estándar de garantía reforzado respecto de la evolución del *right to privacy* en el ordenamiento jurídico británico.

XVIII. Como último estadio en la evolución del *right to privacy* en Reino Unido, cabe destacar que en la actualidad puede reconocerse una fase de parálisis, correlativa a la incertideumbre vivida con posterioridad al *Brexit*. Sobre esta cuestión, puede destacarse la situación en la que se verá abocado Reino Unido en materia de transferencias internacionales de datos, pues a partir de su desconexión de la Unión Europea, puede pasar a considerarse "tercer estado". Asimismo, los riesgos de que el gobierno británico ceda al euroescepticismo y abandone el Convenio Europeo de Derechos Humanos hacen peligrar el marco legal resultante de la *Human Rights Act 1998*.

En este escenario, la entrada en vigor en 2016 del Reglamento General de Protección de datos (UE 2016/679, el GDPR, por sus siglas en inglés) ha supuesto la redacción por el Gobierno británico de una *Data Protection Bill* para adecuar su contenido a las novedades introducidas en el mismo. En esta reforma, en tramitación parlamentaria durante la redacción de esta tesis doctoral, se aprecia una voluntad por parte del legislador británico de incorporar el estándar europeo de protección de datos personales resultante del Reglamento, incluso pese a la previsible consolidación del *Brexit.* De hecho, la salida de la Unión Europea no significaría el fin de la transferencia de datos entre ambas partes, puesto que una evaluación del nivel de protección de datos en territorio británico, en caso de ser favorable, y así lo sería si se incorpora el GDPR, permitiría considerar el Reino Unido como "país seguro" por parte de la Comisión Europea, permitiendo el flujo de datos entre ambos territorios.

Como opciones alternativas, pueden mencionarse la posibilidad de adoptar las llamadas *Binding Corporate Rules*, opción que se recoge expresamente en el Reglamento europeo pero que, sin embargo, podría comportar ciertos problemas prácticos pues para su adopción, se requiere la autorización previa de todas las agencias nacionales de protección de datos, por lo que dependería del estatus que tenga la ICO británica después del *Brexit*. Alternativamente,

otra solución pasaría por emplear *Standard Form Contracts*, es decir, la autorización de las transferencias internacionales de datos en base a cláusulas contractuales tipo, que se regulan en el artículo 46 del GDPR. Sin embargo, el mismo Reglamento, hace hincapié en la conveniencia de complementar los contratos tipo con otras garantías de protección, pues es consciente de la limitada seguridad jurídica que éstas ofrecen como mecanismo efectivo de control.

XIX. Como se ha reiterado, el derecho al olvido como derecho fundamental, se construye a partir de una *refundamentación* de la privacidad capaz de representar una esfera personal del sujeto libre de injerencias de terceros, mucho más amplia que el tradicional concepto de intimidad y como presupuesto indispensable para el ejercicio de la libertad individual, en tanto que deviene una garantía esencial para la protección de la dignidad y el libre desarrollo de la personalidad, de plena adecuación al nuevo contexto de "modernidad líquida".

Si bien los orígenes remotos del derecho al olvido pueden suscitar discrepancias entre la doctrina, lo cierto es que inevitablemente éstos pasan por el "*right to be let alone*" acuñado por la doctrina clásica anglosajona y del "*right to privacy*" cuya base se adecua a la *refundamentación* presentada en esta disertación. Este último, en tanto que comprende de forma integral las nociones de intimidad y vida privada, presenta cierta afinidad con el concepto de privacidad elaborada en esta tesis doctoral sirviendo, asimismo, como presupuesto para la construcción del derecho al olvido desarrollado en estas páginas.

No obstante, la doctrina clásica civilista de la tradición jurídica continental, contiene asimismo principios y derechos que permiten legitimar el derecho al olvido, como la responsabilidad civil por culpa o la prescripción.

XX. La realidad social vigente, con los cambios económicos y culturales que en ella han provocado la masificación de Internet y las nuevas tecnologías de la información y la comunicación, han reivindicado al Derecho una reacción sustancial acorde con las transformaciones acontecidos, como exigencia misma del Estado social y democrático del

Derecho de adecuar sus presupuestos estructurales y su ordenamiento jurídico al cambio de paradigma que ha supuesto la revolución digital.

La proliferación de datos personales ocasionados por las tecnologías del *Big data* así como la memoria virtual y permanente que supone Internet, han propiciado el surgimiento del derecho al olvido frente a las demandas de los ciudadanos ante las prácticas de almacenamiento, procesamiento y transferencia masiva de información personal que han conllevado, en ocasiones, una vulneración del derecho de privacidad. Combatiendo dicha problemática, el derecho al olvido digital permite a los interesados el cifrado y borrado online de sus datos personales cuando éstos sean perjudiciales para sus derechos fundamentales.

XXI. El derecho al olvido, como la mayoría de derechos fundamentales, tiene su origen en la creación jurisprudencial, concretamente en la Sentencia del Tribunal de Justícia de la Unión Europea de 13 de mayo de 2014, conocido popularmente como *caso Google*, que se ha erigido como el *leading case* en la materia puesto que es el primer pronunciamiento jurídico, mediante el cual el TJUE reconoció la existencia de un derecho al olvido por vez primera, afirmando como principio general la prevalencia de los derechos fundamentales frente a la tecnología.

También en nuestro sistema jurídico han abundado recientemente los pronunciamientos en torno al derecho al olvido, reconocido en sentencias tanto de las Audiencias Provinciales, como de la Audiencia Nacional, el Tribunal Supremo y, últimamente, del Tribunal Constitucional. Este último, en su Sentencia de 4 de junio (STC 58/2018), otorga al derecho al olvido un reconocimiento expreso así como le atribuye un carácter fundamental y autónomo sobre la base del derecho a la protección de datos personales, la intimidad y el honor, con todas las implicaciones que ello conlleva.

No es hasta la citada publicación en 2016 del GDPR, que el derecho al olvido deja de ser un derecho de creación jurisprudencial para quedar reconocido expresamente en un instrumento jurídico, el único en vigor hasta la fecha, siendo rebautizado como “derecho de supresión”. De hecho, su denominación no es pacífica así como tampoco lo es su concepto, ya que su

regulación en ese texto jurídico ofrece una concepción relativamente abierta y, por lo demás, su carácter novedoso lo sitúa como un concepto todavía en evolución. Sin embargo, en la presente tesis doctoral se propone una definición más precisa del derecho al olvido: el derecho al borrado digital de hechos pasados que tiene toda persona que se haya sentido vulnerada en su derecho a la privacidad, debido a causas justificadas o porque con el paso del tiempo sus datos personales han perdido su virtualidad, con independencia del perjuicio efectivamente causado o de si éstos son exactos o ciertos.

XXII. Pese a que el soporte jurídico del derecho al olvido es relativamente reciente y en la actualidad tiene una virtualidad propia, su origen y fundamento se sitúa en el derecho fundamental a la protección de datos personales cuyo reconocimiento es más amplio y por ello mismo, le sirve de base.

Así, en el ámbito doméstico el derecho a la protección de datos se inserta en el artículo 18.4 CE tal y como ha confirmado reiteradamente la jurisprudencia, pese a no estar aludido expresamente en el texto constitucional. Ese derecho viene desarrollado en la Ley Orgánica de Protección de Datos de carácter personal, cuyo proyecto de reforma, actualmente en tramitación parlamentaria, hace expresa mención al derecho al olvido, lo que, de prosperar, supondría su primer reconocimiento en un texto legislativo nacional.

En todo caso, son múltiples los instrumentos jurídicos supraestatales dedicados a la protección de los datos personales y la privacidad, que devienen vinculantes para nuestros órganos jurisdiccionales en base al artículo 10.2 de la Constitución, destacando entre ellos, la Declaración Universal de los Derechos Humanos, el Convenio Europeo de Derechos Humanos, el Convenio 108 del Consejo de Europa y los distintos Tratados de la UE.

XXIII. En cuanto a su naturaleza jurídica, un examen en profundidad permite categorizar el derecho al olvido dentro de las cuatro posiciones clásicas que sistematizan los derechos dentro de la doctrina pues, ciertamente, puede concluirse que se trata de un derecho humano, fundamental, subjetivo y de la personalidad. Así, se configura dentro de los derechos humanos de última generación, en tanto que se construye sobre las necesidades e intereses del

ser humano como un todo, dentro del contexto actual, reconfigurando los derechos y libertades de las anteriores generaciones para hacer frente a la "contaminación de las libertades".

El derecho al olvido también es un derecho fundamental en tanto que así lo ha determinado el Tribunal Constitucional y, esencialmente porque, al configurarse como garantía de la privacidad, protege en última instancia el libre desarrollo de la personalidad y, partiendo de la base de que las violaciones de la privacidad suponen en último término una vulneración de la libertad, nuestro ordenamiento jurídico exige que los presupuestos legales de la libertad sean desarrollados por la vía de los derechos fundamentales.

El derecho al olvido es, asimismo, un derecho subjetivo dado que viene integrado por una doble garantía, en primer lugar dotando a su titular de un contenido prestacional para su ejercicio, permitiéndole obtener el borrado digital de sus datos personales cuando se den las circunstancias para ello y, en segundo lugar, porque garantiza a su titular una esfera libre de injerencias ajenas en su privacidad. Este contenido subjetivo se puede predicar frente a los poderes públicos como frente a las relaciones jurídico-privadas, en base a su eficacia horizontal, ante la situación privilegiada de oligopolio de las corporaciones de Internet y su capacidad de condicionamiento sobre las personas, en base a la doctrina *vis expansiva de los derechos*.

Finalmente, siguiendo la doctrina civilista clásica, puede afirmarse que el derecho al olvido es un derecho de la personalidad pues su finalidad última es la protección de la integridad personal del ser humano y de su propia identidad pese a que, por su peculiar naturaleza, no puede afirmarse con total rotundidad su estatus como límite a la autonomía de la voluntad ni su carácter indisponible, pues goza en cierto modo de un contenido patrimonial.

XXIV. En cuanto a la titularidad activa del derecho al olvido, ello no plantea ninguna duda respecto de las personas individuales, pues a diferencia de las condiciones para su ejercicio o la extensión de su contenido, el derecho de supresión es predicable respecto de todas las personas físicas por igual. En cuanto a las personas jurídicas, se ha desarrollado una construcción jurídica que permite defender la titularidad del derecho al olvido por éstas,

principalmente en base a su conexión con otros derechos como el honor, como se deriva de la jurisprudencia del TC, quedando en todo caso excluidas las personas jurídico-públicas.

También se ha discutido la aplicabilidad del derecho al olvido sobre las personas fallecidas afirmando que, contrariamente al principio civilista por el cual la muerte del sujeto de derecho extingue los derechos de la personalidad, ello sí es predicable del derecho al olvido, siendo posible que los herederos puedan solicitar la supresión de los datos del fallecido sin más limitaciones que las establecidas por ley o cuando el difunto lo hubiere prohibido expresamente.

En cuanto al sujeto pasivo del derecho al olvido, se reafirma nuevamente la capacidad de ejercitarlo frente a las personas jurídico-privadas, tanto frente a los propietarios y administradores de una App o dominio web, como frente a un motor de búsqueda, los cuales tienen una legitimación procesal reconocida tanto por la jurisprudencia del TJUE como por el GDPR, pese a que se ha dictado jurisprudencia contradictoria en el Tribunal Supremo.

XXV. El objeto del derecho al olvido tiene un carácter poliédrico, siendo integrado por un conglomerado de derechos fundamentales que interaccionan entre sí, colisionando en ocasiones entre ellos. Así, si bien la privacidad es el bien jurídico protegido por éste, se integran también en él, el derecho al honor, a la propia imagen, a la intimidad, a la protección de datos personales, así como a la dignidad y el libre desarrollo de la personalidad.

Así, el derecho al honor encuentra su vínculo con el derecho de supresión en tanto que permite al sujeto preservar su fama o reputación, del mismo modo que puede afectar a la intimidad cuando un determinado dato personal incida en el ámbito más resguardado de una persona, o al derecho a la propia imagen en tanto que ésta constituye un elemento personal que permite identificar a un individuo. Sin duda, el derecho a la protección de datos fundamenta de forma directa el derecho de supresión en tanto que este último se acciona para el borrado digital de una determinada información personal. Finalmente, el derecho al olvido protege en última instancia la dignidad personal y el libre desarrollo de la personalidad de su titular dado que, de

un lado permite al sujeto configurar libremente su privacidad y, de otro, dichos derechos actúan como pilar ontológico para la existencia del resto de libertades.

En otro orden que es necesario apostillar, el derecho al olvido también está íntimamente relacionado con otros derechos, esto es, la libertad de expresión y de comunicación, que operan fundamentalmente como limitación a su contenido.

XXVI. El derecho al olvido no permite a los sujetos configurar un pasado a su medida ni alterar libremente su identidad digital, sino que dota a su titular de un poder de control sobre sus datos personales, permitiéndole salvaguardar su privacidad. Se le reconoce así un contenido tanto objetivo como subjetivo dado que permite a su titular salvaguardar una esfera libre de injerencias, y le otorga un control sobre sus datos (*habeas data*).

En cuanto al alcance del derecho al olvido, frente a lo que dispuso la jurisprudencia en un origen, se sostiene su efecto multidireccional, permitiendo tanto la desindexación de los enlaces por parte de los motores de búsqueda en relación con los resultados obtenidos a partir de la introducción de los nombres y apellidos de una persona, como el borrado de los datos personales accionado directamente frente a las webmaster fuente, de acuerdo con el *principio de responsabilidad proactiva* del GDPR.

XXVII. Aunque se configura como una suerte de regla general, el derecho al olvido no es absoluto, sino que para salvaguardar la garantía y la coherencia de todo el ordenamiento jurídico, es susceptible de delimitaciones e intromisiones. Se contemplan expresamente limitaciones al derecho de supresión en base a un tratamiento de datos personales que sea necesario para ejercer el derecho a la libertad de expresión e información, para el cumplimiento de una obligación legal o en aras del interés público, con fines de investigación científica, histórica o estadística, así como para la formulación, ejercicio o defensa de reclamaciones.

Se ha tratado en profundidad la eventual colisión entre el derecho al olvido y la libertad de expresión e información, la cual debe de resolverse mediante un ejercicio de ponderación entre ambos intereses jurídicos cuyo resultado variará en función de las circunstancias concretas de cada caso. Respecto de los factores que deben tenerse en cuenta para llevar a cabo

dicho ejercicio hermenéutico, destacan la naturaleza privada o pública del sujeto en cuestión, el carácter público o privado de la información así como el interés público para la opinión general en una sociedad democrática, el tiempo transcurrido desde la publicación de una determinada información, el interés legítimo del responsable del tratamiento, la tecnología disponible y el coste de su aplicación.

Así, la doctrina constitucional en torno a las limitaciones del derecho a la libertad de expresión e información, pese a que presenta ciertos paralelismos con la situación aquí examinada, ha quedado obsoleta por la nueva coyuntura digital, principalmente debido a la invalidación de la veracidad como elemento de ponderación y a la incorporación del factor tiempo como ingrediente esencial de dicho examen hermenéutico.

