Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Programa de Doctorado en Derecho

TESIS DOCTORAL

LOS DATOS PERSONALES EN LA WEB: INTERVENCIÓN DE LOS PODERES PÚBLICOS

DIANA PAOLA GONZÁLEZ MENDOZA

Oviedo, 2021

Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

RESOLUCIÓN DE PRESENTACIÓN DE TESIS DOCTORAL

Año Académico: 2020/2021.

1.- Datos personales del autor de la Tesis		
Apellidos: González Mendoza	Nombre: Diana Paola	
DNI/Pasaporte/NIE:	Teléfono:	Correo electrónico:

2.- Datos académicos
Programa de Doctorado cursado: Programa de doctorado en Derecho. Los retos del Derecho en una sociedad en transformación.
Órgano responsable: Comisión Académica
Departamento/Instituto en el que presenta la Tesis Doctoral: Departamento de Derecho público

Título definitivo de la Tesis	
Español/Otro Idioma: Los datos personales en la web: intervención de los poderes públicos.	Inglés: Personal data on the web: Public Authorities action.
Rama de conocimiento: Derecho público (Derecho administrativo).	
Señale si procede: ☒ Mención Internacional ☐ Idioma de presentación de la Tesis distinto al español ☐ Presentación como compendio de publicaciones	

3.- Autorización del Presidente de la Comisión Académica	
D.: Julio Carbajo González	DNI/Pasaporte/NIE:
Departamento/Instituto: Departamento de Derecho privado y de la empresa.	

Resolución: La Comisión Académica del Programa de Doctorado en Derecho. En su reunión de fecha 22 de enero de 2021, acordó la presentación de la tesis doctoral a la Comisión de Doctorado, previa comprobación de que la tesis presentada y la documentación que la acompaña cumplen con la normativa vigente, según lo establecido en el Art.32.8 del Reglamento de los Estudios de Doctorado, aprobado por el Consejo de Gobierno, en su sesión del día 20 de julio de 2018 (BOPA del 9 de agosto de 2018)

Además, informa:

	Favorable	Desfavorable
• Mención Internacional	☒	☐
• Idioma	☒	☐
• Presentación como compendio de publicaciones	☐	☐

Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

RESUMEN DEL CONTENIDO DE TESIS DOCTORAL

1.- Título de la Tesis	
Español/Otro Idioma: Los datos personales en la web: intervención de los poderes públicos.	Inglés: Personal data on the web: Public Authorities action.

2.- Autor	
Nombre: Diana Paola González Mendoza	DNI:
Programa de Doctorado: en Derecho. Los retos del Derecho en una sociedad en transformación.	
Órgano responsable: Comisión académica del Programa de doctorado en Derecho. Los retos del Derecho en una sociedad en transformación.	

RESUMEN (en español)

Las nuevas tecnologías de la información y comunicación (TIC) han cambiado sin duda la forma de comunicarnos y expresarnos. Este nuevo entorno digital ha permitido que la información se transmita de una forma más rápida y se genere una cantidad ingente de datos, lo que ha acelerado el proceso de globalización. Las personas ahora desarrollan su personalidad a través de este nuevo entorno digital, por lo que su esfera jurídica puede resultar afectada, ya sea por acciones de otros usuarios de los Servicios de la Sociedad de la Información y Comunicación o bien por las propias tecnologías. Esta situación puede ser extrapolable perfectamente a las relaciones que los usuarios mantienen con las diversas Administraciones públicas. Es por ello, que este trabajo de investigación está dedicado de manera principal al estudio del derecho a la protección de datos y la influencia que han tenido las TIC en la actividad de los poderes públicos, especialmente en la actividad de las Administraciones públicas.

El primero de los capítulos está dedicado al estudio de algunos de los derechos fundamentales que consideramos tienen una mayor afectación en el entorno digital. De manera que, se analiza inicialmente la dignidad de las personas, como uno de los mayores axiomas en los que tienen sustento los demás derechos fundamentales, además de valorar la incidencia que se produce en los derechos de la personalidad y los derechos a la libertad de expresión e información.

El segundo de los capítulos está destinado al estudio del derecho fundamental a la protección de los datos personales, ya que también puede afectarse de manera grave por los diversos agentes que intervienen en este nuevo espacio digital. De modo que se analizan sus antecedentes legislativos en sus distintos ámbitos: europeo, comunitario y nacional, su evolución normativa y su interpretación jurisprudencial, hasta llegar al escenario normativo actual: 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 (RGPD) como hito en la materia y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) que se encarga de complementar al RGPD. En este capítulo se hace una especial referencia al «derecho al olvido», tras su configuración como tal en la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 y su posterior incorporación al RGPD y en la LOPDGDD.

El tercero de los capítulos estará dedicado a las autoridades de control como garantes del derecho a la protección de datos personales, por lo que se analiza su configuración, sus competencias, funciones y poderes de la autoridad a nivel estatal, así como de las autoridades a nivel autonómico. En el mismo también se incorpora un estudio de los mecanismos de cooperación y coherencia establecidos en el RGPD.

El cuarto y último capítulo está dedicado al estudio de tratamiento de datos personales llevado a cabo por las Administraciones públicas. Por lo que se analiza su base jurídica de licitud, sus principales obligaciones, los efectos del incumplimiento de la normativa y el ciclo de vida del tratamiento de los datos personales. También se dedica una parte al estudio de la compatibilidad del tratamiento ulterior relacionado con determinados fines: archivísticos, estadísticos y de investigación científica. Igualmente, se incluye una parte específica al

equilibrio entre la transparencia y el derecho a la protección de datos. Finalmente, se hace referencia en materia de contratación cuando las Administraciones externalizan las figuras del encargado de tratamiento de datos y del delegado de tratamiento de datos.

RESUMEN (en Inglés)

The new information and communication technologies (ICT) have undoubtedly changed the way we communicate and express ourselves. This new digital environment has allowed information to be transmitted more quickly and a vast amount of data to be generated, which has accelerated the process of globalization. People now develop their personality through this new digital environment, so their legal sphere may be affected either by the actions of other users from the Information and Communication Society Services or by the new technologies themselves. This situation can be perfectly extrapolated to the relations that users maintain with the various public administrations. Therefore, this research work is mainly devoted to the study of the data protection right and the influence that ICTs have had on the activity of public authorities, especially on the activity of public administrations.

The first chapter is dedicated to the study of some of the fundamental rights that we consider to be affected the most by the digital environment. Thus, the dignity of individuals is initially analyzed as one of the major axioms on which other fundamental rights are based, in addition to assessing the impact on the rights of the personality and the rights to freedom of speech and information.

The second chapter is devoted to the study of the fundamental right to personal data protection, since it can also be seriously affected by the different agents that intervene in this new digital space. Therefore, its legislative background is analyzed in its different fields: European, communitarian and national, its regulatory evolution and its jurisprudential interpretation, until reaching the current regulatory scenario: Regulation (EU) 2016/679 of the European Parliament and Council, of April 27, 2016, on the protection of individuals with regard to the processing of personal data and the free movement of such data (RGPD, according to its Spanish acronym) and repealing Directive 95/46/EC as a milestone in the matter and the Organic Law 3/2018 of December 5, Protection of Personal Data and guarantee of digital rights (LOPDGDD, according to its Spanish acronym) which complements the RGPD. In this chapter, special reference is made to the "right to be forgotten", after its configuration as a right in the Ruling of the Court of Justice of the European Union of May 13th, 2014 and its incorporation to the RGPD and the LOPDGDD.

The third chapter will be dedicated to the control authorities as guarantors of the right to personal data protection, and hence their configuration, competencies, functions and powers of the State-level authority, as well as those of the regional authorities. This chapter also includes the cooperation and coherence mechanisms established in the RGPD.

The fourth and last chapter is dedicated to the study of personal data processing conducted by public administrations. Its legal basis of legality, its main obligations, the effects of non-compliance with the regulations and the life cycle of personal data processing are analyzed. In this context, a part of the study is also dedicated to the compatibility of the subsequent treatment related to certain purposes: archival, statistical and scientific research. In addition, a specific part is also dedicated to the balance between transparency and the right to data protection. Finally, reference is made to the procurement procedures when the Administrations outsource the figures of the data processor and the data processing officer.

SR. PRESIDENTE DE LA COMISIÓN ACADÉMICA DEL PROGRAMA DE DOCTORADO EN DERECHO.

Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Programa de Doctorado en Derecho

TESIS DOCTORAL

LOS DATOS PERSONALES EN LA WEB: INTERVENCIÓN DE LOS PODERES PÚBLICOS

DIANA PAOLA GONZÁLEZ MENDOZA

Directores

DR. D. LEOPOLDO TOLIVAR ALAS

DRA. DÑA. MIRIAM CUETO PÉREZ

Oviedo, 2021

ÍNDICE

ABREVIATURAS EMPLEADAS

AEPD	Agencia Española de Protección de Datos
AN	Audiencia Nacional
ARCO	Derechos de acceso, rectificación, cancelación y oposición.
CC	Código Civil
ccTLDs	Dominio de nivel superior de código de país.
CDFUE	Carta de los Derechos Fundamentales de la Unión Europea.
CE	Constitución Española
CEDH	Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales
Cfr.	Compárese.
Coord.	Coordinador.
CP	Código Penal.
DNI	Documento Nacional de Identidad.
Ed.	Editorial.
EIPD	Evaluación de impacto en la protección de datos.
ETJUE	Estatuto del Tribunal de Justicia de la Unión Europea.
et al.	*Et alli* (otros autores).
EURid	Registro Europeo de Dominios de Internet.
Dle	Diccionario de la lengua española.
DUDH	Declaración Universal de Derechos Humanos.
DSCD	Diario de Sesiones del Congreso de los Diputados.
F.D.	Fundamento de Derecho.

F.J.	Fundamento Jurídico.
GB	GigaBytes.
GT29	Grupo de trabajo del art. 29.
ICANN	Corporación de Internet para la asignación de nombres y número.
Ib.	(*ibídem*) misma obra y distinta página.
Íd.	(*ídem*), misma obra y misma página.
LO	Ley Orgánica.
LODP	Ley Orgánica de Protección de Datos de Carácter Personal
LOPJ	Ley Orgánica del Poder Judicial.
LRJCA	Ley Reguladora de la Jurisdicción Contencioso-administrativa.
LSSI	Ley de Servicio de la Sociedad de la Información y del Comercio electrónico
Núm.	Número
NTIC	Nuevas tecnologías de la información y comunicación.
PIDCI	Pacto Internacional de Derechos Civiles y Políticos
op. cit.	*opus citatum* (obra citada).
RAE	Real Academia Española
RD	Real Decreto
RGPD	Reglamento General de Protección de Datos
SAN	Sentencia de la Audiencia Nacional
SRS	Servicio de Red Social
STC	Sentencia del Tribunal Constitucional.
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea.
STS	Sentencia del Tribunal Supremo.

TC	Tribunal Constitucional de España.
TIC	Tecnologías de la información y comunicación
TJUE	Tribunal de Justicia de la Unión Europea
TFUE	Tratado de Funcionamiento de la Unión Europea
Trad.	Traducción
Vid.	*videtur* (véase)

INTRODUCCIÓN

A mediados del año 2014 recuerdo haber leído en menos de ciento cuarenta caracteres una entrada que anunciaba una sentencia del Tribunal de Justicia de la Unión Europea cuya temática era el derecho a la protección de datos personales y «el derecho al olvido». A continuación, pulsé en un enlace que me dirigía a una nota periodística que hablaba sobre la existencia de un nuevo derecho, sin embargo, a mi parecer era demasiado pronto para anunciar la emergencia de este, pues desde la promulgación de la Constitución Española hasta el año 2000, aún se debatía si el contenido del art. 18.4 era instrumental de los derechos de la personalidad contenidos en el art. 18.1 o si, por el contrario, el derecho a la protección de datos personales tenía un objeto propio. Este acontecimiento, por absurdo que parezca despertó mi interés en el desarrollo de los derechos en el ámbito digital. A partir de ese momento comencé a plantearme preguntas relacionadas con los servicios de la sociedad de la información (SSI), el funcionamiento de las nuevas tecnologías y su repercusión en los derechos de las personas y todo ello, finalmente me condujo a la hora de hacer la elección de tema para mi tesis doctoral al ámbito de lo público, especialmente a la valoración del desarrollo de la actividad de los poderes públicos a través de la web como punto de partida.

Sin duda los datos en el ámbito tecnológico han cobrado especial relevancia, ya que a partir de estos se pueden desarrollar nuevos y mejores productos, así las actividades profesionales o comerciales realizadas por los particulares, ya sean personas físicas o jurídicas, pero también los datos son relevantes para las Administraciones públicas ya que estas tienen un extenso e intenso conocimiento de datos vinculados a las personas, cuya acumulación se produce desde el momento exacto de su nacimiento o incluso antes a través de la historia clínica de la madre, por tanto, los datos van aumentando según el individuo crece y se relaciona con el sector público. Por tanto, la Administración pública desempeña un rol de gran importancia ya que conoce un número de datos más allá de lo que imaginemos sobre la vida de las personas. En consecuencia, la Administración pública se configura como responsable del tratamiento de datos personales que identifican o hacen identificable a la persona. No obstante, las Administraciones públicas están

sometidas a la ley y al Derecho por mandato constitucional, pero cuentan con una serie de prerrogativas que imposibilitan un plano de igualdad entre estas y los ciudadanos, pues su fin último es cumplir los intereses generales. Por este motivo se ha elegido a las Administraciones públicas, de manera que el objetivo principal de este trabajo de investigación es conocer cómo repercuten las tecnologías de la información y comunicación (TIC) en el tratamiento de datos llevado a cabo por el sector público y, a su vez, conocer cómo desempeña el papel de garante del derecho fundamental a la protección de datos personales.

En este sentido hay que abordar los cambios que ha sufrido la sociedad a finales del siglo XX como consecuencia de la mejora de Internet y de las herramientas creadas a su alrededor, como lo es la web. Esta última ha experimentado cambios sustanciales en su configuración y funcionamiento desde su creación hasta nuestros días. Actualmente se habla de la existencia de una web semántica, que relaciona los datos obtenidos a partir de la navegación de los usuarios para darle sentido a los resultados de las búsquedas. A través de la web se prestan SSI, entre los que destacan los servicios de intermediación como redes sociales, blogs, páginas web y motores de búsqueda. Este tipo de servicios han permitido que sus usuarios se hayan convertido en «prosumidores», es decir, que producen y consumen contenido en múltiples formatos a la vez. Es evidente que este tipo de servicios han cambiado la forma de publicar y transmitir información entre los usuarios, en buena parte por su inmediatez. Los cambios descritos anteriormente, han ido ocurriendo de manera progresiva en distintas partes del mundo, lo que ha permitido la visibilización de realidades ya existentes, pero poco conocidas, y acelerando también el proceso de globalización. Igualmente, la utilización de estos medios ha contribuido a la crítica y reflexión de los ciudadanos e incluso se ha utilizado como medio para practicar algún tipo de activismo, como los movimientos de adhesión a diferentes causas en la web. Sin embargo, los SSI pueden resultar invasivos y sus finalidades desproporcionadas con el servicio que prestan. La onda expansiva que genera la utilización de las tecnologías de la información y comunicación (TIC) por los usuarios ha permitido aumentar de manera exponencial la difusión de ideas, la transmisión de información y consecuentemente el daño en la esfera jurídica de los ciudadanos. En tales casos la

propia naturaleza de este medio hace más vulnerables a las personas a este tipo de ataques.

Por ello, en la estructura de este trabajo, se dedicará el Capítulo I al estudio de la incidencia de la dignidad de la persona, como valor jurídico supremo y uno de los mayores axiomas en los que se sustentan los derechos fundamentales, en el ámbito digital, junto con los derechos a la personalidad, es decir, el derecho al honor, a la propia imagen y a la intimidad personal y familiar, contenidos en el apartado primero del art. 18 de la CE, y los derechos a la libertad de expresión e información incluidos en los incisos a) y d) del art. 20.1 de la CE. Estos derechos fundamentales pueden ser transgredidos por o a través de los SSI, por tanto, la responsabilidad puede ser de los usuarios, de los prestadores de SSI o de ambos. Es importante conocer qué valores, principios y derechos tienen proyección en este nuevo espacio digital. Estos dos bloques de derechos ya colisionaban con anterioridad al auge de los SSI con motivo de la manifestación de expresiones o informaciones relacionadas con los demás, dirigidas al público en general por los medios tradicionales. Ante el cambio tecnológico en muchas de las ocasiones se requiere la realización de una ponderación de derechos al caso concreto para conocer la prevalencia de uno u otro según sea el supuesto y la interpretación de la normativa vigente aplicable por los órganos jurisdiccionales, para así poder determinar también la responsabilidad de quienes realizan o intervienen en la vulneración y los medios para resarcir el daño. Durante el análisis individualizado de los derechos de la personalidad destacan determinados aspectos relacionados con cada uno de ellos, que tienen especial importancia en el ámbito digital. Como mencionamos anteriormente, el estudio de los derechos fundamentales no puede realizarse de manera aislada, de tal forma que, además de realizar un estudio por separado de su incidencia, se analizarán algunas de las posibles transgresiones, como consecuencia del ejercicio de otro u otros derechos de la misma naturaleza.

En las colisiones entre el derecho al honor y los derechos a la libertad de expresión e información veremos cómo se aplican los mismos criterios para solventar este tipo colisiones, tal y como si se realizasen en el ámbito analógico, pero considerando las peculiaridades del medio digital. En este sentido es importante señalar que comparativamente el daño en la esfera jurídica de la persona es mucho

mayor si se utilizan medios digitales en relación con los medios escritos o tradicionales como consecuencia de la onda expansiva y global que caracteriza a la web, ya que la publicación dónde se desmerece a una persona es visible por una cantidad ingente de personas y que puede incluso tener repercusión en los medios tradicionales. En este sentido los servicios de intermediación pueden coadyuvar y ser parte de la reparación del daño.

En cuanto al derecho a la intimidad por el que se protege aquella esfera reservada a su titular e inaccesible a las demás personas, durante su análisis en este trabajo se determinará cómo puede verse afectado por publicaciones de otras personas. En este sentido, veremos cómo se regulan aquellas herramientas utilizadas por los servicios de la sociedad de la información que puedan afectar tanto a la intimidad de las personas como a su derecho a la protección de datos. Este tipo de herramientas han evolucionado de tal manera que la regulación actual aplicable a las mismas se antoja cuanto menos insuficiente, al igual que dispar en su aplicación. En este sentido, las transgresiones de los derechos fundamentales ahora no solo encuentran su origen en publicaciones de los usuarios, además han entrado al juego este tipo de tecnologías, entre las que destacan las «cookies».

Con respecto al derecho a la propia imagen en el ámbito digital, que protege la cualidad diferenciadora de las personas reflejo de su aspecto físico su objeto de protección no ha mutado en el ámbito digital. Sin embargo, resulta habitual que se trasgreda este derecho fundamental junto otros derechos de la personalidad como consecuencia de publicaciones de usuarios realizadas sin el consentimiento de su titular a través de los servicios de intermediación, incluso puede vulnerarse este derecho fundamental si los usuarios otorgan su consentimiento de manera inicial y, posteriormente, deciden retirarlo.

En relación con los derechos a la libertad de expresión e información, se explicarán los elementos diferenciadores de cada uno en el ámbito digital. Es un hecho que las manifestaciones de ideas o juicios de valor en muchas ocasiones no resultan bienintencionadas. En este sentido, el problema de estas manifestaciones e informaciones en este tipo de medios es su alcance, las TIC tienen un efecto multiplicador que permite a usuarios de todo el mundo acceder a estas informaciones casi al instante. Lo cual ocurre también con comentarios ultrajantes

y subjetivos sobre otras personas que algunas veces incluso van acompañados de imágenes sobre su persona o familias para identificar plenamente al sujeto objeto de la información. Este tipo de manifestaciones de la libertad de expresión resultan claramente desproporcionadas en algunos casos, con lo cual se tendrá que ponderar la prevalencia o no de este derecho en el caso concreto. Del mismo modo, el derecho a la información deberá ser moderado en base a los criterios de interpretación, solo que en este caso la profesión de la persona, la veracidad y el sujeto objeto de las informaciones resultarán cruciales para dirimir este tipo de controversias. Como consecuencia de lo anterior, se analizarán los criterios de ponderación para determinar si prevalecen los derechos de la personalidad o los derechos a la libertad de expresión e información, su grado de protección, el medio utilizado para la realización de la vulneración y cómo influye que estos derechos se desarrollen en una sociedad libre y democrática como la nuestra.

Una vez analizados estos derechos consideramos importante dedicar un capítulo al derecho a la protección de datos personales pues también puede verse implicado en la colisión de estos dos bloques de derechos fundamentales o colisionar de manera independiente con otros derechos de esta naturaleza. Pensemos, por ejemplo, en una publicación por medio de la cual un usuario atente contra el honor de una persona y publique los datos identificativos de este último, incluida su imagen con expresiones vejatorias. Otro ejemplo lo encontraríamos en publicaciones realizadas por periodistas en el ejercicio de su profesión sobre la vida íntima de una determinada persona sin su consentimiento e incluya datos de carácter personal que la identifique o la haga identificable. En muchos casos los usuarios sin darse cuenta pretendiendo alcanzar determinado estatus de popularidad van introduciendo información sobre su día a día en distintos formatos: fotos, vídeos, entradas sobre sus hábitos, vida personal y familiar. En este tipo de servicios además se puede obtener información cruzada obtenida de publicaciones realizadas por otros usuarios como fotografías grupales, la utilización de etiquetas en las entradas a los muros o entradas de blogs o, la realización de publicaciones directamente en el muro de una persona en distintas redes sociales. Este tipo de publicaciones podrán ser visualizadas por los «amigos» de la persona que publica el contenido y, en algunos casos incluso en las redes sociales de esa tercera persona.

Las redes sociales también tienen determinadas funciones que permiten conocer información valiosa de los usuarios, por ejemplo, por defecto se obtienen información sobre las preferencias de contenido de los usuarios, lo cual permite generar un perfil individualizado sobre la publicidad que deberá visualizar el usuario a partir de sus preferencias. Por lo anteriormente expuesto se intentará explicar con claridad el objeto y el contenido del derecho a la protección de datos personales, cuyo punto de partida será su evolución normativa en distintos ámbitos: el europeo, el comunitario y el nacional. Durante el análisis de este derecho se manera paralela igualmente se analizarán cómo los SSI afectan al derecho a la protección de datos personales de los usuarios. Siguiendo esta línea, se aludirá a uno de los primeros instrumentos normativos en desarrollar el derecho a la protección de datos en el ámbito europeo: el Convenio 108 del Consejo de Europa, el cual se ha ido adaptando poco a poco a la realidad actual, por medio de la incorporación de protocolos, el más reciente es del año 2018 que robustece el nivel de protección en este ámbito. Respecto al ámbito comunitario se hará referencia a la Directiva 95/46/CE, por la cual se protege por primera vez en la Unión el derecho a la protección de datos personales. En este contexto, también se abordará la normativa comunitaria que se introdujo durante su periodo de vigencia que completa la regulación sobre de los SSI y sus agentes intervinientes, con la finalidad de determinar su alcance e importancia.

En cuanto a la evolución normativa en el ámbito nacional del derecho a la protección de datos se describirá su temprana regulación dada por la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, la que era incluso anterior a la normativa en la materia emitida por la Unión. Posteriormente, como consecuencia de la transposición de la Directiva 95/46/CE se aprueba la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal y su reglamento. Un año después de la publicación de esta LO, el Tribunal Constitucional emite una sentencia que supone un antes y un después en la configuración del derecho a la protección de datos. A partir de la STC 292/2000 de 30 de noviembre, se reconoce el encaje constitucional del derecho a la protección de datos personales como derecho fundamental, con contenido y objeto propio respecto a los derechos de la personalidad.

Según transcurría el tiempo y se desarrollaban nuevas tecnologías la regulación a nivel comunitario y nacional comenzaba a resultar insuficiente. En este sentido, el contenido de la Directiva 95/46/CE se veía comprometido por las normas de transposición en cada Estado miembro de la UE, de modo que su aplicación no era homogénea, y aunque sus principios seguían vigentes se necesitaba un marco jurídico nuevo. En el año 2012 por iniciativa de la Comisión Europea se empieza a gestar un nuevo reglamento que sustituirá a la Directiva 95/46/CE con el objetivo de paliar la insuficiencia regulatoria en la materia debido a la evolución tecnológica. 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 (RGPD) ve la luz en el año 2016, sin embargo, es aplicable de manera directa en todos los estados miembros a partir del 28 de mayo de 2018.