Por último y como regla general, el principio de buena fe y la prohibición del abuso del derecho, comprendidos en el artículo 7 del Código Civil, actúan asimismo como límites del derecho al olvido en tanto que tienen un alcance general sobre el ordenamiento jurídico.

XXVIII. La protección del derecho de supresión, puede dar lugar a distintas reacciones jurídicas, esto es, a una tutela constitucional, penal, civil o contencioso-administrativa. Sobre la construcción anterior del carácter fundamental del derecho al olvido, se sostiene la posibilidad de recurrir en amparo ante el Tribunal Constitucional así como se afirma su directa aplicación y tutela conforme a un procedimiento basado en los principios de preferencia y sumariedad.

En cuanto al procedimiento habitual para la tutela del derecho al olvido, éste puede ejercitarse por el titular directamente frente al editor del contenido web de origen o frente al motor de búsqueda, empleando sus propios formularios o solicitando por escrito, y de manera motivada, los datos que desean suprimirse. Transcurrido el plazo previsto sin obtener respuesta o siendo ésta negativa, el interesado podrá interponer una reclamación ante la autoridad de control que dictaminará su decisión, a su vez, susceptible de recurso ante los Tribunales.

Asimismo, el GDPR parece facultar a los sujetos para que directamente, mediante demanda civil, soliciten el borrado de determinados datos personales ante los órganos jurisdiccionales. Así las cosas, se echa en falta una ley de desarrollo que contemple

detalladamente el proceso a seguir para el ejercicio del derecho al olvido y que proporcione una regulación unitaria del mismo, acabando con la pluralidad procedimental actual.

En cuanto a la protección penal del derecho al olvido, ello no se refleja expresamente en la legislación punitiva que, sin embargo, sí que tutela la esfera de privacidad de los sujetos en base a determinados tipos delictivos contenidos en los artículos 197 y siguientes del Código Penal relativos al descubrimiento y revelación de secretos, así como los artículos 205 y 208 CP referentes al delito de calumnias y de injurias, para la protección del derecho al honor.

El derecho al olvido, aunque no siempre de forma expresa, también tiene reconocido un ámbito supranacional de garantía en cuanto a la esfera de privacidad del sujeto se refiere, cuya protección viene sustentada por el GDPR así como por el CEDH, la CDFUE y demás tratados y acuerdos internacionales sobre la materia.

XXIX. Los daños y perjuicios que se causen mediante el almacenamiento, tratamiento, difusión o publicidad de unos determinados datos, deben de compensarse al afectado por quien los haya causado, con independencia de que éstos se deriven de una responsabilidad contractual (cuando el afectado haya aceptado las condiciones generales de un determinado producto o servicio) o de una responsabilidad extracontractual (cuando se origine por el motor de búsqueda, por ejemplo). Este último suele ser el mecanismo más habitual de resarcimiento en el caso del derecho al olvido, pues entre el perjudicado y el causante del daño, no suele haber una vinculación contractual previa.

El Código Civil dispone con carácter general el régimen de responsabilidad civil aunque éste ha sido ampliado notoriamente mediante la legislación especial. Concretamente, el GDPR regula varias vías a través de las cuales una persona puede obtener la tutela de su derecho al olvido, pues quien haya sufrido daños y perjuicios como consecuencia de una infracción de sus disposiciones, tendrá derecho a recibir una indemnización por los daños y perjuicios padecidos, incluyendo perjuicios patrimoniales y morales. Por otra parte, ante el incumplimiento de las disposiciones del Reglamento, cada autoridad de control tiene facultades para imponer, de forma individual, multas administrativas efectivas, proporcionadas y disuasorias.

Otra legislación especial es la relativa a los servicios de la sociedad de la información y de comercio electrónico, esto es, la Directiva 2000/31/CE y la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSICE) que incide de manera acotada. A este respecto, la STJUE del caso *Google* afirmó que los motores de búsqueda realizaban tratamiento de datos en el desarrollo de su actividad, siendo a tal efecto responsables y, en consecuencia, quedando sujetos a la legislación de protección de datos, no siendo aplicable lo dispuesto en la normativa reguladora de los servicios de la sociedad de la información cuyo objeto, principalmente, quedaría limitado a los supuestos de tratamiento ilícito de datos personales.

También debe acudirse a 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 cuando una vulneración del derecho al olvido conlleve, asimismo, una violación de alguno de los derechos que contempla. Entre las vías previstas en esta Ley para resarcir las lesiones al honor, intimidad o propia imagen, se encuentra la indemnización de los daños y perjuicios que se presupone aplicable siempre que exista una intromisión ilegítima, e incluye asimismo el daño moral.

XXX. Se ha distinguido el derecho al olvido de otras figuras jurídicas afines como son el derecho de cancelación, el derecho de oposición y el derecho de rectificación, con las que mantiene un nexo común debido a los bienes jurídicos que protegen o a los mecanismos de garantía que incorporan.

El derecho de cancelación, integrado dentro de los llamados derechos ARCO y regulado en la LOPD, ha sido omitido en la redacción del GDPR pues, según se entiende, queda reemplazado por el derecho de supresión. Dado que el contenido de ambas figuras es muy similar puede decirse que, mediante el derecho de supresión, se ha modernizado la figura de la cancelación, adaptándola a las circunstancias exigidas por el *Big data* y la interacción de Internet. Sin embargo, mientras no se apruebe el Proyecto de Ley Orgánica de Protección de Datos que sigue la tendencia del GDPR, ambas figuras coexisten en el ordenamiento jurídico, pudiendo apreciarse algunas diferencias entre ellas. Así, mientras que el derecho de cancelación debe ejercitarse por el afectado frente al responsable del fichero, el derecho al

olvido puede accionarse indistintamente, contra el responsable o gestor de una página o contenido web, o frente a un motor de búsqueda. Por otra parte, el derecho al olvido se constituye como una regla general, mientras que el derecho de cancelación tiene unos supuestos tasados.

El derecho de oposición diverge del derecho de supresión, principalmente por la extensión de su garantía pues el primero, sólo se manifiesta como la potestad del sujeto de impedir una determinada finalidad del tratamiento de sus datos personales y no a su borrado o desaparición total. Asimismo, los supuestos por los que puede ejercitarse el derecho de oposición están tasados legalmente y otorgan al sujeto afectado la carga de la prueba. Estas diferencias entre ambas figuras, hacen de ellas dos herramientas jurídicas para preservar el derecho a la protección de datos personales, lo que explica su coexistencia en el GDPR.

El derecho de rectificación, contemplado en la Ley Orgánica 2/1984, de 26 de marzo, sobre el Derecho de Rectificación (LODR), ha sido incorporado en el GDPR, sin embargo, su configuración no parece adaptarse al contexto ocasionado por la irrupción de Internet, pues no tiene en cuenta la idiosincrasia propia del nuevo medio, caracterizado por una inmediatez y mutabilidad continua. Su pervivencia en el Reglamento sólo se explica por su aplicabilidad práctica en concretos y reducidos supuestos jurídicos, fundamentalmente asemejados con los que pueden identificarse en los medios de comunicación más tradicionales. Por otra parte, su coexistencia en el GDPR con el derecho al olvido se explica por las divergentes finalidades para las que ambos han sido concebidos pues, mientras que el derecho de rectificación busca restablecer la exactitud o veracidad de una determinada información publicada, el derecho al olvido persigue preservar la privacidad, pese a que los datos publicados sean exactos o veraces.

XXXI. A lo largo del trabajo se presenta el derecho al olvido como un mecanismo eficiente para la solventar los problemas jurídicos originados a raíz del paradigma expuesto, en el que destacan la proliferación de Internet y el empleo masivo de datos por las nuevas tecnologías y las corporaciones del *Big data*. No obstante, se cuestiona la idoneidad de dicha solución legal a un problema que parece ser eminentemente de tipo estructural y que, teniendo en cuenta la arquitectura propia de Internet (con la dificultad técnica, se arguye, de aislar y

borrar todos los rastros de una alusión personal, por ejemplo), el inmovilismo de los Gobiernos que eluden adoptar políticas intervencionistas en la materia y la tolerancia social ante ciertos comportamientos abusivos de las empresas privadas que comercian con los datos personales, cuesta afirmar con rotundidad que se pueda borrar toda información personal de Internet de forma efectiva.

Por otra parte, muchas de las cuestiones tratadas a lo largo de la presente disertación no están exentas de críticas como es el caso de la exigencia al interesado de un comportamiento activo para el ejercicio del derecho al olvido, la privatización del juicio de ponderación en caso de conflicto entre bienes jurídicos, su eficacia respecto a retos jurídicos futuros o inmediatos como el caso del *Blockchain* o los intereses subyacentes de la normativa europea de protección de datos, así como la omisión del impacto de género en dicha legislación.

Un paso más en la garantía de la privacidad, pasa por la adopción de políticas de privacidad por defecto y desde el diseño, que limiten la acción tecnológica para que apriorísticamente los derechos fundamentales de los ciudadanos queden salvaguardados sin necesidad de interacción alguna por su parte. Se trata de provocar la inversión del modelo actual de garantía de la privacidad, de modo que ésta deje de operar como una reacción del interesado ante la vulneración de sus derechos fundamentales para llevarse a cabo de manera proactiva y preventiva por quienes diseñan los productos o sistemas que pueden dar lugar a la vulneración de datos personales. Se trata de generar un escenario que hoy por hoy cuenta con pocos visos de hacerse realidad, dados los intereses que priman, económicos o de control, sobre el almacenamiento y tratamiento de datos.

Asimismo, es exigible una regulación específica y unitaria del derecho al olvido, que precise las condiciones para su ejercicio y su relación con otros derechos afines que puedan interactuar en un mismo supuesto de hecho, acabando así con la disparidad normativa actual y la tendencia a la hiperregulación que, lejos de simplificar, dificulta la garantía jurídica de los derechos fundamentales. Dicha propuesta de *lege ferenda* debe ser capaz de articular los parámetros concretos que deben enmarcar todo análisis jurisprudencial del derecho al olvido siendo deseable, asimismo, la inclusión expresa de éste en el artículo 18 de la Constitución,

junto al derecho a la protección de datos personales. Sólo de esta manera, se logará dotar a los ciudadanos de una mayor seguridad jurídica, al mismo tiempo que se reduce el margen de discrecionalidad de los órganos jurisdiccionales en torno a la configuración del derecho al olvido, cumpliendo con las exigencias propias del Estado social y democrático de Derecho.

XXXII. En esta tesis doctoral se ha pretendido aportar una visión reflexiva y crítica acerca del fenómeno del *Big data* y las nuevas tecnologías, en relación con la defensa de los derechos fundamentales de la ciudadanía y, por ende, sobre su incidencia en el ordenamiento jurídico. El contexto presentado ha evidenciado la necesaria reconstrucción del ámbito de libertad personal de los sujetos, lo que se ha pretendido llevar a cabo a partir de una *refundamentación* de la privacidad, como presupuesto indispensable para la protección de la dignidad y el libre desarrollo de la personalidad en dicho marco.

Desde esta perspectiva, se ha mostrado el derecho al olvido como la réplica ofrecida desde el Derecho al estado de las cosas, en forma de garantía personal que aspira a proteger la privacidad y poner solución a los daños e inconvenientes provocados por las nuevas condiciones sociales derivadas del tratamiento masivo de datos personales. Se reconoce así la importancia del desarrollo del derecho al olvido como derecho fundamental a la vez que se ponen de relieve los problemas y lagunas que se desprenden de su reciente alumbramiento, entre ellos, los debidos a la falta de una regulación unitaria precisa en la materia.

En consecuencia, se concluye que el desarrollo tecnológico no puede ser en ningún caso un argumento legitimador que excuse ciertas vulneraciones de los derechos fundamentales, pues las nuevas herramientas tecnológicas deben respetar los derechos y libertades propias de un Estado social y democrático de Derecho, que debe adoptar los mecanismos necesarios para lograr un progreso tecnológico y social correctamente arbitrados por el ordenamiento jurídico.

FINAL CONCLUSIONS

Throughout the chapters that make up this doctoral thesis, the conclusions obtained from the discussion presented in the development of the research have been expounded, in a fragmented way but as thoroughly as possible, with the goal of establishing the relevant connections. Now, in this section of final conclusions, the inputs gathered by this study as a whole will be organised and put into context.

I. We live in a time of continuous technological expansion, where the digital revolution has produced a substantial change in the behaviour patterns of individuals. In this state of constant change, technology never stops advancing and knowledge becomes leading edge or anachronistic at an accelerated rate. In what has been termed "liquid modernity," a radical change is produced in human cohabitation and in the social conditioning of the politics of daily life.

In this context, each of the movements in the network generates information that is digitised in binary code and massively stored, so that using the most complex techniques, the data can be analysed and new references extracted that in the future can be applied to the transformation of the real world. Thus it involves the massive use and processing of data with the aim of inferring, from their analysis, new perceptions or indicators, which have a value or axiological dimension that can serve as a basis for the transformation of markets, organisations or entities, and even the very way that the state and its citizens relate to each other.

II. What we call *Big Data* refers to the storage, processing and transfer of data on a large scale through Internet technologies. In the globalisation of the 21st century, technological innovations, together with the new economic and social model, have led to the proliferation of an enormous number of databases related to tangible realities (physical data) or intangible *a priori* but converted by algorithms into digital information. Within these databases is found a huge quantity of personal data. The relevance of these massive databases not only affects issues

directly and indirectly linked to our privacy, but also has a transcendence that encompasses the very make up of the social fabric.

III. Accordingly, *Big data* is not only about accumulating data, but also interrelating them in order to exponentially increase the quantity of information and thus secure a greater advantage. This process has been called *aggregation*: shaping the profile of a person through the triangulation and organisation of the information that has been obtained about them, thereby obtaining new information about an individual. The filtering of the data (*data mining*) allows them to be cross-referenced according to the parameters that are appropriate for the specific purpose, and the information obtained is once again stored in other databases, called data banks, and compartmentalised according to the criteria used. Subsequently, the process is completed with so-called *reality mining*, which is the technique of processing massive quantities of data obtained from mobile devices in order to extract inferences and make predictions about human behaviour.

IV. In the *Big data* practices as a phenomenon of societal transformation, the pre-eminent position assumed by the algorithmic calculation is unquestionable. On this question, the use of algorithms has been defended from the neutrality assigned to scientific thought, as a language perfectly codified by the use of mathematics as a vehicle, propelled by the dominant position adopted by the hegemony of neoliberal thought in capitalist societies itself. Accordingly, *Big data*, which is evolving through ever more sophisticated algorithms, cannot be considered as a neutral social reality while at the same time, and in spite of its scientific-technical nature, the manner of directing its evolution (for example, with regard to the monetary value assigned to the massive data banks) exhibits a clear ideological slant. This possibility of distorting an ideological position is nothing more than a demonstration that every social process is guided by a specific ideological frame of reference.

V. As much as algorithms can respond to mathematical reasoning as a result of a scientific logic, this does not prevent them from having certain biases or limitations when they go beyond the scope of the ideal rigor of scientific thought, to be applied in the conflictive heart of societal processes. On this question, the possibility of establishing variables related to

the economic level or the social origin of the target subjects of the algorithmic calculation has been discussed. Although it can be presented as a technical criterion without any discriminatory spirit with regard to its recipients, the risks cannot be denied that this type of practice may end up becoming a mere process of labelling individuals based on their access to resources. Consequently, there is a danger that a labelling process may occur with respect to certain groups, based on discriminatory practices of a social or economic nature, which may result in the exclusion of the affected groups. This process can lead to the creation of a society of digital classes.

VI. Thus there is a need to challenge those forms of thought that, protected by technology or neutrality, involve a limitation of the critical capacity based on values that are presented as immutable, and that therefore must be accepted with a confidence that becomes blind. In this state of affairs, a real public discussion about the limits of this *life based on the algorithm* is absolutely necessary, not seeking the complete rejection of the model, but of those issues that may limit the free development of the personal identity of citizens.

According to the above, this possibility would be especially stifling in the field of legal sciences. This is not only because of the dynamics of reform of the legal system based on social needs, but also on the practical application of legal rules by the jurisdictional bodies. Therefore, if we considered as irrefutable any prediction developed according to an algorithmic calculation, there would be doubts about the possibility of affirming free will as an inherent characteristic of the human being.

VII. On this issue, criticism has been levelled against the possibility of normalising, based on the postulates of *Big data*, a new culture of surveillance in accordance with what has been called *Dataveillance*.

From the concept of a *digital panopticon*, following the successive contributions in the philosophy of social control by BENTHAM, FOUCAULT and HAN, the possibility of establishing new monitoring and surveillance spaces based on the sensation of *permanent monitoring*, characteristic of what has been dubbed the *society* of *transparency* or *the society of*

exhibition. In the new context of the digital revolution, especially if we consider the preeminent role of social networks, a new form of surveillance appears, highlighting the absence of coercive power over the monitored, while they themselves voluntarily accept this role. This occurs as a result of the mass processing of personal data, voluntarily given by the public in exchange for access to certain applications, or by the digital fetishism of social networks, as shown by the approach taken by the Spanish penal system regarding the offense of glorifying terrorism on social networks.

VIII. According to the above, it will be absolutely necessary to build legal tools that allow this new environment of surveillance to at least meet a minimum standard of privacy protection. When the steps we take in the digital world can involve perpetual observation, it is necessary to equip ourselves with instruments to protect the rights of individuals who, forced by their own social dynamics, voluntarily lend themselves to be part of this *digital panopticon*. For this reason, the development of the right to be forgotten as a fundamental right involves an imperative need in the advancement of legal science, insofar as it requires an adaptation to this new context in order to guarantee legal security and the protection of the rights and freedoms of the public.

IX. As regards the commercialisation of personal data in the *Big data* context, we can speak of an unprecedented expropriation of privacy. Personal data has become a proprietary asset of great economic value in the market, the petroleum of the current century, which guides the development and use of new products and services. The collection of personal information has two great allies: on one hand, the new technological tools and, on the other, legislative fragmentation or even deregulation, which gives free rein to the marketing of personal data without too many restraints.

These two factors have turned privacy into the flagship product to be marketed by the large *Big data* corporations. The business is more than profitable: users freely provide their personal data to companies that are dedicated to storing them, selling them to third parties or processing them for later analysis, usually with marketing objectives. On this point, we can highlight the activity of data brokers, companies whose objective is to make money from our

privacy by collecting data from consumers (most times without their consent) and selling them to third parties.

X. With this in mind, Internet corporations and telecommunication operators have an unprecedented capacity for constraining users that, collaterally, translates into the progressive suppression of privacy through the delivery of services that are falsely free of charge and that impose unilaterally abusive clauses regarding the personal data of its users. As a result, users of these services are no longer passive consumers but, through a considerable loss of privacy, become part of the product whose profitability, however, they do not perceive. Without Internet users being fully aware of what has happened, the *Internet of things* has morphed into the *Internet of corporations*, in which the *things* are people and where personal data is the new product to be marketed. To this is added the arrangement, sometimes unavoidable, for individuals to deliver their personal data to different corporations, be they online businesses, free applications or social networks. In this scenario, it becomes essential to rethink the concept of privacy in order to adapt it to the necessary protection of the personal sphere of the individual.

XI. To develop the *refoundation* of the concept of privacy proposed in this work, we have started from the confrontation between the notions of intimacy and private life, which become complementary with the dialectic understanding of both concepts, which allows for the *refoundation* of privacy in terms that are acceptable to establish it as a methodological underpinning for the development of the right to be digitally forgotten. At this point in the conclusions, we will examine how this understanding has been formulated between the two concepts.

Intimacy is confined to the most personal area of the individual, to the stronghold of each human being free of all external interference and in which the most personal and non-transferable decisions are forged and the individual develops their own personality in its entirety. Regarding privacy, however, although it also incorporates a protective environment for the individual free from external interference, this sphere of protection is much greater in that it exceeds the circumscribed perimeter of the strictly intimate to encompass other daily and

personal facets and behaviours subject to the control of individual sovereignty. Unlike intimacy, the scope of privacy protection is flexible and subject to change because it depends on the context, the behaviour patterns of a place, of customs or of social needs.

Therefore, intimacy is the area in which the individual fully exercises their personal autonomy, the ultimate stronghold of identity, where one is fully sovereign to decide his or her forms of social, private or public behaviour. Moreover, privacy can exhibit various characteristics depending on the nature of the interpersonal relationships that develop in that area—for example, the more that the role that an individual plays in society acquires public overtones, the smaller the sphere of their private life will be—being composed of rules of coexistence that tend to preserve personal privacy and are erected as barriers against the invasion of the public.

It could be said that while the right to intimacy is related to the power that each individual has to control external interference in their most intimate sphere, the right to privacy provides control over the access, reach and spread of others into that intimate domain. Equally, while intimacy is necessary to safeguard personal autonomy and the free development of personality, privacy encompasses a larger dimension in the context of interpersonal relationships, providing a free space to carry out a multiplicity of acts, among which is included the exchange of personal information. In this way, intimacy and privacy are different but related realities and have a common goal: the absence of dissemination—to avoid unwanted attention—reserving for the individual a space that is free from interference.

Within this context, a concept of privacy has developed that is framed within the very social reality derived from *Big data*. Accordingly, there is some recognition as to how the digital and technological revolution poses risks for the protection of the personal sphere of the individual that, without necessarily penetrating their strict intimacy, does affect the sphere of their privacy. In accordance with the above, we understand privacy as that personal sphere, composed of information and non-intimate behaviours that the individual wishes to be known only by them or by certain people with whom they voluntarily want to share them, removing their knowledge from the wider nuclei of society.

XII. In the context of *Big data*, privacy refers to the sphere of freedom that every human being has with respect to their personal data, information that, although it is not able to harm their intimacy in all cases, does affect another sphere that is less restricted but equally protected by law. Consequently, the traditional conception of private life as a negative *status* should be abandoned since the protection of privacy is undoubtedly an active right of control, or of defence if preferred, that allows each individual to control their desired sphere of privacy, while at the same time providing effective tools to respond to any attack.

In this way, the close connection between the right to informational self-determination and the right to intimacy does not have to be translated into an individualist conception of privacy, insofar as privacy itself is no longer the privilege of the isolated human being and has become a constitutional value of community life. What is intended is to recognise the plurality of expressions that the private sphere possesses, granting all of them legal protection, but whose content, however, will vary from major to minor, depending on the proximity to the most intimate core of the identity. The social, cultural and historical circumstances show us the wisdom of extending the concept and the safeguards of the private from "intimacy" to "privacy" in a unitary and global conception. In accordance with the foregoing, the *refoundation* proposed in this work involves using the term "privacy" consciously and in contrast to the concept of "intimacy," as the safeguards of the latter term are understood as being integrated into the conceptual understanding of privacy.

This would be the conceptual delimitation on which the methodological underpinnings of this work are established, with the *refoundation* of privacy proposed in this doctoral thesis culminated with the provisions of the following section of these conclusions, where the enforceability of its content is established as a legal action necessary for the protection of the free development of personality in a social and democratic state governed by the rule of law.

XIII. The concept of privacy proposed in this work is integrated into a complex social reality, such as "liquid modernity" and the mutability that it entails, as it gives rise to a permanent sense of volatility in society, which no doubt means uncertainty and, of course, legal insecurity. In this arena, *Big data* has brought about a paradigm shift in the protection of the

personal sphere of the individual, and it is therefore necessary to develop a coherent doctrinal approach that harmonises the protection of the rights and freedoms of the public with this new state of affairs. Recognising this as one of the many conflicting realities resulting from *postmodernism*, the adopted position does not mean denying the use of massive databases, because this scenario, besides being irreversible, can be beneficial for the public provided that its development is inspired by the structural assumptions of a social and democratic state governed by the rule of law.

At this point, the *refoundation* of privacy presented in this doctoral thesis could be completed. In order to effectively respect the personal sphere of the individual, it is necessary to develop a protective standard for the safeguarding of public rights and freedoms. On this issue, it can be recalled how fundamental rights do not respond to immutable values, but have arisen as a response to the need for social protection in times of social conflict with regard to values and interests, such as in the context of *Big data*.

Therefore, fundamental rights emerge as a response to such conflicts, in order to ultimately guarantee respect for the dignity of the person and their capacity to develop in accordance with the general principle of freedom. One cannot ignore the need to ensure respect for the material conditions that permit the full enjoyment of this freedom, or in other words, it is not the same to be free as to have the capacity to be free. It is difficult for a person to act freely if respect is lacking for their capacity for self-determination in a personal sphere of action or thought, represented by the concept of privacy developed in this work.

Given the conflict that *Big data* represents for the protection of privacy, this thesis proposes the construction, from the fundamental rights, of a protective model of the right to be digitally forgotten, which permits, without renouncing the enjoyment of technological advances, the protection of this sphere of privacy, of freedom, and ultimately, of citizenry. Accordingly, the right to be forgotten as a fundamental right is a requirement derived from the space of objective predictability that the state must offer to the citizenry to know the limits in the exercise of their rights and freedoms, but also the restrictions established in the face of the

possible infringement of those rights and freedoms by third parties, as would happen in the case of privacy.

XIV. Through the use of the right to privacy formula, it is understood in the legal field of the common law, in particular in the British legal system, as a series of values or legal interests into which intimacy and private life are gathered, but also other peripheral issues such as the right to honour or to one's self-image. Likewise, it is from the right to privacy that the regulations arise related to the protection of personal data.

Accordingly, this work has presented an approach to the evolution of the so-called right to privacy, firstly for its suitability with respect to the methodological underpinnings of this doctoral thesis in its approach to the proposed *refoundation* of privacy. Next, it should prove interesting to reinforce the comparative scope of this research, given that it provides a view of a characteristic structuring of the Anglo-Saxon legal culture traditionally neglected by the continental doctrine, despite being part of the European sphere.

XV. The development of the right to privacy is influenced by the features inherent in the legal sphere of the common law. In this respect, its evolution has faced the dichotomy of a legal system typical of the Anglo-Saxon legal culture, maintaining the dominance of the judicial precedent, which has been subject to a greater influence of legal positivism as a result of the integration of EU regulations into its legal system.

To this must be added the fact that the United Kingdom does not have a written constitution, but functions with what has been called an "unwritten constitution" based on the binding force of common law, legislative acts of parliamentary origin and international treaties. Similarly, all these issues are guided by the rule of law maxim, from which protective standards for the safeguarding and promotion of the rights and freedoms of the public must be deployed

This particular constitutional order permits the mutability of its content and the adaptation of its propositions to the changing social circumstances of each historical moment. This volatility permeates the exercise of the rights and freedoms of the citizenry, as shown by the evolution of the British model of privacy protection.

XVI. The development of the right to privacy is constantly evolving in the British legal system. Thus, mention may be made of the enactment of the Data Protection Act 1984, as a result of the Council of Europe Convention of 1981 relating to the protection of personal data. One of the key aspects of this law was the establishment of the fundamental principles on which all action related to personal data should be based, consisting of eight very general points. As for the safeguards, for the first time it enshrined rights of information, access, rectification and deletion of personal data, required those who store personal data to register in a specific registry, created an independent lead supervisory authority for its supervision (The Office of the Data Protection Registrar) and established special jurisdictional bodies to deal with data protection matters (the Information Rights Tribunal), among others.

The Data Protection Act 1984 was extended by the Data Protection Act 1998, which incorporated the EC requirements of Directive 95/46/EC. The latter act recognises the right to the protection of personal data as an inherent feature of the legal protection of intimacy and privacy. Similarly, it introduces an adequate system for its safeguarding, providing legal tools to the courts that, until that moment, only granted scant protection to privacy through some traditional common law actions such as breach of confidence, defamation or nuisance. Although it reproduces the regulatory framework of 1984, it incorporates new subjective rights related to the protection of the individual's sphere of privacy, as well as integrating new rights of access and the right to be informed about automated decisions. Finally, it establishes as a general rule the prohibition on exporting data to other countries.

XVII. In addition to the development of the different versions of the Data Protection Act, mention may be made of the importance of the adoption of the Human Rights Act 1998 ("HRA"), which incorporates into the British legal system the declaration of rights and freedoms contained in the European Convention on Human Rights ("ECHR"). The HRA made up for the absence of a Bill of Rights in the United Kingdom, making the content of the ECHR binding. In relation to the protection of the right to privacy, Article 8 of the HRA recognises the legal protection of private life and intimacy.

In this regard, the HRA establishes as prescriptive that the interpretation of the British legislation be carried out in accordance with the rights and freedoms recognised in the ECHR, in addition to the obligation on the British courts to interpret the right to privacy in accordance with the case law of the European Court of Human Rights. In this way, it establishes a reinforced standard of protection regarding the development of the right to privacy in the British legal system.

XVIII. As the last stage in the development of the right to privacy in the United Kingdom, it should be noted that, at the present time, a paralysis phase could be recognised, corresponding to the uncertainty experienced after *Brexit*. On this issue one may highlight the situation that the United Kingdom will face with regard to international data transfers, since after its disconnection from the European Union it would be considered a "third party" and face restrictions on the flow of data with the European Union. In addition, the risk of the British government giving in to *Euroscepticism* and abandoning the ECHR jeopardises the legal framework resulting from the Human Rights Act 1998.

Against this backdrop, the recent entry into force of the General Data Protection Regulation (EU) 2016/679 ("GDPR") has involved the drafting by the British government of a Data Protection Bill to adapt its content to the new developments introduced in the regulations. In this amendment, going through parliamentary proceedings during the writing of this doctoral thesis, there appears to be willingness on the part of British lawmakers to incorporate the European standard of personal data protection resulting from the new regulations, despite the strengthening of *Brexit*. In fact, the departure of the UK from the European Union would not mean the end of the transfer of data between both parties, since an evaluation of the level of data protection in British territory, if favourable, and it would be if the GDPR is incorporated into British law, would allow the European Commission to consider the United Kingdom as a "safe country," thereby allowing the flow of data between both territories.