El RGPD supone un hito en la protección de datos, especialmente en lo referente a la regulación de los servicios de la sociedad de la información, las obligaciones a cargo del responsable del tratamiento y lo relativo al consentimiento. Una de las principales novedades que aborda es la responsabilidad proactiva a cargo de los responsables del tratamiento de datos. Con este nuevo reglamento se deberá minimizar la cantidad de datos a tratar, pudiéndose adoptar medidas de seudonimización, esta última consiste según el RGPD en realizar el tratamiento de datos de manera que no puedan atribuirse a un determinado sujeto, a menos de que se cuente con información adicional, la cual debe estar separada del resto de datos. El RGPD también introduce nuevos derechos como el de portabilidad, limitación del tratamiento y a no ser objeto de decisiones individuales automatizadas a partir de herramientas tecnológicas (y que tengan efectos jurídicos sobre este o afecte de algún modo similar). Otra cuestión que introduce y destaca por su novedad es la configuración de un sistema de cooperación entre autoridades de control, al igual que la implementación de un mecanismo de coherencia a cargo del Comité Europeo de Protección de Datos. Este Comité sustituye al Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE, como organismo europeo de supervisión en la materia a nivel comunitario.

Es evidente que el nuevo panorama comunitario en la materia ha influido también en la actualización de la normativa nacional y, a pesar de que el RGPD se debe aplicar de manera directa, a nivel nacional se necesitaba, más que armonizar, completar algunos aspectos que son competencia de los Estados o que el propio reglamento delega al mismo, sin que su aplicación deje de ser coherente y efectiva dentro de la UE, de forma que se aprueba en este sentido la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Durante el tiempo comprendido entre el Convenio 108 hasta la transposición de la normativa comunitaria en España, los motores de búsqueda han evolucionado rápidamente, los resultados que se obtienen son cada vez más precisos y cuantiosos, debido a la utilización de herramientas tecnológicas como cookies, la memoria caché etc. Los buscadores web son una herramienta tecnológica con gran aceptación y utilización por la mayoría de la población, permiten obtener un listado con muchos sitios web relacionados con el parámetro de búsqueda. En relación con lo anterior este servicio de intermediación también nos permite obtener resultados a partir del nombre de las personas como parámetro de búsqueda, de manera que pueden verse afectados varios derechos inherentes a la persona, especialmente el derecho a la protección de datos. En este sentido, el TJUE dicta la sentencia de 13 de mayo de 2014, por la cual se resuelven cuestiones prejudiciales relacionadas con la aplicabilidad de la normativa comunitaria y nacional en materia de protección de datos y, si determinados derechos contenidos en dicha normativa podían ser ejercitables frente a los motores de búsqueda con el objeto de eliminar enlaces obtenidos a partir de búsquedas a partir del nombre de una persona. Como se mencionó anteriormente, a partir de esta sentencia se comienza una discusión doctrinal y jurisprudencial relacionada con los alcances de la configuración del derecho al olvido digital, ejercitable frente a los motores de búsqueda. Alguna parte de la doctrina tempranamente consideraba que este derecho de configuración jurisprudencial era una manifestación del derecho a la protección de datos personales o un «haz de facultades» de este, concretamente lo relacionaban con el derecho de cancelación que preveía la Directiva 95/46/CE y la LO 15/1999, de 13 de diciembre y con el valor supremo de la dignidad de la persona.

A partir de este momento se producen numerosas sentencias tanto en el ámbito contencioso-administrativo como en el civil y, se comienza a elaborar el referido RGPD, en el cual se pretendía incorporar el contenido de la STJUE de 13 de mayo de 2014, sin embargo, a lo largo del proceso de elaboración de la norma sufre determinadas modificaciones que distan del contenido de la referida sentencia. Este derecho también se introduce en el texto de la LOPDGDD en los mismos términos del RGPD, pero además se añade un precepto específico que sobre el derecho al olvido en búsquedas de Internet.

Una vez que conocemos el contenido del derecho a la protección de datos y su relación con otros derechos, se procede de lleno al estudio del objeto principal de esta tesis doctoral que es conocer la intervención de los poderes públicos en el tratamiento automatizado de datos desde una doble perspectiva: la de garante y la de responsable. El sector público, como bien sabemos, está sometido a la ley y al Derecho y tiene como objeto cumplir con intereses generales, sin embargo, también se encarga del correcto cumplimiento de la normativa en la materia a través de autoridades de control que vigilan el correcto cumplimiento del RGPD y de la LOPDGDD. Debido a la notable función que desempeñan estas autoridades requieren ser dotadas de determinadas características de modo que nada ni nadie interfiera en el cumplimiento de sus fines, por lo que su configuración, sus poderes y funciones son objeto de estudio en este trabajo de investigación, entre los que destacan los poderes de investigación y correctivos, atendiendo a la gravedad de las infracciones y los criterios a tener en cuenta para la imposición de las posibles sanciones. Al hilo de lo anterior, se ha de señalar que en el Estado compuesto en el que vivimos existen varias autoridades de control: la Agencia Española de Protección de Datos, la Agencia Vasca de Protección de Datos, la Autoridad Catalana de Protección de Datos y con algunas peculiaridades el Consejo de Transparencia y Protección de Datos; todas y cada una de ellas deberán cumplir con lo establecido en el RGPD, como consecuencia, apenas habrá variación competencial entre la autoridad estatal y las autonómicas debido al derecho europeo unificador, salvo en determinados sectores concretos. Como se refirió anteriormente, dos de las novedades introducidas por el RGPD relacionadas con este tipo de autoridades son los mecanismos de cooperación y de coherencia, por ello a lo largo del capítulo III se

analizará el marco competencial de las autoridades de control cuando el responsable o el encargado realice tratamientos de datos transfronterizos. En relación con el Comité Europeo de Protección de Datos en este trabajo se analizará la función de velar por la coherente aplicación del RGPD en todo el territorio de la UE, a través de la emisión de dictámenes con el objeto de dirimir las controversias que puedan suscitarse entre las diferentes autoridades de control en el mecanismo de ventanilla única o, sobre cuestiones interpretativas que le sean planteadas.

El capítulo IV estará dedicado al análisis del tratamiento de datos personales realizado por el sector público, por este motivo primeramente se estudiarán aquellas bases jurídicas que hacen posible que actúe como responsable del tratamiento y se efectúe de manera lícita de acuerdo con el RGPD. Se continuará con el estudio de las principales obligaciones que corren a cargo de este tipo de responsables, concretamente la incorporación de un delegado de protección de datos y el establecimiento de medidas técnicas y organizativas relacionadas con la seguridad de los datos, como son la evaluación de impacto, la evaluación de riesgos y las medidas de seguridad contenidas en el Esquema Nacional de Seguridad (ENS), así como el registro de actividades de tratamiento de cada una de las autoridades administrativas. Igualmente, en este Capítulo IV se estudiarán los efectos del incumplimiento del nuevo marco jurídico en la materia por el sector público, incluyendo las formas en que las administraciones públicas son sancionadas y la forma de exigir su responsabilidad patrimonial en caso de que dicho incumplimiento le ocasione un daño al interesado.

Como sabemos la relación existente entre el sector público y el ciudadano abarca así todos los aspectos imaginables. En este sentido se han elegido determinados sectores y finalidades concretas, para ser desarrolladas en este trabajo de investigación desde la perspectiva de la protección de datos, que están presentes en la vida diaria de los ciudadanos y también aquellas que resultan de gran importancia en la vida democrática de nuestro país, como son el ciclo de vida de los datos personales cuando el tratamiento de datos se realiza como consecuencia de la relación por medios electrónicos entre el ciudadano y la administración, los tipos de transparencia existentes y su relación con el derecho a la protección de datos personales como límite, el tratamiento de datos automatizado

en el sector sanitario y, el tratamiento de datos con fines archivísticos, estadísticos y de investigación científica o histórica. Este estudio se realizará sistemáticamente de manera separada.