As an alternative option, the possibility of adopting the so-called Binding Corporate Rules can be mentioned, an option that is expressly included in the European regulation. Nevertheless, this could involve certain practical problems because, for its adoption, the prior authorisation of all the national data protection agencies is required, so it will depend on the status that the British Information Commissioner's Office will have after *Brexit*. Alternatively, another solution would be to use Standard Form Contracts, that is, the authorisation of international data transfers based on standard contractual clauses, which are regulated in Article 46 of the GDPR. However, the same regulation emphasises the advisability of supplementing standard contracts with other safeguards, since it recognises the limited legal protection that these offer as an effective control mechanism.

XIX. The right to be forgotten as a fundamental right is based on a *refoundation* of the concept of privacy capable of representing a personal sphere of the individual free from interference by third parties, much wider than the traditional concept of intimacy and as an indispensable presupposition for the exercise of individual freedom, insofar as it becomes an indispensable safeguard for the protection of dignity and the free development of personality, in complete alignment with the new context of "liquid modernity."

While the remote origins of the right to be forgotten may give rise to discrepancies between the doctrines, the fact is that they inevitably pass through the "right to be let alone," coined by the classic Anglo-Saxon doctrine, and the "right to privacy," whose core is adapted to the *refoundation* presented in this dissertation. However, the classic civilist doctrine of the continental legal tradition also contains principles and rights that allow the right to be forgotten to be legitimised, such as civil responsibility through fault or prescription.

XX. The current social reality, with the economic and cultural changes that have fostered the spread of the Internet and the new information and communication technologies, has led to the emergence of the right to be digitally forgotten as a legal mechanism of response, due to the demands of the social and democratic state governed by the rule of law to adapt its structural underpinnings and its legal order to the change of paradigm brought about by the digital revolution and, especially, *Big data*.

The proliferation of personal data caused by *Big data* technologies, as well as the virtual and permanent memory that the Internet involves, has led to the emergence of the right to be forgotten in response to the demands by the public regarding the storage, processing and mass transfer of personal information that have involved, at times, a violation of the right of privacy. Combating this problem, the right to be digitally forgotten allows interested parties to encrypt and delete their personal data online when they are detrimental to their fundamental rights.

XXI. The right to be forgotten, like most fundamental rights, has its origin in the creation of case law, specifically in the CJEU Judgement of 13 May 2014, popularly known as the *Google case*, which was established as the leading case in this matter. This is the first legal pronouncement about the right to be forgotten, in which the CJEU acknowledged for the first time the existence of a right to be forgotten, affirming as a general principle the primacy of fundamental rights over technology.

In the Spanish legal system as well, recent pronouncements regarding the right to be forgotten have abounded, with rulings from the Provincial Courts, the National Court, the Supreme Court and, more recently, the Constitutional Court. The latter, in STC 58/2018 of 4 June, attributes an express recognition to the right to be forgotten, as well as ascribing it a fundamental and autonomous nature, on the basis of the right to the protection of personal data, intimacy and honour, with all the implications that this entails.

It is not until the publication of the GDPR that the right to be forgotten ceases to be a right of jurisprudential creation and is expressly recognised in a legal instrument, the only one in force to date, which has been renamed the "right to erasure" (Article 17 GDPR).

In fact, its name is not peaceful and neither is its concept, because, on the one hand, the only legal text that regulates it to date offers a relatively open conception and, on the other hand, its novel nature establishes it as a still-evolving concept. However, this doctoral thesis submits a definition of the right to be forgotten as the right to the digital erasure of past events, held by every person who has felt violated in a fundamental right due to justified causes or

because, over time, their personal data has lost its essence, regardless of the damage actually caused or whether they are accurate or true.

XXII. Although legal support for the right to be forgotten is relatively recent and currently has its own virtuality, its origin and foundation lie in the fundamental right to the protection of personal data, whose recognition is broader and serves as a basis for the right to be forgotten.

Thus, in the domestic sphere, the right to the protection of data is inserted into Article 18.4 of the Spanish Constitution, as confirmed repeatedly by constitutional jurisprudence, despite not being expressly recognised. Similarly, the right is developed in the Personal Data Protection Act, whose reform bill, currently working its way through the Spanish parliament, makes express mention of the right to be forgotten, which would mean its first recognition in a national legislative text.

There are also multiple supranational legal instruments dedicated to the protection of personal data and privacy that are binding on our jurisdictional bodies based on Article 10.2 of the Constitution, including: the Universal Declaration of Human Rights, the ECHR, Convention 108 of the Council of Europe and various EU treaties.

XXIII. Regarding its legal nature, an in-depth examination makes it possible to categorise the right to be forgotten within the four classic positions that systematise rights within the doctrine, since it can certainly be concluded that it is a right that is fundamental, subjective, human and related to identity. Thus it is set within the latest generation of human rights, while it is constructed on the needs and interests of the human being as a whole, within the current context, reshaping the rights and freedoms of the previous generations to confront the "contamination of freedoms."

The right to be forgotten is also a fundamental right insofar as it has been determined as such by the Constitutional Court and, fundamentally, because by being seen as a safeguard of privacy, it ultimately protects the free development of personal identity. Moreover, on the basis

that violations of privacy ultimately involve a violation of freedom, our legal system requires that the legal underpinnings of freedom be developed by way of the fundamental rights.

The right to be forgotten is also a subjective right, given that it comes bundled with a double protection. Firstly, it provides its holder with a useful tool for its exercise, allowing them to obtain the digital deletion of their personal data when the circumstances arise, and, secondly, it guarantees its holder a sphere free from external interference with regard to privacy. The subjective nature of this right can be argued for both by public authorities and in the face of legal-private relations, based on their horizontal effectiveness, the result of the privileged oligopolistic position of Internet corporations and their capacity for influencing people, based on the doctrine of the expansive view of rights.

Finally, following the classic civilist doctrine, it can be claimed that the right to be forgotten is a right of personal identity since its ultimate purpose is the protection of the personal integrity of the human being and their identity. This is despite the fact that, due to its peculiar nature, its status as a limit on the autonomy of the will or its non-transferable nature cannot be affirmed with absolute certainty, since it enjoys in a certain way a proprietary tenor.

XXIV. Regarding the active ownership of the right to be forgotten, this does not raise any doubt regarding natural persons, because unlike the conditions for its exercise or the extension of its content, the right to erasure is assertable with respect to all natural persons equally. As for non-human legal entities, a legal construction has been developed that permits the assertion of their entitlement to the right to be forgotten, mainly on the basis of its connection with other rights such as honour, derived from the jurisprudence of the constitutional court, excluding in any case public legal entities.

The applicability of the right to be forgotten for deceased persons has also been discussed, affirming that, contrary to the civilist principle by which the death of the rights holder extinguishes the rights of personal identity, the right to be forgotten does apply to the deceased. Hence it is possible that the heirs may request the erasure of the data of the deceased

without further limitations than those established by law or when the deceased person had expressly prohibited it.

Regarding the passive subject of the right to be forgotten, the ability to exercise it against private legal entities is reaffirmed, both against the owners and administrators of an App or web domain, and against a search engine. These have a procedural legitimation recognised both by the jurisprudence of the CJEU and the GDPR, despite the fact that jurisprudence to the contrary has been rendered in the Supreme Court.

XXV. The object of the right to be forgotten has a polyhedral nature, being composed of a conglomerate of fundamental rights that interact with each other, at times colliding with each other. Thus, while privacy is the legal right protected by it, within the right to be forgotten may also be found the right to honour, to one's own image, to privacy, to the protection of personal data, as well as to dignity and to the free development of one's personal identity.

Therefore, the right to honour finds its connection with the right of erasure insofar as it allows the individual to preserve their reputation or acclaim, in the same way that it can affect privacy when a certain piece of personal data affects the most protected area of a person, or the right to one's own image insofar as it constitutes a personal element that identifies an individual. Undoubtedly, the right to the protection of data provides a direct basis for the right of erasure, as the latter is activated by the digital erasure of certain personal information. Finally, the right to be forgotten ultimately protects the personal dignity and free development of the personality of its owner, given that, on the one hand, it allows the subject to freely configure their privacy and, on the other, these rights act as an ontological pillar for the existence of other freedoms.

Finally, the right to be forgotten is closely related to freedom of expression and communication, which operate fundamentally as a limitation on its content.

XXVI. The right to be forgotten does not permit individuals to construct a tailor- made past or freely alter their digital identity, but it does grant the holder some power of control over their personal data, allowing them to protect their privacy. It is thus recognised as both an

objective and a subjective content, in that it allows its holder to safeguard a free sphere of interference, and grants its holder control over their data (*habeas data*).

In terms of the scope of the right to be forgotten, in contrast to what was originally established by jurisprudence, its multidirectional effect has been maintained, allowing both the de-indexing of links by search engines in relation to the results obtained from the introduction of a person's name, as well as the deletion of personal data by acting directly against the source webmaster, in accordance with the *principle of accountability* of the GDPR

XXVII. Although it is set up as a sort of general rule, the right to be forgotten is not absolute, but is susceptible to limitations and encroachments in order to protect the security and coherence of the entire legal system. There are express limitations on the right of erasure based on the processing of personal data that is necessary to exercise the right to freedom of expression and information, for the fulfilment of a legal obligation or for the public interest in terms of scientific research, historical or statistical purposes, as well as for the formulation, exercise or defence of claims.

The possible collision between the right to be forgotten and freedom of expression and information has been dealt with in depth, which must be resolved by means of a weighting exercise between both legal interests, the result of which will vary according to the specific circumstances of each case. Regarding the factors that must be taken into account when carrying out said hermeneutical exercise, one can highlight the public or private nature of the subject in question, the public or private nature of the information, as well as the public interest for general awareness in a democratic society, the time elapsed since the publication of certain information, the legitimate interest of the data controller, and the available technology and the cost of its application.

Thus, the constitutional doctrine regarding the limitations on the right to freedom of expression and information, despite the fact that it has certain parallels with the situation examined here, has become obsolete under the new digital situation, mainly due to the

invalidation of veracity as an element of weighting and the incorporation of the time factor as an essential ingredient of said hermeneutical examination.

Lastly, and as a general rule, the principle of good faith and the prohibition against the abuse of the law, included in Article 7 of the Spanish Civil Code, also act as limits on the right to be forgotten as they have a general application on the legal order.

XXVIII. The protection of the right of erasure can give rise to different legal reactions, that is, to a constitutional, criminal, civil or contentious-administrative tutelage. Regarding the prior construction of the fundamental nature of the right to be forgotten, the possibility of seeking a writ of amparo before the Constitutional Court has been affirmed, as has its direct application and tutelage by means of a preferential and summary procedure.

As for the usual procedure for the protection of the right to be forgotten, this can be exercised by the holder or an entity, organisation or association constituted for that purpose, directly against the publisher of the source web content or against the search engine, using its own forms or by requesting in writing, and in a reasoned manner, the data that they wish to have deleted. If the deadline expires without obtaining a response or if it is negative, the interested party may file a claim with the lead supervisory authority that will issue its decision, which in turn may be appealed before the Courts.

Furthermore, the GDPR seems to empower the subjects so that directly, through a civil suit, they may request the erasure of certain personal data before the jurisdictional bodies. With this in mind, a regulatory decree is lacking that contemplates in detail the process to be followed for the exercise of the right to be forgotten, as well as providing a single regulation over it, ending the current procedural duality. Other issues under debate include the fact that the weighting of legal interests is left in the hands of private interests, or that the affected individuals are given full responsibility for enforcing their rights.

Regarding the criminal protection of the right to be forgotten, this is not expressly reflected in its legislation. However, the law does protect the sphere of privacy of the subjects based on certain types of crime contained in Articles 197, *et seq.* of the Criminal Code relating

to the discovery and disclosure of secrets, as well as Articles 205 and 208 concerning the crimes of slander and libel for the protection of the right to honour.

The safeguards contained in the right to be forgotten, although not always expressly stated, are also recognised as having a supranational scope in terms of the sphere of privacy of the individual, whose protection is supported by the GDPR, as well as by the ECHR, the Charter of Fundamental Rights of the European Union and other treaties and international agreements on the matter.

XXIX. Damages caused by the storage, processing, dissemination or disclose of certain data, which may be protected by the right to be forgotten, must be compensated to the affected party by the responsible party, regardless of whether it is derived from a contractual liability (when the affected party has accepted the general conditions of a certain product or service) or a non-contractual liability (when originated by the search engine, for example). The latter is usually the most common mechanism of compensation in the case of the right to be forgotten, since there is usually no previous contractual relationship between the injured party and the party causing the damage.

The Spanish Civil Code provides, in general terms, the civil liability regime, although this has been significantly expanded through special legislation. Thus the GDPR regulates several pathways through which a person can get custody of her or his right to be forgotten, because whoever has suffered damages as a consequence of an infraction of its provisions, will be entitled to receive compensation for the damages and losses suffered, including patrimonial and moral damages. Likewise, in the event of non-compliance with the provisions of the Regulation, each supervisory authority is empowered to impose individual, effective, proportionate, and dissuasive administrative fines.

The 2000/31/EC Directive on certain legal aspects of information society services and the Spanish *Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico* (LSSICE) is another special legislation related to information society services and electronic commerce, however, the CJEU Judgment in *Google Spain* case stated

that search engines were processing data in the development of their activity, being to that effect responsible. Consequently, it should be subject to data protection legislation, not being applicable the information society services legislation, the purpose of which would be limited mainly to cases of illicit processing of personal data.

Another law on the subject is the Spanish *Ley Orgánica 1/1982, de 5 de mayo*, on civil protection of the right to honor, personal and family privacy and own image (LOPD), when a violation of the right to be forgotten also entails a violation of some of the rights that it protects. Among the options provided in this law regarding compensation for damage to honor, privacy or own image, is the compensation for damages which is assumed whenever there is an illegitimate interference, and also includes moral damage.

XXX. The right to be forgotten has been distinguished from other related legal entities such as the right to cancellation, the right to object and the right to rectification, with which it maintains a common link due to the legal rights that these statutes protect or the incorporation of mechanisms that they guarantee.

The right to cancellation, integrated within the so-called "*ARCO rights*" and regulated in the LOPD, has been omitted in the drafting of the GDPR, and has been replaced by the right to erasure. The content of both provisions is very similar, and it seems that, by means of the right to be forgotten, the right to cancellation has been modernized and adapted to the circumstances required by *Big data* and Internet interaction. However, until the new LOPD -that follows the trend of the GDPR- is passed, both provisions currently coexist in the Spanish legal system, with some differences between them. Thus, while the right to cancellation must be exercised by the affected party against the person responsible for the file, the right to be forgotten can be exercised indistinctly, against the controller in charge or manager of a website or content, or against a search engine, and can even be exercised by a non-profit entity, organization or association. On the other hand, the right to be forgotten is constituted as a general rule, while the right to cancellation has a set of assessed assumptions.

The right to object diverges from the right to erasure, mainly due to the extension of its guarantee, since the former is only manifested as the subject's power to prevent a certain purpose of the processing of her or his personal data and not to the total erasure or disappearance. Likewise, the assumptions by which the right to object may be exercised are legally assessed and grant the affected subject the burden of proof. These differences between these provisions make them two legal tools for the preservation of the right to the protection of personal data, which explains their coexistence in the GDPR.

The right to rectification, contemplated in the Spanish *Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación* (LODR), has been incorporated in the GDPR, however its configuration has not been adapted to the current context caused by the eruption of the Internet. Furthermore, it does not take into account the idiosyncrasy of this new medium, characterized by an immediacy and continuous mutability. Its survival of regulation can only be explained by its practical applicability in concrete and small legal cases, similar mostly to those that can be identified in the traditional media. On the other hand, its coexistence in the GDPR with the right to be forgotten is explained by the divergent purposes for which they have been conceived. While the right to rectification seeks to reestablish the accuracy or veracity of certain published information, the right to be forgotten seeks to preserve privacy, despite the fact that the published data are accurate or true.

XXXI. Throughout this thesis, the right to be forgotten is presented as an efficient mechanism to resolve the legal problems arising from the paradigm presented, one characterized by the proliferation of the Internet and the massive use of data by new technologies and *Big data* corporations. However, the suitability of this legal solution to a problem that seems to be eminently structural remains to be seen. Given the architecture of the Internet, the immobility of governments to adopt interventionist policies in these matters and the social tolerance to certain abusive behaviors of private companies that deal with personal data, it is hard to affirm with completeness that all personal information on the Internet can be effectively erased.

On the other hand, many of the issues addressed throughout this dissertation are not exempt from criticism. This is the case regarding the requirement of the interested party to actively exercise the right to be forgotten, the privatization of the weighting judgment in case of conflict between legal assets, their effectiveness regarding future or immediate legal challenges such as the *Blockchain* case, or the underlying interests of European data protection regulations, as well as the omission of the gender impact in that legislation.

One more step in the guarantee of privacy, is the adoption of privacy policies by default and by design, which limit technological action so that *a priori* the fundamental rights of citizens are safeguarded without any interaction on their part. The goal is to reverse the current model of privacy guarantee, so that it ceases to operate as a reaction of the interested party to the violation of their fundamental rights, to be carried out in a proactive and preventive manner by those who design the products or systems which may lead to the violation of personal data.

In addition, a specific and unitary regulation of the right to be forgotten is required, setting out the conditions for its exercise and its relationship with other related rights that may interact in the same factual situation, ending the current regulatory disparity and the tendency of hyper-regulation that, far from simplifying, actually hinders the legal guarantee of fundamental rights. This proposal of *lege ferenda* must be able to articulate the specific parameters that must frame all jurisprudential analysis of the right to be forgotten, and also, its inclusion in the article 18 of the Spanish Constitution, along with the right to the protection of personal data, is desirable. Only then, will it be possible to provide citizens with greater legal security, while reducing the margin of discretion of the jurisdictional bodies around the configuration of the right to be forgotten, complying with the requirements of the social and democratic rule of law.

XXXII. This doctoral thesis seeks to provide a reflexive and critical perspective regarding the *Big data* phenomenon and new technologies, especially concerning its incidence in the legal system. The context presented has evidenced the necessary reconstruction of the area of personal freedom of the individual, which has been done starting in the *refoundation* of

privacy, as an indispensable presupposition for the protection of the dignity and free development of the personality in that frame.

From this perspective, the right to be forgotten has been shown as the replica offered from the law to the state of things, in the form of a personal guarantee that aspires to protect privacy and to solve the damages and inconveniences caused by the new social conditions derived from the handling of massive quantities of personal data. This recognizes the importance of the development of the right to be forgotten as a fundamental right, while at the same time highlighting the problems and shortcomings that stem from its recent birth, as well as the lack of a unitary, precise regulation in the matter.

Consequently, technological development cannot in any case be an argument that legitimizes certain infringements of fundamental rights, since the new technological tools must respect the rights and freedoms of the social and democratic rule of law, which must adopt the mechanisms necessary to achieve technological and social progress with respect for the legal system.

BIBLIOGRAFÍA

AGUILAR, M. A. "La opacidad necesaria" en *La transparencia engaña*, (Albergamo ed.), Biblioteca Nueva, Madrid, 2014.

ALBALADEJO. *Derecho Civil I. Introducción y Parte General*, Edisofer, Madrid, 2009.

ALBERTO GONZÁLEZ. "Responsabilidad proactiva en el tratamiento de datos masivos", *Dilemata*, nº 24, 2017.

ALEXY, R. *Teoría de los Derechos Fundamentales*, Centro de Estudios Políticos y Constitucionales, Madrid, 2001.

- *Teoría de la argumentación jurídica*, Centro de Estudios Políticos y Constitucionales, Madrid, 1989.

ALLAN, T.R.S. *The sovereignty of law,* Oxford University Press, Oxford, 2013.

- *Constitutional Justice, A liberal theory of the rule of law,* Oxford University Press, Oxford, 2011.

ÁLVAREZ CARO, M. "El derecho de supresión o al olvido", en *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad* (Piñar Mañas dir.), Reus, Madrid, 2016.

- *Derecho al olvido en Internet: el Nuevo paradigm de la privacidad en la era digital,* Reus, Madrid, 2015.

ÁLVAREZ GARCÍA, F. J. *Sobre el principio de legalidad*, Tirant lo Blanch, València, 2009.

ÁLVAREZ-CIENFUEGOS SUÁREZ, J. M. *La defensa de la intimidad de los ciudadanos y la tecnología informática*, Aranzadi, Pamplona 1999.

AÑÓN ROIG, M. J.: "Derechos sociales: cuestiones de legalidad y de legitimidad", *Anales de la Cátedra Francisco Suárez*, Vol. 44, 2010, p. 23.

ANSUÁTEGUI ROIG. "La cuestión de la universalidad de los derechos: de las instituciones a los problemas" en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. IV, Dykinson, Madrid, 2013.

ARA PINILLA, I. *Las transformaciones de los derechos humanos*, Tecnos, Madrid, 1990.

ARDEN, M. "Criminal Law at the Crossroads: The Impact of Human Rights from the Law Commission's Perspective and the Need for a Code", *Criminal Law Review*, Sweet and Maxwell, London, 1999.

ARENAS RAMIRO, M. "Reforzando el ejercicio del derecho a la protección de datos" en *Hacia un nuevo Derecho europeo de Protección de Datos* (Rallo Lombarte/García Mahamut eds.), Tirant lo Blanch, València, 2015.

- "El derecho a la protección de datos personales en la jurisprudencia del TJCE", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, Vol. 4, 2006.

ARENDT, H. *Los orígenes del totalitarismo*, Alianza, Madrid, 2006.

ASHTON, K. "That 'Internet of Things' Thing", *RFID Journal*, 2009.

ASHWORTH, A. "What have Human Rights done for Criminal Justice in the UK?", *University of Tasmania Law Review*, Vol. 23, nº 2, 2004.

ASHWORTH/EMMERSON/MACDONALD. *Human Rights and Criminal Justice*, Sweet & Maxwell, 3ª ed., London, 2012.

ASÍS ROIG, R. *Las paradojas de los derechos fundamentales como límites al poder*, Dykinson, Madrid, 2000.

ATIENZA, M. *El sentido del Derecho*, Ariel, Barcelona, 2003.

BAINBRIDGE, D. *Data Protection Law*, XPL publishing, Great Britain, 2005.

BAMBERGUER, K.A. /MULLIGAN, D. *Privacy on the Ground. Driving Corporate Behavior in the United States and Europe*, Massachusetts Institute of Technology Press, Cambridge, 2015.

BARRÈRE, M.A. "La interseccionalidad como desafío al *mainstreaming* de género en las políticas públicas", *Revista Vasca de Administración Pública*, nº 87-88, 2010

BASTIDA FREIJEDO, F. J./ VILLAVERDE MENÉNDEZ, I. et al. *Teoría general de los derechos fundamentales en la Constitución española de 1978*, Tecnos, Madrid, 2001.

BAUMAN, Z. *Modernidad líquida*, Fondo de Cultura Económica, Madrid, 2017.

BÉJAR, H. *El ámbito íntimo. Privacidad, individualismo y modernidad*, Alianza, Madrid, 1989.

BENITO GARCÍA, J.M. "El derecho de rectificación electrónica: una forma interactiva de participación", en *La ética y el derecho de la información en los tiempos del postperiodismo*, Fundación COSO de la Comunidad Valenciana para el Desarrollo de la Comunicación y la Sociedad, Valencia, 2007.

BENTHAM, J. *Panóptico,* Círculo de Bellas Artes, Madrid, 2011.

BERGELSON, V. "It's Personal but Is It Mine? Toward Property Rights in Personal Information", *UC Davis Law Review*, Vol. 37, nº 379, 2003.

BERMEO ÁLVAREZ, L.F. "Las normas jurídicas: una aproximación desde el convencionalismo jurídico y el análisis económico del derecho", *Inciso*, Vol. 18, nº1, 2016.

BERROCAL LANZAROT, A. I. *Derecho de supresión de datos o derecho al olvido*, Editorial Reus, Madrid, 2017.

BINGHAM, T. *The rule of law*, Penguin Group, London, 2011.

- "The European Convention of Human Rights – Time to incorporate", *Law Quarterly Review*, nº 109.

BOIX PALOP, A. "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* nº 38, 2015.

BOIX REIG, J. /JAREÑO LEAL, A. *La protección jurídica de la intimidad*, Iustel, Madrid, 2010.

BOYLE, J. "Foucault in cyberspace: surveillance, sovereignty, and hardwired censors", *University of Cincinnati Law review*, nº 66, 1997.

BROTONS MOLINA, O. "Caso Google: Tratamiento de datos y derecho al olvido. Análisis de las conclusiones del abogado general, asunto C-131712", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 33.

BURDEN, P. *News of the world? Fake Sheikhs & Royal Trappings*, Eye Books, London, 2008.

BUSTAMANTE DONAS, J. "Hacia la cuarta generación de Derechos Humanos. Repensando la condición humana en la sociedad tecnológica", *CTS+I: Revista Iberoamericana de Ciencia, Tecnología, Sociedad e Innovación*, nº 1, 2001.

BUTLER, J. *Deshacer el género*, Paidos, D.L., Barcelona, 2006

- *El género en disputa: el feminismo y la subversión de la identidad*, Paidos, México, 2001

CAPELLA, J. R. "Estado y Derecho ante la mundialización: aspectos y problemáticas generales", en *Transformaciones del Derecho en la mundialización*, Consejo General del Poder Judicial, Madrid, 1999.

CARBONELL MATEU, J.C. *Derecho penal: concepto y principios constitucionales*, Tirant lo Blanch, Valencia, 1999.

CAREY, P. *Data Protection: a practical Guide to UK and EU Law*, Oxford University Press, Oxford, 2015.

- *Data Protection Handbook*, The Law Society, London, 2008.
- *Data Protection Act 1998*, Blackstone Press Limited, London, 1998.

CARRILLO LÓPEZ, M. "Libertad de expresión, personas jurídicas y derecho al honor", *Derecho Privado y Constitución*, nº 10, 1996.

CERNADA BADÍA. "El derecho al olvido judicial en la red" en *Libertad de Expresión e información en Internet. Amenazas y protección de los derechos personales* (Corredoira y Alfonso, y Cotino Hueso coord.), Centro de Estudios Políticos y Constitucionales, Madrid, 2013.

CIGÜELA SOLA, J. *Exclosos i transparentats. Del panòptic a la pantalla digital*, Institució Alfons el Magnànim, Centre Valencià d'Estudis i d'Investigació, València, 2017.

CLARKE. *Introduction to Dataveillance and Information Privacy*, Australian National University, 2006.

CLAYTON, R. "Judicial Deference and Democratic Dialogue: the Legitimacy of Judicial Intervention under the Human Rights Act 1998", *Public Law*, Sweet and Maxwell, London, 2004.

CLAYTON, R. / TOMLINSON, H. *Privacy and Freedom of Expression*, Oxford University Press, Oxford, 2010.

COLVIN, M. *Developing Key Privacy Rights*, Hart publishing, Portland, 2002.

CONCEPCIÓN RODRÍGUEZ, J.L. *Derecho de daños*, Bosch, Barcelona, 1999.

CONSTANT, B. *Cours de Politique Constitutionelle*, Didier, París, 1836.

COOLEY, T. M. *The law of torts*, Callaghan, Chicago, 1930.

- *A treatise on the Law of Torts*, Callaghan, Chicago, 1888.

COOPER, J. "Horizontality: The Application of Human Rights Standards in Private Disputes", en *An Introduction to Human Rights and the Common Law*, (English/Havers eds.), Hart Publishing, Oxford and Portland (Oregon), 2000.

CORRECHER MIRA, J. *Principio de legalidad penal: ley formal vs. law in action*, Tirant lo Blanch, València, 2018.

- "El delito de enaltecimiento del terrorismo y humillación a las víctimas tras la reforma de la LO 2/2015 en materia de delitos de terrorismo", *Revista General de Derecho penal*, nº 27, 2017.

COTINO HUESO, L. "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata,* nº 24, 2017.

CRAIG, P. "Formal and substantive conceptions of the rule of law: an analytical framework", *Public Law*, Sweet and Maxwell, London, 1997.

CUERDA ARNAU, M.L. "Proporcionalidad penal y libertad de expresión: la función dogmática del efecto de desaliento", *Revista General de Derecho penal*, nº 8, 2007.

DAVIS, H. *Human Rights and Civil Liberties*, Willan Publishing, Cullompton, 2003.

DE CABO MARTÍN, C. *Dialéctica de sujeto, dialéctica de la Constitución*, Trotta, Madrid, 2010.

DE LUCAS, J. "La globalización no significa universalidad de los derechos humanos", *Jueces para la democracia*, nº 32, 1998.

DE TERWANGNE, C. "The Right to be Forgotten and Informational Autonomy in the Digital Environment" en *The ethics of memory in a digital age. Interrogating the right to be forgotten* (Ghezzi/Guimares Pereira eds.), Palgrave Macmillan Memory Studies, UK, 2014.

- Privacidad en Internet y el derecho a ser olvidado", *Revista de Internet, Derecho y Política*, nº 13, 2012.

DEL FRESNO GARCÍA, M. "Internet como macromedio: la cohabitación entre los medios sociales y los medios profesionales", *Revista de Pensamiento sobre Comunicación, Tecnología y Sociedad*, nº 99, 2014.

DENNINGER. *Menschenrechte und Grundgesetz. Zwei Essays*, Belt Athenäum, Weinheim, 1991.

- Government Assistance in the Exercise of Basic Rights" en *Critical Legal Thought: An American-German Debate* (Joerges/Trubek eds.), Nomos, Baden-baden, 1989.
- "El derecho a la autodeterminación informativa" en *Problemas actuales de la documentación y la informática jurídica*, (Pérez Luño ed.), Tecnos, Madrid, 1987.