En cuanto al tratamiento de datos realizado en la administración electrónica primero se señalan las diferentes definiciones establecidas al efecto en la legislación y por la doctrina. Posteriormente se abordará la influencia de la introducción de TIC y sus efectos, seguido de su evolución normativa y los presupuestos para el funcionamiento de esta: el Esquema Nacional de Interoperabilidad y el Esquema Nacional de Seguridad. Una vez determinados estos supuestos, el análisis de la relación existente entre el derecho a la protección de datos con la administración electrónica se realizará a partir del ciclo de vida de los datos personales, es decir, todas las etapas por las que pasan los datos personales de los ciudadanos: recogida de datos, clasificación y almacenamiento, comunicación de datos, conservación y destrucción. En este caso no se trata de un estudio exhaustivo de todos los cambios ni de la implementación de todas las TIC, pero sí se abordarán las cuestiones que se estiman más relevantes.

En este Capítulo se abordará también la relación entre la transparencia y la protección de datos personales. El análisis de esta cuestión partirá del estudio de las divergencias en la regulación de la materia en distintos ámbitos: internacional, europeo, comunitario y nacional. Posteriormente se introducirán los tipos de transparencia existentes. Siguiendo esta línea, para el caso de la transparencia activa o también llamada publicidad activa, conoceremos que autoridades están obligadas a publicar en su portal información relacionada con su funcionamiento, organización, normativa aplicable, información económica, presupuestaria y estadística, junto con la lista de tratamientos de datos personales que efectúe. En este caso, uno de los límites de la transparencia activa es precisamente el derecho a la protección de datos personales, por tanto, se explicará su alcance. Por otro lado, en relación con la vertiente pasiva de la transparencia se analizarán los criterios de ponderación que permiten determinar la prevalencia de alguno de estos dos derechos y sus matices, dependiendo del tipo de datos a los que se pretenda acceder por medio de una solicitud.

En lo concerniente a la reutilización de datos o transparencia colaborativa, se analizará su configuración normativa tanto a nivel comunitario como nacional y, como se le aplican los mismos límites previstos en la Ley 19/2013, de 9 de diciembre, de transparencia, buen gobierno y acceso a la información pública, por tanto, le es aplicable el límite del derecho a la protección de datos en determinados casos. En este apartado se señalarán los cambios introducidos por la Directiva 2019/1024, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público (en estos momentos su transposición al sistema jurídico español aún no se llevado a cabo).

Respecto a los tratamientos de datos con determinadas finalidades que tienen especial importancia para la consecución de los intereses generales y de obligado cumplimiento para las Administraciones públicas y a las que expresamente hace mención el RGPD, como son aquellas vinculadas al archivo, a los fines estadísticos y a los de investigación científica o histórica. En consecuencia, se analizarán a la luz de la normativa vigente en protección de datos y su configuración en la legislación a nivel estatal, sin perjuicio de la concurrencia competencial en el ámbito autonómico. Es importante señalar que estos tres ámbitos materiales están estrechamente relacionados, pues están orientados a la generación de conocimiento y, a su vez están relacionados con otras obligaciones de las Administraciones públicas como la reutilización de datos, la transparencia activa y la eficacia en la utilización de recursos financieros. En el estudio de los tratamientos de datos con fines de archivo, estadísticos y de investigación científica o histórica se detallarán las medidas técnicas y organizativas que deberán implementarse con el nuevo marco normativo, a fin de garantizar la minimización de datos y el cumplimiento de estas finalidades del tratamiento, efectuándose siempre que sea posible la seudonimización cuando no interfiera con el logro de estas. Este tipo de tratamientos podrán limitar los derechos de los interesados de manera proporcional, como consecuencia de la importancia que suponen para los intereses generales de los Estados. En este apartado también se prevé el estudio de la investigación biomédica, pues cuenta con una norma específica que la regula al tratarse de datos de categorías especiales. Se analizará el presupuesto legal que habilita su tratamiento, las particularidades y tipos de datos biomédicos. El derecho

a la protección de datos constituye un límite para este tipo de investigaciones y la anonimización de los datos es la fórmula para la inaplicación de este límite permitiendo la reutilización de datos y la difusión de los resultados de la investigación, sin perjuicio de que pueda utilizarse la seudonimización de este tipo de datos en caso de no ser posible la ruptura de la cadena de identificación.

En ocasiones el sector público no puede hacer frente a algunas de las obligaciones establecidas en el RGPD como puede ser directamente el tratamiento de datos personales, al no contar con personal especializado que pueda realizar tal labor conforme al marco jurídico vigente o, no poder incorporar un delegado de protección de datos en su estructura organizativa, este tipo de problemáticas se podrían solventar a través de la contratación administrativa de personal cualificado a tales efectos. Es por lo que la parte final del Capítulo IV versará sobre los contratos celebrados por el sector público en su calidad de responsable del tratamiento para sufragar estas necesidades. De tal forma que, se estudiará el régimen jurídico aplicable a estos contratos que depende en buena parte de quién actúe como contratante. Además, se pormenorizará el tipo y el objeto del contrato que consideramos adecuado, las obligaciones de las partes y los requisitos que deberán cumplir los contratistas de acuerdo con el RGPD. Lo anterior es también aplicable, salvo determinadas particularidades, a los contratos que tengan por objeto externalizar la figura de delegado de protección de datos.

Con el objeto de facilitar la comprensión y la lectura de esta tesis doctoral se realiza a modo de anexo una guía de conceptos para el seguimiento del trabajo: Derecho y nuevas tecnologías. En la que se abordará la evolución y funcionamiento de las distintas herramientas utilizadas en el ámbito digital que han sido referenciadas a lo largo de este trabajo de investigación. Entre las que se encuentran aquellas que son desarrolladas y utilizadas a partir de la web, que consideramos tienen mayor afectación en los derechos y libertades de las personas, como: las redes sociales y profesionales, los foros, los blogs, las wikis, los motores de búsqueda, los servicios de transmisión de archivos, las aplicaciones de mensajería instantánea, la computación en la nube, la sindicación de contenidos y el big data.

El estudio desarrollado a lo largo de esta tesis doctoral pretende, por un lado, obtener el panorama jurídico actual del derecho a la protección de datos personales

y su relación con otros derechos, cuando se desarrolle en el ámbito digital. La jurisprudencia en la materia nos permitirá vislumbrar aquellas cuestiones que aún no han sido resueltas por la normativa actual. En relación con el objetivo principal conoceremos los retos que suponen para la Administración pública la utilización de medios electrónicos para el cumplimiento de sus fines en relación con el nuevo marco jurídico dado por el RGPD y la LOPDGDD. Lo anterior, será la base que nos ayudará a plantear algunas posibles renovaciones de la legislación o la revisión de algunos puntos concretos que se han visto superados por el avance tecnológico.

Tim Berners-Lee, considerado el padre de la web, en su discurso en el CERN en abril de 2019 con motivo del trigésimo aniversario de su puesta en funcionamiento, a la luz de la deriva en que la misma estaba incurriendo, advirtió de que a la vez que la web había creado oportunidades también había generado nuevas vías para la comisión de delitos y había dado voz a los que proclaman el odio, lo que le llevó a finales de ese mismo año a formular el llamado contrato web, donde se implica a las Administraciones Públicas, a los ciudadanos y a las empresas para el cumplimiento de una serie de principios; conforme a este contrato las Administraciones deben garantizar el acceso a todos los ciudadanos a internet, la continuidad del servicio en todo momento y el respeto y protección de los derechos de la personas sobre sus datos y su privacidad en la red. A este último propósito, muy modestamente, pretende contribuir esta tesis doctoral.

CAPÍTULO I

PRINCIPIOS Y DERECHOS QUE SE DESARROLLAN EN LA WEB.

1. APROXIMACIÓN A LA REALIDAD DE LA WEB.

De conformidad con el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI) en su estudio «Perfil sociodemográfico de los internautas. Análisis de datos INE 2019», España cuenta con más de 35 millones de internautas que se conectan a diario a Internet [1]. De acuerdo con el «Estudio anual de redes sociales 2020» realizado por la asociación IAB *Spain*, las redes sociales más utilizadas en España son por este orden: *WhatsApp, Instagram, Facebook, Byte, YouTube, Telegram, Spotify, Twitter, TikTok, Twitch, HouseParty, 21 buttons, Tumblr, Tinder, Snapchat*, entre otras (Figura 1) [2].

La web que conocemos hoy en día implica inmediatez, la apertura de nuevos espacios dónde expresarnos y encontrar información a nivel global. Ahora los ciudadanos se han convertido en prosumidores de todo tipo de información albergada en la web. Como señala IGLESIA PRADOS: «*La aparición de las nuevas tecnologías, la facilidad de su empleo y la rápida y amplia difusión de sus contenidos ha generado una revolución en las formas de transmisión del pensamiento pues a través de éstas cualquier persona puede dar publicidad a sus ideas, que pueden ser recibidas, además por un mayor número de sujetos con más facilidad e inmediatez*» [3].