DESANTES GUANTER , *Los límites de la información. La información en la jurisprudencia del Tribunal Constitucional: las 100 primeras sentencias*, APM, Madrid, 1991.

– "Intimidad e información, derechos excluyentes", *Nuestro tiempo*, nº 213, Pamplona, 1972.

DETERMANN, L. *Determann's Field Guide to Data Privacy Law*, Edward Elgar publishing, Cheltenham, 2015.

DE TEREWAGNE, "Privacidad en Internet y el derecho a ser olvidado", *Revista de Internet, Derecho y Política*, nº 13, 2012.

DI PIZZO CHIACCHIO, A. *La expansion del derecho al olvido digital. Efectos de "Google Spain" y el Big Data e implicaciones del nuevo Reglamento Europeo de Protección de Datos*, Atelier, Barcelona, 2018.

DIAZ, E. *Sociología y filosofía del derecho*, Taurus, Madrid, 1989.

DÍAZ FRAILE, J.M. "Aspectos jurídicos más relevantes de la directiva y del proyecto de ley español de comercio electrónico" en *Contratación y comercio electrónico* (Orduña Moreno coord.), Tirant lo Blanch, València, 2003.

DICEY, A. V. *Introductory to the study of the law of the constitution (The Oxford Edition of Dicey),* Oxford University Press, Oxford, 2013.

DÍEZ-PICAZO GIMÉNEZ, L. M. *Sistema de derechos Fundamentales*, Civitas, Madrid, 2013.

DIEZ-PICAZO, L. *Experiencias jurídicas y teoría del Derecho*, Ariel, Barcelona, 1983.

– *Derecho y masificación social. Tecnologia y derecho privado (dos esbozos)*, Civitas, Madrid, 1979.

DIEZ-PICAZO, L./ GULLÓN, A. *Sistema de Derecho Civil*, Tecnos, Vol. 1, Madrid, 1992.

DOMENECH PASCUAL, G. "Por qué y cómo hacer análisis económico del Derecho", *Revista de administración pública*, nº 195, 2014.

DOMÍNGUEZ MEJÍAS, I. "Hacia la memoria selectiva en Internet. Honor, intimidad y propia imagen en la era digital a partir de la jurisprudencia española" en *Revista Iberoamericana de Ciencia, Tecnología y Sociedad*, nº 32, Vol. 11, 2016.

DWORKIN, G. "The Younger Committee Report on Privacy", *The Modern Law Review*, Vol. 36, nº 4, 1973, pp. 399-406.

DWORKIN, R. *A matter of principle,* Harvard University Press, Cambridge, 1985.

- *Los derechos en serio*, Ariel, Barcelona, 1984.

DUASO CALÉS, R. "Los principios de protección de datos desde el diseño y protección de datos por defecto" en *Reglamento General de Protección de datos. Hacia un nuevo modelo europeo de privacidad* (Piñar Mañas dir.), Reus, Madrid, 2016.

EAGLE, N./ GREENE, K. *Reality mining. Using big data to engineer a better world*, MIT Press, Boston, 2014.

EKINS, R. "Right-Consistent Interpretation and The Human Rights Act 1998", *Law Quarterly Review*, Sweet and Maxwell, London, 2011.

ELLIOTT, M. /THOMAS, R. *Public law*, Oxford University Press, Oxford, 2014.

ENDICOTT, T. "'International Meaning': Comity in Fundamental Rights Adjudication", *International Journal of Refugee Law*, Vol. 13, Issue 3, 2001.

ERDOS, D. "Confused? Analysing the Scope of Freedom of Speech protection vis-à-vis European Data Protection", *Oxford Legal Studies Research Paper,* nº 48, 2012.

- "Stuck in the Thicket? Social Research Under the First Data Protection Principle", *International Journal of Law and Information Technology*, Vol. 19, 2011.

ESPINOSA. "Reflexiones antropolíticas sobre el mundo digital y la autonomía personal", *Dilemata,* nº 24.

EWING, K. /GEARTY, C. *Freedom under Thatcher*, Oxford University Press, 1990.

FAYOS GARDÓ, A. "Los derechos a la intimidad y a la propia imagen: un análisis de la jurisprudencial española, británica y del Tribunal Europeo de Derechos Humanos", *InDret*, nº 4, 2007.

FAZLIOGLU, M. “Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet”, *International Data Privacy Law*, Vol. 3, nº 3, 2013.

FELDMAN, D. *English Public Law*, Oxford University Press, Oxford, 2009.

FENWICK, H. /PHILLIPSON, G. “Breach of Confidence as a Privacy Remedy in the Human Rights Act Era”, *Modern Law Review*, nº 63, 2000.

FERNÁNDEZ SALMERÓN, M. “Rectificación y réplica. Reflexiones sobre su proyección en la Web” en *Libertades de expresión e información en Internet y las redes sociales: ejercicio, amenazas y garantías* (Cotino Hueso, ed.), Universitat de València, València, 2011.

FERRAJOLI, L *Derecho y razón. Teoría del garantismo penal*, Trotta, Madrid, 2009.

- *Derechos y garantías. La ley del más débil*, Trotta, Madrid, 2004.

FOUCAULT, M. *Vigilar y castigar*. *Nacimiento de la prisión*, Siglo XXI, Madrid, 2009.

FRÍGOLS I BRINES, E. *Fundamentos de la Sucesión de Leyes en el Derecho penal español. Existencia y aplicabilidad temporal de las normas penales*, Bosch, Barcelona, 2004.

FROSINI, V. *Informática y Derecho*, Temis, Bogotá, 1988.

- *Cibernética, derecho y sociedad*, Tecnos, Madrid, 1982.

GALPARSORO, J. “Big data y psicopolítica. Vía de escape: de la vida calculable a la vida como obra de arte, *Dilemata,* nº 24, 2017.

GARCÉS, M. *Nueva ilustración radical*, Anagrama, Barcelona, 2017.

GARCÍA MAHAMUT, R. “Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español”, *UNED. Teoría y Realidad Constitucional*, nº 35, 2015.

GARCÍA LOPEZ, M. A. *El impacto de Internet en el libre desarrollo de la personalidad*, Wolters Kluwer, Madrid, 2018.

GARCÍA PASCUAL, C. *Legitimidad democrática y poder judicial*, Edicions Alfons El Magnànim, València, 1997.

GARCÍA SAN MIGUEL, L. *Estudios sobre el derecho a la intimidad*, Tecnos, Madrid, 1992.

GARRIGA DOMÍNGUEZ, A. "Nuevas tecnologías, derecho a la intimidad y protección de datos personales" en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. VI, Libro II, Dykinson, Madrid, 2013.

GARZÓN VALDÉS, E. "Lo íntimo, lo privado y lo público", *Claves de la razón práctica*, nº 137, Madrid, 2003.

GEARTY, C. "Reconciling Parliamentary democracy and human rights", *Law Quaterly Review*, nº 118, 2002.

GIL RUIZ, J. M. "Nuevos instrumentos vinculantes para una ciencia de la legislación renovada: impacto normativo y género", *Anales de la Cátedra Francisco Suárez*, 47, 2013

GÓMEZ MONTORO, A. J. "La titularidad de derechos fundamentales por personas jurídicas: un intento de fundamentación", *Revista Española de Derecho Constitucional*, año nº22, nº65, 2002.

GONZÁLEZ PÉREZ, J. *La dignidad de la persona*, Civitas, Madrid, 2017.

GOOLD, B./LAZARUS, L./SWINEY, G. *Public Protection, Proportionality and the Search for Balance*. Ministry of Justice Research Series, September 2007.

GROSZ, S./BEATSON, J./DUFFY, P. *Human Rights. The 1998 Act and the European Convention*, Sweet and Maxwell, London, 2000.

GUTIÉRREZ GOÑI, L. *Derecho de rectificación y libertad de información*, J. M. Bosch, Navarra, 2003.

GUTIÉRREZ GUTIÉRREZ, I. *Dignidad de la persona y derechos fundamentales*, Marcial Pons, Madrid, 2005.

HABERMAS, J. *El discurso filosófico de la modernidad*, Taurus, Madrid, 1991.

HAN, B.C. *Psicopolítica*, Herder, Barcelona, 2014.

- *La sociedad de la transparencia*, Herder, Barcelona, 2013.

HARARI, Y. N. *Homo Deus. Breve historia del mañana*, Debate, Barcelona, 2016.

HARCOURT, B. *Exposed. Desire and Disobedience in the Digital Age*, Harvard University Press, Cambridge, 2015.

- "Governing, Exchanging, Securing: Big Data and the production of a digital knowledge", *Public Law and Legal Theory Working Paper Group*, Columbia Law School, 2014.

HAVERS QC, P. /GARNHAM, N. "The Convention and the Human Rights Act: A New Way of Thinking", en *An Introduction to Human Rights and the Common Law* (English/Havers eds.), Hart Publishing, Oxford and Portland (Oregon), 2000.

HERNÁNDEZ MARTÍN, M. A. "La privacidad: una mirada desde la economía" en *En torno a la privacidad y la protección de datos en la sociedad de la información* (Aparicio Vaquero/Batuecas Caletrío coord.), Comares, Granada, 2015.

HERRERO TEJEDOR, F. *Honor, Intimidad y Propia Imagen*, Colex, Madrid, 1994.

HICKMAN, T. *Public Law after the Human Rights Act*, Hart Publishing, Oxford, 2011.

- "Constitutional Dialogue, Constitutional Theories and the Human Rights Act 1998", *Public Law*, Sweet and Maxwell, London, 2005.

HIJMANS, H. *The European Union as Guardian of Internet Privacy Law*, Springer International Publishing, Switzerland, 2016.

HUBMANN, H. *Das Persönlichkeitsrecht*, Böhlau, Colonia, 1967.

IGLESIAS GARZÓN, A. "Tecnología, comunicación y política en el siglo XX", en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. I, Libro I, Dykinson, Madrid, 2013.

INNES, J. *Privacy, Intimacy and Isolation*, Oxford University Press, New York, 1992.

JAY, R. *Guide to the General data Protection Regulation*, Sweet & Maxwell, London, 2017.

- *Data Protection Law and Practice*, Sweet & Maxwell, London, 2012.

JOINSON, A. N. “Looking at, Lookinf up, or Keeping up with People? Motives and uses of Facebook, en *CHI 2008 Proceedings: Online Social Networks*, 2008.

KAVANAGH, A. *Constitutional Review under the UK Human Rights Act*, Cambridge University press, Cambridge, 2009.

KLUG, F. “Judicial Deference under the Human Rights Act 1998”, *European Human Rights Law Review*, Sweet and Maxwell, London, 2003.

KROTOSZYNSKI, R. *Privacy Revisited. A Global Perspective on the Right to Be Left Alone*, Oxford University Press, Oxford, 2016.

LERMAN, J. “Big data and its exclusions”, *Stanford Law Review*, 66, 2013.

LIZARRAGA VIZCARRA, I. El Derecho de Rectificación, Aranzadi, Navarra, 2005.

LÓPEZ GUERRA, L. *Derecho Constitucional*, Tirant lo Blanch, València, 2007.

LÓPEZ JACOISTE, J. J. “Una aproximación tópica a los derechos de la personalidad”, *Anuario de Derecho Civil*, Vol. 39, nº14, 1986.

LORD LESTER OF HERNE HILL. “The Art of Possible: Interpretating Statutes under the Human Rights Act”, *European Human Rights Law Review*, Sweet and Maxwell, London, 1998,

MADDEN, M./ RAINIE, L. “Americans’ attitudes about privacy, security and surveillance”, en *Pew Research Center*, 2015. Disponible online en: http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

MARKESINIS, B. “The Right to Be Let Alone versus Freedom of Speech”, *Public Law*, nº 1, 1986.

MARKESINIS, B. /O’CINNEIDE, C. /FEDTKE, J. /HUNTER-HENIN, M. “Concerns and ideas about the developing English Law of Privacy (And How Knowledge of Foreign Law Might Be of Help)”, *American Journal of Comparative Law*, nº 52, 2004.

MARTÍN I CASALS, M. "Indemnización de daños y otras medidas judiciales por intromisión ilegítima contra el derecho al honor" en *El mercado de las ideas* (Salvador Coderch dir.), Centro de Estudios Constitucionales, Madrid, 1990.

MARTÍNEZ DE AGUIRRE ALDAZ, C. "Los derechos de la personalidad", en *Curso de Derecho Civil (I). Derecho de la Persona*, (De Pablo Contreras, coord.), Edisofer, Tomo I, Vol. 2, Madrid, 2016.

MARTÍNEZ OTERO, J.M. "El derecho al olvido en Internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja", *Revista de Derecho Político*, nº 93, 2015.

MARTÍNEZ VELENCOSO, L. "El nuevo concepto de onerosidad en el mercado digital. ¿Realmente es gratis la App?", *InDret*, nº 1, 2018.

MATHIESON, K. *Privacy Law Handbook*, The Law Society, London, 2010.

MAYER-SCHÖNBERGER, V. /FOSTER, T. "Free Speech and the Global Information Infrastructure", *Michigan Telecommunications and Technology Law Review*, Vol. 3, nº 45, 1997.

MAYER-SCHÖNBERGER, V. *Delete. The Virtue of Forgetting in the Digital Age*, Princeton University Press, New Jersey, 2011.

MAYER-SCHÖNBERGER/CUKIER. *Big data. La revolución de los datos masivos*, Turner, Madrid, 2015

MEDINA GUERRERO, M. *La vinculación negativa del legislador a los derechos fundamentales*, McGraw-Hill, Madrid, 1996.

MERCADO PACHECO, P. *El análisis económico del derecho: una reconstrucción teórica*, Centro de Estudios Constitucionales, Madrid, 1994.

MERGES, R.P. "Contracting into Liability Rules: Intellectual Property Rights and Collective Rights Organizations", *Southern California Law Review* Vol. 8, nº 1293, 1996.

MINERO ALEJANDRE, G. "A vueltas con el 'derecho al olvido'. Construcción normativa y jurisprudencial del derecho de protección de datos de carácter personal en el entorno digital", *Revista Jurídica de la Universidad Autónoma de Madrid*, nº 30, 2014.

MIRA BENAVENT, F.J. "Algunas consideraciones político-criminales sobre la función de los delitos de enaltecimiento del terrorismo y humillación a las víctimas del terrorismo", en *Terrorismo y contraterrorismo en el Siglo XXI. Un análisis penal y político criminal* (Pérez Cepeda Dir.), Ratios Legis, Salamanca, 2016.

MONASTERIO ASTOBIZA. "Ética algorítmica: implicaciones éticas de una sociedad cada vez más gobernada por algoritmos", *Dilemata*, nº 24, 2017.

MONTÉS PENADÉS, V. / BLASCO GASCÓ, F. et al. *Derecho civil. Parte general*, Tirant lo Blanch, València, 1992.

MORENO MUÑOZ, M. Privacidad y procesado automático de datos personales mediante aplicaciones y bots", *Dilemata,* nº 24, 2017.

MÜLLER, F. "Tesis acerca de la estructura de las normas jurídicas", *Revista Española de Derecho Constitucional*, nº 27, 1989.

MUÑOZ, J. "El llamado derecho al olvido en Internet y la responsabilidad de los buscadores", *Diario la Ley*, nº 8317, 2014.

MUÑOZ RODRÍGUEZ, J. "La desindexación de contenidos del índice de resultados de buscadores de internet tras la sentencia del TJUE sobre derecho al olvido", *Abogacía Española*, 2014. Disponible online en: https://www.abogacia.es/2014/10/13/la-desindexacion-de-contenidos-del-indice-de-resultados-de-buscadores-de-internet-tras-la-sentencia-del-tjue-sobre-derecho-al-olvido/

MUÑOZ SORO, J.F./ OLIVER-LALANA, A.D. *Derecho y cultura de protección de datos. Un estudio sobre la privacidad en Aragón*, Dykinson, Madrid, 2012.

NAVAS NAVARRO, S. *Mercado digital. Principios y reglas jurídicas*, Tirant lo Blanch, Valencia, 2016.

NOAIN SÁNCHEZ, A. *La protección de la intimidad y vida privada en internet: la integridad contextual y los flujos de información en las redes sociales (2004-2014)*, Boletín Oficial del Estado, Madrid, 2016.

NOORDA, C./ HANLOSER, S. *E-Discovery and Data Privacy. A Practical Guide*, Kluwer Law International, The Netherlands, 2011.

O'CALLAGHAN MUÑOZ, X. *Libertad de expresión y sus límites: honor, intimidad e imagen*, Edersa, Madrid, 1991.

O'NEIL, K. *Armas de destrucción masiva. Cómo el Big data aumenta la desigualdad y amenaza la democracia*, Capitán Swing, Madrid, 2018.

ORDUÑA MORENO, F.J./ SÁNCHEZ MARTÍN, C. *La transparencia como valor del cambio social: su alcance constitucional y normativo. Concreción técnica de la figura y doctrina jurisprudencial aplicable en el ámbito de la contratación*, Aranzadi, navarra, 2018.

PAUNER CHULVI, C. "La actividad periodística en los ordenamientos nacionales y europeo sobre protección de datos" en *Hacia un nuevo Derecho europeo de Protección de Datos* (Rallo Lombarte/García Mahamut eds.), Tirant lo Blanch, València, 2015.

- "El impacto de las nuevas tecnologías en los derechos fundamentales: el reto de la privacidad en la prensa digital" en *Nuevas tecnologías y derechos humanos* (Pérez Luño ed.), Tirant lo Blanch, València, 2014.
- Privacidad y periodismo: el escándalo Murdoch sobre escuchas telefónicas en News of the World", *Revista de Derecho Político*, nº 88, 2013.

PAZOS CASTRO, R. "El derecho al olvido frente a los editores de hemerotecas digitales", *InDret*, nº 4, 2016.

- "El funcionamiento de los motores de búsqueda en Internet y la política de protección de datos personales, una relación imposible?", *InDret*, nº 1, 2015.
- "El mal llamado derecho al olvido en la era de Internet", Boletín del Ministerio de Justicia, nº 2183, 2015.

PECES-BARBA MARTÍNEZ, G. *Curso de derechos fundamentales. Teoría general*, Universidad Carlos III-Boletín Oficial del Estado, Madrid, 1999.

PEÑA LÓPEZ. F. "De las obligaciones que nacen de culpa o negligencia" en *Comentarios al Código Civil* (Bercovitz Rodríguez-Cano Dir.), Tomo IX, Tirant lo Blanch, València, 2013.

PÉREZ CEPEDA, A. "La criminalización del radicalismo y extremismo en la legislación antiterrorista", en *Terrorismo y contraterrorismo en el Siglo XXI. Un análisis penal y político criminal*, Ratios Legis, Salamanca, 2016.

PÉREZ LUÑO, A.E. *Nuevas tecnologías y derechos humanos*, Tirant lo Blanch, València, 2014.

- "El derecho al honor y a la intimidad", en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. I, Libro II, Dykinson, Madrid, 2013.
- "Las generaciones de derechos humanos", en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. I, Libro I, Dykinson, Madrid, 2013.
- *Teoría del derecho. Una concepción de la Experiencia Jurídica*, Tecnos, Madrid, 2012.
- *Los derechos humanos en la sociedad tecnológica*, Universitas, Madrid, 2012.
- *Derechos Humanos, Estado de Derecho y Constitución*, Tecnos, Madrid, 2010.
- "Los derechos humanos en la sociedad global", en *La tercera generación de derechos humanos*, Thomson-Aranzadi, Cizur Menor, 2006.
- *La seguridad jurídica*, Ariel, Barcelona, 1991.

PÉREZ LUÑO, A.E. /GONZÁLEZ-TABLAS, R. "Ciberciudadanía y teledemocracia", en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. I, Libro II, Dykinson, Madrid, 2013.

PÉREZ TREMPS, P. *Derecho constitucional. El ordenamiento constitucional. Derechos y deberes de los ciudadanos*, Tirant lo Blanch, València, 2016.

- "La interpretación de los derechos fundamentales", en *Interpretación constitucional* (Ferrer Mac-Gregor coord.), Tomo II, Porrúa, México, 2005.

PHILIPSON, G. "(Mis) representing section 3 of the Human Rights Act 1998", *Law Quarterly Review*, Sweet and Maxwell, London, 2003.

PLAZA PENADÉS, J. "Doctrina del Tribunal de Justicia de la Unión Europea sobre protección de datos y derecho al olvido", *Revista Aranzadi de Derecho y Nuevas Tecnologías*, nº 35, 2014.

- "La responsabilidad civil de los intermediarios en Internet y otras redes" en *Contratación y comercio electrónico* (Orduña Moreno coord.), Tirant lo Blanch, València, 2003.
- "Los principales aspectos de la Ley de Servicios de la Sociedad de la Información y Comercio electrónico" en *Contratación y comercio electrónico* (Orduña Moreno coord.), Tirant lo Blanch, València, 2003.

PORTILLA CONTRERAS, G. "Los excesos del formalismo jurídico neofuncionalista en el normativismo del Derecho penal", *Revista General de Derecho penal*, nº 4, 2000.

POULLET, Y. "Pour une troisiène génération de réglementations de protection des domnées", en *Jusletter*, nº 3, 2015.

- "Hacia nuevos principios de protección de datos en un nuevo entorno TIC", en *Revista de Internet, Derecho y Política*, nº 5, 2007.

PRIETO SANCHÍS, L. *El constitucionalismo de los derechos. Ensayos de filosofía jurídica*, Trotta, Madrid, 2013,

- *Estudio sobre derechos fundamentales*, Debate, Madrid, 1990.

PROSSER, W. L. /KEETON, W. P. *On the Law of torts*, West, St. Paul, 1984.

PUYOL MORENO, J. "Una aproximación a Big Data", *Revista de Derecho, UNED*, nº 14, 2004.

RALLO LLOMBARTE, A. "El debate europeo sobre el derecho al olvido en Internet" en *Hacia un nuevo Derecho europeo de Protección de Datos* (Rallo Lombarte/García Mahamut eds.), Tirant lo Blanch, València, 2015.

- *El derecho al olvido en Internet. Google versus España*, Centro de Estudios Políticos y Constitucionales, Madrid, 2014.

– "El derecho al olvido en el tiempo de Internet: la experiencia española" en *Percosi costituzionali. Libertà in Internet* (de Vergottini ed.), Jovene editore, nº 1, Napoli, 2014.

RAZ, J. "On the Authority and Interpretation of Constitutions: Some preliminaries", en *Constitutionalism. Philosophical Foundations*, (Alexander, L. ed.), Cambridge University Press, Cambridge,1998.

– "The rule of law and its virtue", *The authority of law. Essays on law and morality,* Oxford Clarendon Press, Oxford, 1979.

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

– "Prólogo", *Panóptico,* Círculo de Bellas Artes, Madrid, 2011.

REGLERO CAMPOS, L.F/BUSTO LAGO, J.M. *Tratado de responsabilidad civil*, Aranzadi, Navarra, 2014.

RÍOS MARTÍN, J.C. *Los ficheros de internos de especial seguimiento. Análisis de la normativa reguladora, fundamentos de su ilegalidad y exclusión del ordenamiento jurídico*. Disponible en: http://www.derechopenitenciario.com/comun/fichero.asp?id=995

RODRÍGUEZ MOURULLO, G. *Aplicación judicial del Derecho y lógica de la argumentación jurídica*, Civitas, Madrid, 1988.

ROZENBERG, J. *Privacy and the Press*, Oxford University Press, New York, 2004.

RUIZ-RICO RUIZ, G. "Una exploración necesariamente sintética sobre el concepto y los límites de las libertades de expresión e información" en *Historia de los Derechos Fundamentales* (Peces-Barba et al. eds.), Tomo IV, Vol. VI, Libro II, Dykinson, Madrid, 2013.

SALVADOR CODERCH, P. *El mercado de las ideas*, Centro de estudios constitucionales, Madrid, 1990.

– *¿Qué es difamar? Libelo contra la Ley del Libelo*, Civitas, Madrid, 1987.

SCHWARTZ, P. M. “Privacy and Democracy in Cyberspace”, *Vanderbilt Law Review*, Vol. 52, 1999.

SCHWARTZ, P.M. /REIDENBERG, J. R. *Data Privacy Law*, Michie Law Publishers, Charlottesville, 1996.

SIMÓN CASTELLANO, P. *El reconocimiento del derecho al olvido digital en España y en la UE. Efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, Barcelona, 2015.

- *El régimen constitucional del derecho al olvido digital*, Tirant lo Blanch, València, 2011.

SMITH, A. T. H. “The Human Rights Act 1998 (1) The Human Rights Act and the Criminal Lawyer: The Constitutional Context”, *Criminal Law Review*, Sweet and Maxwell, London, 1999.

SOFSKY, W. *Defensa de lo privado*, Pre-textos, 2009.

SOLOVE, D. J. “I’ve Got Nothing to Hide and Other Misunderstandings of Privacy”, *San Diego Law Review*, Vol. 44, 2007.

- “A Taxonomy of Privacy”, *University of Pennsylvania Law Review*, Vol. 154, nº 13.
- “Conceptualizing Privacy”, *California Law Review*, Vol. 90, nº 1087, 2002

TRAVIS, H. *Cyberspace Law. Censorship and regulation of the Internet*, Routledge, New York, 2013.

TREACY, B./BAPAT, A. “Purpose limitation – clarity at last?”, *Privacy & Data Protection Journals*, Vol. 3, Issue 6, 2013.

TRONCOSO REIGADA, A. *La protección de datos personales. En busca del equilibrio*, Tirant lo Blanch, Valencia, 2010.

TUGENDHAT QC, M./CHRISTIE, I. *The law of Privacy and The Media*, Oxford University Press, New York, 2002.

UNGER. *Law in modern society: towards a criticism of social theory,* Free Press, New York, 1976.

VIDAL MARÍN, T. "Derecho al honor, personas jurídicas y tribunal constitucional", *InDret*, nº 1, 2007.

WACKS, R. *Privacy and Media Freedom*, Oxford University Press, Oxford, 2013.

- *Privacy and Press Freedom*, Blackstone Press Limited, London, 1995.

WADHAM, J. /MOUNTFIELD Q.C. /PROCHASKA, E. *Blackstone's guide to The Human Rights Act*, 1998, Oxford University Press, Oxford, 2015.

WARREN, S./BRANDEIS, L. *El derecho a la intimidad,* Civitas, Madrid, 1995.

- "The Right to Privacy", *Harvard Law Review*, vol. IV, nº 5, 1890.

WESTIN, A. *Privacy and freedom*, Athenaeum, New York, 1967.

YOUNG A. *Parliamentary Sovereignty and the Human Rights Act*, Hart Publishing, Oxford, 2009.

YZQUIERDO TOLSADA "Daños a los derechos de la personalidad (Honor, Intimidad y Propia imagen)" en *Tratado de responsabilidad civil* (Reglero Campos y Busto Lago coord.), Aranzadi, Navarra, 2014.

ZACCARIA, G. "La libertad del intérprete: creación y vínculo en la praxis jurídica", en *Razón jurídica e interpretación* (Messuti, Ed.), Thomson-Civitas, Navarra, 2004.

ZIZEK, S. *Primero como tragedia, después como farsa*, AKAL, Madrid, 2013.

- "Un permanente estado de excepción económica", *New Left Review*, nº 64, 2010.