Las tecnologías implicadas en el ámbito web mayormente ofrecen sus servicios dentro de la sociedad de la información. Esto supone que los derechos fundamentales van a precisar ser objeto de especial protección en este nuevo marco. Los servicios de la sociedad de la información de conformidad con lo establecido en el art. 1.1.b) de la Directiva 2015/1535, del Parlamento Europeo y del Consejo, de 9

---

[1] ONTSI, Perfil sociodemográfico de los internautas. Análisis de datos INE 2019, p. 4. Disponible en: https://www.ontsi.red.es/sites/ontsi/files/2020-06/PerfilSociodemograficoInternautas2019.pdf (consulta y descarga: 29 de julio de 2019)

[2] Cfr. Anexo II de este trabajo.

[3] IGLESIA PRADOS, E. DE LA, «La responsabilidad de las redes sociales por la difusión de actos de vulneración del honor y la intimidad», CAPILLA RONCERO, F., *et al.* (Dir.), *Derecho Digital: Retos y cuestiones actuales.* Aranzadi, Navarra, 2018, p. 207.

de septiembre de 2015, por el que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (versión codificada), son todos aquellos prestados «*normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios. A efectos de la presente definición, se entenderá por: i) "a distancia", un servicio prestado sin que las partes estén presentes simultáneamente, ii) "por vía electrónica", un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético, iii) a petición individual de un destinatario de servicios", un servicio prestado mediante transmisión de datos a petición individual*». Dentro de estos servicios se encuentran las redes sociales, las páginas web de medios de comunicación o de difusión de contenidos, hemerotecas virtuales, motores de búsqueda, etc.

El ser humano por el solo hecho de ser persona tiene de manera intrínseca una serie de derechos que le son reconocidos, los cuales junto con la dignidad de la persona *«son el fundamento del orden político y de la paz social»* [4]. Estos derechos están reconocidos y contenidos en las Constituciones de los Estados, en Tratados Internacionales, en leyes y demás normativa. España forma parte de una serie de Tratados que contemplan el respeto y la observancia a una serie de derechos humanos. Entre los instrumentos de protección destacables encontramos la Declaración Universal de Derechos Humanos (DUDH) [5], el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales [6], el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) [7]. A nivel europeo, al ser parte de la Unión Europea [8], y de conformidad con los tratados constitutivos, España

[4] Art. 10.1 de la CE.
[5] Por mandato Constitucional, conforme al art. 10.2.
[6] Fue firmado el día 24 de noviembre de 1977 por España y el 4 de octubre de 1979.
[7] Firmado por España el 28 de septiembre de 1976, entró en vigor el día 27 de julio de 1977.
[8] Es parte de la Unión Europea desde el 12 de junio de 1985, con la firma del Tratado de Adhesión en Madrid y miembro desde el 1 de enero de 1986.

deberá observar así lo establecido por la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE) [9].

A nivel nacional encontramos como máxima fuente de derechos y libertades de la persona a la Constitución Española de 1978 (CE), la cual prevé en su Título I Capítulo Segundo Sección Primera los Derechos Fundamentales de observancia nacional. Consecuentemente, los derechos de la personalidad previstos en el art. 18 derecho al honor, la intimidad, la propia imagen y los contemplados en el art. 20, específicamente, los derechos a la libertad de expresión e información encuentran su base axiológica en la dignidad de la persona contemplada en el art. 10.1 de la CE.

Los derechos fundamentales de acuerdo con lo establecido por FERRAJOLI, son *«todos aquellos derechos subjetivos que corresponden universalmente a "todos" los seres humanos en cuanto dotados del status de personas, de ciudadanos o personas con capacidad de obrar; entendiendo por "derecho subjetivo" cualquier expectativa positiva (de prestaciones) o negativa (de no sufrir lesiones) adscrito a un sujeto por una norma jurídica; y por "status" la condición de sujeto, previsto asimismo por una norma jurídica positiva, como presupuesto de su idoneidad para ser titular de situaciones jurídicas y/o autor de los actos que son ejercicio de éstas»* [10]. Para PÉREZ LUÑO, el concepto de derechos fundamentales tiene dos acepciones *«La axiológica objetiva y la subjetiva»,* la primera de ellas *«representa el resultado del acuerdo básico de las diferentes fuerzas sociales, logradas a partir de situaciones de tensión y los consiguientes esfuerzos de cooperación encaminados al logro de metas comunes»,* así pues en su dimensión subjetiva *«determinan el estatuto jurídico de los ciudadanos, lo mismo en sus relaciones con el Estado que en sus relaciones entre sí. Tales derechos tienden, por tanto, a tutelar la libertad, autonomía y seguridad de la persona no solo frente al poder, sino también frente a los demás miembros del cuerpo social»* [11].

Los cambios tecnológicos en la sociedad de la información han provocado que, a partir de cierto *software* o *hardware*, se desarrollen nuevas aplicaciones que

[9] Conforme a lo establecido en el art. 6 de la versión consolidada del Tratado de la Unión Europea, así como en lo establecido en las declaraciones relativas a disposiciones de los Tratados, numero 1 contenido en la versión consolidada del Tratado de Funcionamiento de la Unión Europea.
[10] FERRAJOLI, L., *Los fundamentos de los derechos fundamentales. Edición traducida de CABO DE y PISARELLO,* Trotta, Madrid, 2001, p. 19.
[11] PÉREZ LUÑO, A., Los *derechos fundamentales.* 7ª edición, Tecnos, Madrid, 1998, pp. 20-22.

ayuden a facilitar el día a día de las personas. La complejidad del diseño de aplicaciones o versiones móviles de redes sociales o motores de búsqueda, no permiten que sepamos con certeza qué datos son tratados y con qué finalidades. Las herramientas tecnológicas proporcionan una gran cantidad de ventajas a los usuarios, sin embargo, su falta de información puede llevarlos a infringir en mayor o menor medida los derechos de la personalidad o los derechos a la libertad de expresión e información. Hay que mirar desde distintos prismas estas tecnologías que, si bien mejoran la calidad de vida de las personas en muchos aspectos, también pueden resultar invasivas ya que usualmente registran hábitos de navegación, geolocalización, o cualquier otro dato imaginable, y puedan servir como medios para la transgresión de algún derecho fundamental.

En este Capítulo se ejemplificarán algunos casos en que los derechos fundamentales que se estudian a continuación pueden verse trasgredidos, como consecuencia de alguna de las acciones llevadas a cabo por un usuario genérico en un ámbito igualmente genérico.

2. LA DIGNIDAD DE LA PERSONA

La dignidad es uno de los aspectos irrenunciables con la que cuentan los seres humanos, y pese a su intangibilidad la importancia que tiene en nuestro ordenamiento jurídico es innegable. Esta ha sido objeto de estudio desde diversas perspectivas [12], entre ellas la jurídica, sin que ello implique que «*exista sólo allí donde*

[12] Esta ya había sido objeto de estudio del filósofo alemán Immanuel Kant, para él el hombre es un fin en sí mismo, debido a esto es considerado como precursor de la corriente filosófica del personalismo, la cual define OEHLING DE LOS REYES como: «*una filosofía basada en la dignidad de la persona*», *vid.* OEHLING DE LOS REYES, A., «El concepto constitucional de dignidad de la persona: Forma de comprensión y modelos predominantes de recepción en la Europa continental», *Revista Española de Derecho Constitucional*, Centro de Estudios Políticos y Constitucionales, Madrid, 2011, p. 137. Según PRIETO ÁLVAREZ, T., la dignidad para Kant encontraba su fundamento en «*la autonomía, de modo que la dignidad humana se reduce al carácter autonormativo y libre del hombre ("el hombre es su propia ley"). Esto comporta que "desde los presupuestos kantianos se identifica dignidad y autonomía o libertad»,* sigue este autor diciendo que entonces «*en este sentido, podríamos decir que el hombre, por tener dignidad, es un ser libre; de modo que goza de una cabal autonomía, de una capacidad de autodeterminación en su vida»,* Cfr. PRIETO ÁLVAREZ, T. «Luces y sombras de la integración europea en derechos de la persona. En particular, en riesgo de que la base del sistema jurídico se traslade desde la dignidad humana a la autonomía personal», LAGUNA DE LA PAZ, J. C., SANZ RUBIALES, I. y MOZOS Y TOUYA, I. M. DE LOS. (Coord.), *Derecho administrativo e integración europea. Estudios homenaje al Profesor José*

el derecho la reconoce, y en la medida en que la reconoce», entonces «*la dignidad no sólo es lo que el Derecho dice que es. Lo único que podrán lograr las diversas "versiones" del reconocimiento a nivel jurídico de la dignidad será una aproximación, un retrato más o menos fidedigno de la dignidad de la persona*» [13].

La importancia de la dignidad en la contemporaneidad acontece en los tiempos de postguerra [14]. En este sentido OEHLING DE LOS REYES, haciendo referencia la contribución realizada por el profesor SMED, determina que la conciliación entre el positivismo y el derecho natural supuso una solución de gran aceptación, pues *«la referencia de esta visión contribuyó en buena medida a la consolidación de una Constitución fundamentada en valores» [15].*

Actualmente la dignidad está reconocida en la mayoría de los textos constitucionales occidentales [16], en instrumentos de carácter internacional [17] y en la propia CDFUE [18]. Sin embargo, el gran referente en Europa constitucionalmente hablando, desde nuestra perspectiva está dado por la Ley Fundamental de Bonn, la

Luis Martínez López-Muñiz, Madrid, Reus, 2017, p. 194. Para un análisis más en profundidad, véase LLANO-ALONSO, F. H., La influencia de Kant en el universo actual, *vid.* RUIZ DE LA CUESTA, A. (Coord.), *Bioética y derechos humanos: implicaciones sociales y jurídicas*, Universidad de Sevilla, España, 2005, pp. 29-58, y VERGÉS RAMÍREZ, S., «La dignidad del hombre según Kant», *Letras de Deusto*, núm. 42, vol. 18, pp. 5-20.

[13] Citando a GONZÁLEZ PÉREZ, J. en ALEGRE MARTÍNEZ, M.A., *La dignidad de la persona*, Civitas, Madrid, 1986, pp. 19-20.

[14] En relación con esta afirmación GÓMEZ SÁNCHEZ, Y., establece que: *«El reconocimiento constitucional de la dignidad tiene su reflejo más nítido en los textos constitucionales posteriores a la Segunda Guerra Mundial cuyo grado de destrucción alentó y auspició diversos movimientos en favor del reconocimiento efectivo de los derechos humanos como vía para el mantenimiento de la paz», vid.* GÓMEZ SÁNCHEZ, Y., *Constitucionalismo multinivel: Derechos fundamentales,* 3ª ed., Sanz y Torres/UNED, Madrid, 2015, p. 166.

[15] OEHLING DE LOS REYES, establece que la SMED «*suponía para el pensamiento jurídico de posguerra, y especialmente para la doctrina alemana, una solución que tuvo una importante aceptación*», Cfr. OEHLING DE LOS REYES, A., *op. cit*., p.136.

[16] Por ejemplo, se contempla en el art. 3 de la Constitución de la República Italiana, en el art. 1 de la Constitución de la República Portuguesa, art. 54 de la Constitución de la Republica húngara, art. 7 de la Constitución Federal de la Confederación de Suiza.

[17] Está contemplada en la Declaración Universal de Derechos Humanos (principalmente en el Preámbulo y art. 1: «*Todos los seres humanos nacen libres e iguales en dignidad y derechos y, dotados como están de razón y conciencia, deben comportarse fraternalmente los unos con los otros*», y también se menciona en el art. 22 y 23 de la misma Declaración), en el Pacto Internacional de los Derechos Civiles y Políticos (preámbulo), en el Convenio para la protección de los derechos humanos y dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina (Convenio relativo a los derechos humanos y la biomedicina), entre otros.

[18] Está contemplada en el art. 1: «*La dignidad humana es inviolable. Será respetada y protegida*».

cual sitúa a la dignidad de la persona como *obligación de todo poder público*[19], sin embargo, esta tiene un nivel de protección equivalente a un derecho fundamental[20], distinto a que se le reconoce en el sistema jurídico español, y al que haremos referencia más adelante.

En relación con el concepto de dignidad, el Diccionario de la Lengua española la define como aquello que tiene «*cualidad de digno*»[21] y a su vez, digno es «merecedor de algo»[22]. El Tribunal Constitucional determina que es «*un valor espiritual y moral inherente a la persona*»[23]. Es una cualidad intrínseca y exclusiva de los seres humanos es aquello que se nos debe, pero que a su vez le debemos al otro[24]. La dignidad de uno no es mayor que la del resto, nos iguala[25]. PANEA MÁRQUEZ establece que «*la dignidad humana es reconocer que estamos en deuda con el hombre, y que, por tanto, tal condición, por sí misma, reclama, exige, demanda un actuar en cierto sentido. Reconocer que el hombre tiene dignidad es reconocer que tiene exigencias que le son debidas, unos derechos que le pertenecen»,* esta cualidad humana hace «*referencia a algo que nos eleva, que nos realza, que nos cualifica y que, por tanto, sobrepasa la mera facticidad, los meros hechos. La dignidad es, en este sentido, un referente crítico, una suerte de canon, de medida, con el que cabe enjuiciar los hechos,*

[19] El art. 1 de la Constitución de la República Federal de Alemania, establece a tenor literal: «*La dignidad humana es intangible. Respetarla y protegerla es obligación de todo poder público*»

[20] Pues está contemplada formalmente en el apartado primero correspondiente a los derechos fundamentales. Para un estudio en mayor profundidad, *vid.* OEHLING DE LOS REYES, A., *op. cit*., pp. 140-156.

[21] *Vid.* Dle, https://dle.rae.es/?id=DlX5ZXZ (consulta: 1 de septiembre de 2019).

[22] *Vid.* Dle, https://dle.rae.es/?id=DldD5zV (consulta:1 de septiembre de 2019).

[23] F. J. 8, de la STC (Pleno) 53/1985, de 11 de abril, (RTC\1985\53; ECLI:ES:TC:1985:53).

[24] PANEA MÁRQUEZ, J. M., «La imprescindible dignidad», RUIZ DE LA CUESTA, A. (coord.), *Bioética y derechos humanos: implicaciones sociales y jurídicas*, Universidad de Sevilla, España, 2005, p. 20. En este sentido, ALEGRE MARTÍNEZ establece que «*la dignidad ajena (y también la propia en la medida en que los derechos inherentes a la misma son irrenunciables) se convierte en un límite de los derechos propios. Si ello es así, si la dignidad es un límite, al respeto a esa dignidad (ajena y propia, en la medida en que estamos ante derechos irrenunciables), y a los derechos inviolables que son inherentes a la persona en razón de ella, es un deber genérico derivado de la propia dignidad», vid.* ALEGRE MARTÍNEZ, M.A., *op. cit*., pp. 139-140.

[25] Para DÍAZ REVORIO: *«la dignidad nos iguala en nuestra esencia humana a todos los demás seres humanos, pero nos diferencia de cada uno de ellos porque cada persona es irrepetible»,* Cfr. DÍAZ REVORIO, F. J., «Los valores superiores del ordenamiento jurídico», PENDÁS, B. (Dir.), *España constitucional (1978-2018). Trayectorias y perspectivas,* Tomo III, Centro de Estudios Políticos y Constitucionales, Madrid, 2018, p. 1752.

que pueden estar o no en con concordancia con ese ideal o referente crítico que la dignidad incorpora»[26].

La dignidad de la persona está contemplada de manera primaria en el ordenamiento jurídico español, en el artículo 10.1 de la CE dispone que: «*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*». De acuerdo con OEHLING DE LOS REYES el apartado primero de este artículo «*muestra bastante bien la influencia del pensamiento personalista*» continúa diciendo que «*en general, la versión jurídica del personalismo, busca dotar a la realidad objeto de sus desvelos –el hombre- de mayor protección legal posible; de lo cual constituye la necesidad elemental de conceptuar al individuo como base y objeto de todo ordenamiento, reconociendo su dignidad como punto de partida*»[27].