ANEXO I. JURISPRUDENCIA CITADA

1. Jurisprudencia del Tribunal Constitucional español

STC 11/1981, de 8 de abril

STC 6/1981, de 14 de abril

STC 21/1981, de 15 de junio

STC 25/1981, de 14 de julio

STC 53/1985, de 11 de abril

STC 104/1986, de 17 de julio

STC 170/1987, de 30 de octubre

STC 64/1988, de 12 de abril

STC 107/1988, de 8 de junio

STC 231/1988, de 2 de diciembre

STC 168/1988, de 22 de diciembre

STC 23/1989, de 2 de febrero

STC 37/1989, de 15 de febrero

STC 120/1990, de 27 de junio

STC 171/1990, de 12 de noviembre

STC 197/1991, de 17 de octubre

STC 214/1991, de 11 de noviembre

STC 15/1993, de 18 de enero

STC 254/1993, de 20 de julio

STC 117/1994, de 25 de abril

STC 132/1995, de 11 de septiembre

STC 139/1995, de 26 de septiembre

STC 190/1996, de 25 de enero

STC 104/1996, de 11 de junio

STC 190/1996, de 25 de noviembre

STC 1/1998, de 12 de enero

STC 11/1998, de 13 de enero

STC 94/1998, de 4 de mayo

STC 76/1999, de 26 de abril

STC 134/1999, de 15 de julio

STC 136/1999, de 20 de julio

STC 180/1999, de 11 de octubre

STC 202/1999, de 8 de noviembre

STC 241/1999, de 20 de diciembre

STC 110/2000, de 5 de mayo

STC 115/2000, de 5 de mayo

STC 290/2000, de 30 de noviembre

STC 292/2000, de 30 de noviembre

STC 297/2000, de 11 de diciembre

STC 49/2001, de 26 de febrero

STC 119/2001, de 24 de mayo

STC 156/2001, de 2 de julio

STC 225/2002, de 9 de diciembre

STC 14/2003, de 28 de enero

STC 61/2004, de 18 de mayo

STC 125/2007, de 21 de mayo

STC 177/2007, de 23 de julio

STC 23/2010, de 27 de abril

STC 176/2013, de 21 de octubre

STC 208/2013, de 16 de diciembre

STC 26/2014, de 13 de febrero

STC 58/2018, de 4 de junio

2. Jurisprudencia del Tribunal Supremo español

STS 781/1995, de 26 de julio

STS 3433/1996, de 5 de junio

STS 448/1998, de 18 de mayo

STS 6652/1999, de 25 de octubre

STS 559/2011, de 10 de febrero

STS 511/2012, de 24 de julio

STS 805/2013, de 7 de enero

STS 2245/2013, de 4 de marzo

STS 312/2014, de 5 de junio

STS 696/2014, de 4 de diciembre

STS 557/2015, de 18 de febrero

STS 545/2015, de 15 de octubre

STS 1055/2016, de 11 de marzo

STS 574/2016, de 14 de marzo

STS 1103/2016, de 15 de marzo

STS 210/2016, de 5 de abril

STS 1280/2016, de 5 de abril

STS 1381/2016, de 13 de junio

STS 1382/2016, de 13 de junio

STS 1383/2016, de 13 de junio

STS 1384/2016, de 13 de junio

STS 1385/2016, de 13 de junio

STS 1386/2016, de 13 de junio

STS 1387/2016, de 13 de junio

STS 1388/2016, de 13 de junio

STS 1454/2016, de 20 de junio

STS 1455/2016, de 20 de junio

STS 1456/2016, de 20 de junio

STS 1457/2016, de 20 de junio

STS 1458/2016, de 20 de junio

STS 1459/2016, de 20 de junio

STS 1460/2016,, de 20 de junio

STS 1529/2016, de 27 de junio

STS 1531/2016, de 27 de junio

STS 1532/2016, de 27 de junio

STS 1533/2016, de 27 de junio

STS 1534/2016, de 27 de junio

STS 1535/2016, de 27 de junio

STS 1536/2016, de 27 de junio

STS 1610/2016, de 4 de julio

STS 1611/2016, de 4 de julio

STS 1612/2016, de 4 de julio

STS 1613/2016, de 4 de julio

STS 1615/2016, de 4 de julio

STS 1618/2016, de 4 de julio

STS 1689/2016, de 11 de julio

STS 1690/2016, de 11 de julio

STS 1693/2016, de 11 de julio

STS 1694/2016, de 11 de julio

STS 1695/2016, de 11 de julio

STS 1696/2016, de 11 de julio

STS 1697/2016, de 11 de julio

STS 1797/2016, de 18 de julio

STS 1799/2016, de 18 de julio

STS 1800/2016, de 18 de julio

STS 1801/2016, de 18 de julio

STS 1802/2016, de 18 de julio

STS 1803/2016, de 18 de julio

STS 1805/2016, de 18 de julio

STS 1806/2016, de 18 de julio

STS 1807/2016, de 18 de julio

STS 1808/2016, de 18 de julio

STS 1809/2016, de 18 de julio

STS 1810/2016, de 18 de julio

STS 1910/2016, de 21 de julio

STS 1911/2016, de 21 de julio

STS 1912/2016, de 21 de julio

STS 1913/2016, de 21 de julio

STS 1915/2016, de 21 de julio

STS 1916/2016, de 21 de julio

STS 1917/2016, de 21 de julio

STS 1918/2016, de 21 de julio

STS 1919/2016, de 21 de julio

STS 1920/2016, de 21 de julio

STS 4/2017, de 18 de enero

STS 426/2017, de 6 de julio

STS 446/2017, de 13 de julio

STS 493/2018, de 26 de febrero

STS 388/2018, de 21 de junio

3. Jurisprudencia de la Audiencia Nacional

SAN 5236/2014, de 2 de diciembre

SAN 5129/2014, de 29 de diciembre

SAN 9/2017, de 29 de marzo

SAN 2562/2017, de 19 de junio

SAN 3257/2017, de 13 de julio

SAN 3029/2017, de 18 de julio

SAN 3260/2017, de 25 de julio

SAN 34/2017, de 4 de diciembre

4. Jurisprudencia de las Audiencias Provinciales

SAP Barcelona 486/2013, de 11 de octubre, Sección 14

SAP Barcelona 364/2014, de 17 de julio, Sección 16

5. Jurisprudencia del Tribunal de Justicia de la Unión Europea

STJUE, de 6 de noviembre de 2003, *Swedish Prosecutor's Office v. Bodil Lindqvist*, Asunto C-101/01

STJUE (Gran Sala), de 9 de noviembre de 2004, *British Horseracing Board Ltd and Others v. William Hill Organization Ltd*, Asunto C-203/02, [2004] ECR I-10415

STJUE (Gran Sala), de 29 de enero de 2008, *Productores de Música de España –Promusicae– v. Telefónica de España S.A.U*, Asunto C-275/06

STJUE (Gran Sala), de 16 de diciembre de 2008*, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy*, Asunto C-73/07

STJUE (Sala Tercera), de 7 de mayo de 2009, *College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer,* Asunto C-553/07

STJUE (Gran Sala), de 23 de marzo de 2010, *Google France SARL y Google Inc. v. Louis Vuitton Malletier SA,* Asuntos acumulados C-236/08 y C-238/08

STJUE (Gran Sala), de 9 de noviembre de 2010, *Volkerund Markus Schecke Gbr y Hartmut Eifert v. Land Hessen*, Asuntos acumulados C-92/09 y C-93/09

STJUE (Gran Sala), de 25 de octubre de 2011, *eDate Advertising GmbH v. X*; Olivier *Martinez and Others v. Société MGN Limited*, Asuntos acumulados C-509/09 y C-161/10

STJUE (Gran Sala), de 8 de abril de 2014, *Digital Rights Ireland Ltd v. Minister for Communications and Others; Kärntner Landesregierung v. Michael Seitlinger and Others,* Asuntos acumulados C-293/12 y C-594/12

STJUE (Gran Sala), de 13 de mayo de 2014, *Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, Asunto C-131/12

STJUE (Gran Sala), de 6 de octubre de 2015, *Maximillian Schrems v. Data Protection Commissioner,* Asunto C-362/14

STJUE (Gran Sala), de 21 de diciembre de 2016*, Tele2 Sverige AB v. Post- och telestyrelsen*; *Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis*, Asuntos acumulados C-203/15 y C-698/15

6. Jurisprudencia del Tribunal Europeo de Derechos Humanos

STEDH, *Handyside v. United Kingdom* [1976] 1 EHRR 737 at 754

STEDH *Tyrer c. Reino Unido*, de 25 de abril de 1978

STEDH, *X v. Austria* [1979] 18 D.R. 154 9

STEDH, *Sporrong and Lonnroth v. Sweden* [1982] 5 EHRR 35 at 52

STEDH, *X and Y v. the Netherlands*, de 26 de marzo de 1985, [1985] 8 EHRR 235

STEDH, *Malone v. United Kingdom*, de 26 de abril de 1985, [1985] 7 EHRR 14

STEDH, *Leander v. Sweden*, de 26 de marzo de 1987, Series A Nº 116, [1987] 9 EHRR 433

STEDH, *Gaskin v. United Kingdom*, de 7 de julio de 1989, [1989] 12 EHRR 36

STEDH, *Niemietz v Germany*, de 16 de diciembre de 1992, (App. 13710/88), [1992] 16 EHRR 97

STEDH, *Friel v. Austria*, de 31 enero 1995, Series A Nº 305B, [1995] 21 EHRR 83

STEDH, *Z v. Finland*, 25 de febrero de 1997, (App. 22009/93), [1997]

STEDH, *Bladet Tromso and Stensaas v. Norway*, de 20 de mayo de 1999, (App. 21980/93), [1999] 23 EHRR CD 40

STEDH, *Halford v. United Kingdom* [1997] 24 EHRR 523

STEDH, *Steward-brady v. United Kingdom* [1997] 24 EHRR CD 38

STEDH, *Kopp v. Switzerland* [1998] HRCD 356

STEDH, *Spencer v. United Kingdom*, de 16 enero 1998, (Apps. 28851/95 y 28852/95), [1998] 23 EHRR CD 105

STEDH, *Guerra v. Italy* [1998] 26 EHRR 357

STEDH, *Botta v Italy*, de 24 de febrero de 1998 [1998] 26 EHRR 241

STEDH, *McGinley v. United Kingdom* [1999] 27 EHRR 1

STEDH, *Amann v. Switzerland*, de 16 de febrero de 2000, [2000] 30 EHRR 843

STEDH, *Rotaru v. Romania*, de 4 de mayo de 2000 [2000] 8 BHRC 449

STEDH, *PG v. United Kingdom* [2001] Po LR 325

STEDH, *Pretty v. United Kingdom*, de 29 de abril de 2002, (App. 2346/02), [2002] ECHR 423

STEDH, *Peck v. United Kingdom*, 28 de Enero de 2003, (App. 44647/98), [2003] ECHR 44, (2003) 36 EHRR 41, [2003] 36 EHRR 719

STEDH, *Odièvre v. France*, de 13 de febrero de 2003, TEDH 2003/8

STEDH, *Von Hannover v. Germany* [2004] 24 ECHR 294

STEDH, *Connors v. United Kingdom* [2005] 40 EHRR 9

STEDH, *Babylonová v. Slovakia*, 20 de Junio de 2006, (App. 69146/01) [2008] 46 EHRR 183, ECHR 2006-VIII

STEDH, *Copland v. United Kingdom* [2006] 43 EHRR SE5

STEDH, *Gurgenidze v. Georgia* [2006] 71678/01

STEDH, *L.L. v. France*, de 10 de octubre de 2006

STEDH, *Turek v. Slovakia*, 14 de febrero de 2007, (App. 57986/00), [2007] 44 EHRR 861, ECHR 2006-II

STEDH *Copland v. United Kingdom*, de 3 de abril de 2007

STEDH, *Tysiac v. Poland* [2007] 22 BHRC 155

STEDH, *Dickson v. United Kingdom,* 4 de Diciembre de 2007 [GC], (App. 44362/04), [2008] 46 EHRR 927, ECHR 2007-XIII

STEDH, *Wieser and Bicos Beteiligungen v. Austria* [2008] 46 EHRR 54

STEDH, *Khuzhin and others v. Russia*, 23 de octubre de 2008, (App. 1347/02)

STEDH, *S and Marper v. United Kingdom*, de 4 de diciembre de 2008 [GC], (App. 30562/04 y 30566/04), [2008] ECHR 1851 [2009] 48 EHRR 1169

STEDH, *Times Newspapers v. United Kingdom*, de 10 de marzo de 2009

STEDH, *Reklos v. Greece* [2009] EMLR 16

STEDH, *Gardel v. France*, 17 de diciembre de 2009, (App. 16428/05), ECHR 2009

STEDH, *A v. Croatia*, 14 de octubre de 2010, App No 55164/08

STEDH, *Gillan v. United Kingdom* [2010]

STEDH, *MAK and RK v. United Kingdom* [2010] ECHR 363

STEDH, *Mosley v. United Kingdom*, de 10 de mayo de 2011, [2011] 10 ECHR 774

STEDH, *Von Hannover v. Germany*, de 7 de febrero de 2012 [GC], (N 2) (App. 40660/08 y 60641/08), ECHR 2012

STEDH, *Gillberg v. Sweden*, 3 de abril de 2012 [GC], (App. 41723/06)

STEDH, *Ahmet Yildrim v. Turkey*, de 18 de diciembre de 2012

STEDH, *Avilki,na and others v. Russia*, 6 de junio de 2013, (App. 1585/09)

STEDH, *Delfi AS v. Estonia*, de 10 de octubre de 2013

7. Jurisprudencia de los tribunales británicos

Entick v. Carrington [1765] EWHC KB J98 95 ER 807, King's Bench

Bonnard v. Perryman [1891] 2 Ch. 269

Tolley v. JS Fry & Sons Ltd [1931] AC 333, HL

Bernstein v. Skyviews and General Ltd [1978] QB 479

Community Charge Registration Officers of Runnymede Borough Council v. South Northamptonshire [DA/ 90 24/49/3]

Community Charge Registration Officer of Rhondda Borough Council v. Data Protection Registrar [DA/90 25/49/2]

Kaye v. Robertson [1991] FSR 62

Derbyshire County Council v. Times Newspapers [1993] A.C. 534, Court House of Lords

R v. Ministry of Defence, ex parte Smith [1996] QB 517, Court of Appeal of England and Gal·les

Creation records v. News Group Newspapers Ltd [1997] E.M.L.R. 444

Hunter v. Canary Wharf Ltd [1997] AC 655

Regina v. Brentwood Borough Council, ex parte Peck [1998] EMLR 697 (QBD)

British Gas Trading Limited v. Data Protection Registrar [1998] UKIT DA98 3/49/2

Reynolds v. Times Newspapers and others [1998] 3 WLR 862

McKerry v. Teesdale & Wear Valley Justices [2000] Div Ct

Woolgar v. Chief Constable of Sussex Police and Anor [2000] 1 WLR 25 (CA)

Secretary of State for the Home Dept v. Waiwright [2001] EWCA

W (children) [2001] EWCA Civ 757

A v. B plc [2002] 3 WLR 542

Campbell v. Mirror Group Newspapers Ldt [2002] EWHC 499, Court Queen's Bench Division

B. v. H Bauer Publishing Ltd [2002] EMLR 8

Campbell v. Mirror Group Newspapers Ldt [2004] UKHL 22, Court House of Lords

Edmund Irvine Tidswell Ldt v. Talksport Ldt [2002] EWHC 367

P. v. Wozencroft [2002] 2 FLR 1118

R. v Secretary of State for the Home Department [2002] UKHL 46

Theakston v. MGN Ltd [2002] EMLR 398

Totalize Plc v. The Motley Fool Ltd [2002] 1 WLR 1233

Bellinger v. Bellinger [2003] UKHL 21

Durant v. Financial Services Authority [2003] EWCA Civ 1746

Peck v. United Kingdom [2003] 28 ECHR 44

Wainwright v. Home Office [2003] UKHL 53, 3 WLR 1137, Court House of Lords

Michael Douglas & Catherine Zeta-Jones v. Hello! Ldt [2003] EWHC 2629 (Ch), EEWHC 786 (Ch), Court Chancery Division

Campbell v. Mirror Group Newspapers Ldt [2004] UKHL 22, Court House of Lords

Ghaidan v. Godin-Mendoza [2004] UKHL

Nigel Roberts v. Media Logistics [2005]

Smith v. Lloyds TSB Bank Plc [2005] EWHC 246

McKennitt v. Ash [2006] EWCA Civ 1714

Microsoft Corporation v. Paul Martin *McDonald* (trading as *Bizads UK*) [2006] EWHC 3410 (Ch), All ER (D) 153, High Court of Justice Chancery Division

Ezsias v. Welsh Ministers [2007] All ER (D) 65 (Dec)

Johnson v. Medical Defence Union [2007] EWCA Civ 262

Murray v. Big Pictures (UK) Ltd [2008] EWCA Civ 446

RST v. UVW [2009] EWHC 2448 (QB)

Edem v. IC & Financial Services Authority [2014] EWCA Civ 92

Secretari of State for the Home Department v. Watson & Others, C1/2015/2612 & 2613 [2018] EWCA Civ 70, Court of Appeal (Civil Division) of High Court of Justicie Queen's Bench Division

8. Jurisprudencia de los tribunales norteamericanos

Roberson v. Rochester Folding Box Co., de 27 de junio de 1902, 64 N.E. 442 (NY)

Sidis v. F. R. Publishing Corp, U.S. Court of Appeal for the Second Circuit - 113 F. 2d 806 (2d Cir. 1940), 22 de julio de 1940.