El Tribunal Constitucional fue acotando el contenido del apartado primero de este artículo constitucional, primeramente, ha estimado que se trata de un valor que es presupuesto del orden político y de la paz social[28], y como tal, uno de los mayores axiomas contenidos en nuestra norma fundamental y, por tanto, constituye «*el prius lógico y ontológico para la existencia y especificación de los demás derechos*»[29]. También es considerado por el supremo interprete de la constitución como «*un mínimum invulnerable que todo estatuto jurídico debe asegurar, de modo que, sean unas u otras las limitaciones que se impongan en el disfrute de derechos individuales, no conlleven menosprecio para la estima que, en cuanto ser humano, merece la persona*»[30].

La doctrina en relación con lo anterior ha entendido también que la dignidad tiene un carácter axiológico que sustenta el sistema de derechos contemplados en la constitución, LUCAS VERDÚ determinó que «*Nuestra Constitución expresa esa proyección cuando recoge en su articulado el conjunto de valores que aportan la*

[26] PANEA MÁRQUEZ, J. M., *op. cit*., p. 20.
[27] OEHLING DE LOS REYES, A., *op. cit*., p. 168.
[28] LUCAS VERDÚ, P., *Estimativa y política constitucionales. Los valores y principios rectores del ordenamiento constitucional español*, Universidad de Madrid, Madrid, 1984, p. 109.
[29] F.J. 3 de la STC (Pleno) 53/1985, de 11 de abril (RTC\1985\53; ECLI:ES:TC:1985:53).
[30] F. J. 8 de la STC (Pleno) 53/1985, de 11 de abril(RTC\1985\53; ECLI:ES:TC:1985:53).

dimensión axiológica de sus prescripciones. Así, los valores informan y sostienen toda su estructura normativa y, en particular, los derechos y libertades de los ciudadanos (artículos 14-38)»[31]. Los valores y en específico la dignidad presenta un «*contenido muy indeterminado de carácter ético, finalístico o axiológico)*»[32], incluso hay quien piensa que la dignidad de la persona debería estar incluida en el apartado 1 del art. 1 de la CE, como valor supremo junto a la justicia, la libertad, la igualdad y el pluralismo político[33].

En segundo lugar, el TC ha determinado que pese a su valor axiológico como fundamento del orden político, de la paz social y como punto de partida de los derechos fundamentales contenidos en la Constitución, por tanto este no es en sí mismo un derecho fundamental y, no puede solicitarse su protección de manera autónoma, ejemplo de ello es el Fundamento Jurídico (FJ)Segundo, del Auto del TC 149/1999, de 14 de junio: «*la dignidad de la persona no se reconoce en nuestra Constitución como un derecho fundamental sino como "fundamento del orden político y la paz social" (art. 10 C.E.), para rechazar eventuales violaciones de ese mandato constitucional susceptibles de protección autónoma a través del proceso constitucional de amparo*»[34]. El F.J. 1 de la STC 64/1986, de 21 de mayo, establece que: «*Ante todo, habrá que destacar que la norma contenida en el artículo 10.1 de la Constitución con independencia de que pueda servir de criterio de interpretación de los derechos fundamentales y libertades públicas en general no puede servir de base a una pretensión autónoma de amparo, por impedirlo lo dispuesto en el art. 53 de la propia Constitución, que permite a los ciudadanos recabar amparo para la tutela de las libertades públicas y derechos fundamentales, pero limitándolo a los reconocidos en el art. 14, en la sección primera del capítulo segundo y el párrafo 2.° del art. 30*»[35]; y por tanto, la dignidad también tiene esa vertiente relacional con otros derechos,

[31] LUCAS VERDÚ, P., «Sobre los valores» (en línea), *Teoría y realidad constitucional,* núm. 23, 2009, p. 118-119 Disponible en: https://dialnet.unirioja.es/descarga/articulo/3003932.pdf (consulta: 17 de julio de 2019).
[32] PASCUAL MEDRANO, A., «La dignidad humana como principio jurídico del ordenamiento constitucional español», CHUECA, R. (coord.), *Dignidad humana y derecho fundamental*, Centro de Estudios Políticos y Constitucionales, Madrid, 2015, p. 304.
[33] Cfr. *Ib.*, p. 305.
[34] Auto TC (Sala Primera) 149/1999, de 14 de junio, F.J. 2 (RTC\1999\149 AUTO; ECLI:ES:TC:1999:149A).
[35] F. J. 1 de la STC (Sala Primera) 64/1986, de 21 de mayo, (RTC\1986\64; ECLI:ES:TC:1986:64).

pues «*sólo en la medida en que tales derechos sean tutelares en amparo y únicamente con el fin de comprobar si se han respetado las exigencias que, no en abstracto, sino en el concreto ámbito de cada uno de aquéllos, deriven de la dignidad de la persona, habrá de ser ésta tomada en consideración por este Tribunal como referente. No, en cambio, de modo autónomo para estimar o desestimar las pretensiones de amparo que ante él se deduzcan*» [36]. Como consecuencia de no ser considerada como un derecho fundamental, su regulación no tiene que ser llevado a cabo por medio de Ley Orgánica [37].

En base a lo anteriormente expuesto, puede expresarse que todos los derechos de la personalidad, de manera forzosa son una expresión de la dignidad de la persona ligado a su autonomía y libertad como ser humano [38], y debe entenderse como un *valor jurídico fundamental* [39]. Así pues, «*el artículo 10 contiene una norma jurídica vinculante, con exigencia de ejecutividad*» [40], vinculante a todos los ciudadanos con respecto a la dignidad de otros, de observancia a empresas respecto a sus trabajadores y viceversa, y también por parte del Estado frente a los ciudadanos, es decir, engloba a todos los agentes de la vida democrática del país y es exigible a todos, en cualquier ámbito donde se desarrolle la persona, inclusive en Internet.

3. DERECHOS DE LA PERSONALIDAD

Derivados de la dignidad humana, primeramente estudiaremos los denominados «Derechos de la personalidad», los cuales en palabras de PASCUAL

[36] F.J. 4º de la STC (Pleno) 120/1990, de 27 de junio (RTC\1990\120; ECLI:ES:TC:1990:120).
[37] Tal y como lo establece la STC (Pleno) 116/1999, de 17 de junio, F.J. 4 (RTC\1999\116; ECLI:ES:TC:1999:116): *«la reserva de ley orgánica establecida en el art. 81.1 de la Constitución ha de entenderse referida a los derechos y libertades públicas regulados en la sección primera del Capítulo Segundo del Título I , entre los que, obviamente, no se encuentra la dignidad de la persona que, además, es reconocida en nuestra Constitución como «fundamento del orden político y de la paz social» (art. 10.1 CE).*
[38] En relación con lo anterior, a modo ejemplificativo, el contenido del F.J. 1 de la STC 214/1991, de 11 de noviembre (RTC\1991\214; ECLI:ES:TC:1991:214): «*el derecho al honor y otros de los derechos reconocidos en el art. 18. C.E. aparecen como derechos fundamentales vinculados a la propia personalidad, derivados sin duda de la "dignidad de la persona" que reconoce el art. 10 C.E.».*
[39] F.J. 3 de la STC (Pleno) 53/1985, de 11 de abril (RTC\1985\53; ECLI:ES:TC:1985:53).
[40] RUÍZ-GIMÉNEZ CORTÉS, J. y RUÍZ-GIMÉNEZ ARRIETA, I., «El artículo 10 Derechos Fundamentales de la persona», ALZAGA VILLAAMIL, O (Coord.), *Comentarios a la Constitución Española de 1978,* Ed. De derecho reunidas, Madrid, 1997, p. 57.

MEDRANO son *«derechos derivados de la propia naturaleza humana, y destinados, justamente, a la protección integral de la persona»* [41], los cuales tienen un contenido *«propio y específico»* [42]*;* por su parte, SIMÓN CASTELLANO estima que *«se les ha catalogado como derechos de libertad y autonomía porque fueron concebidos para garantizar una esfera reservada al individuo frente a la acción de los demás»* [43]*.* Estos derechos tienen carácter de irrenunciables, inalienables e imprescriptibles, ya que reconocen y protegen los aspectos más intrínsecos del ser humano, su esfera más propia, y, por tanto, no puede efectuarse renuncia de los mismos, cualquier manifestación en este sentido resultaría totalmente nula. REBOLLO DELGADO, establece que este tipo de derechos tienen un doble carácter: el interno y el externo, el primero de ellos «*alcanza hasta donde lo hace el derecho ajeno, la moral vigente, el orden público y el bien común*» [44], y el segundo se refiere a su intangibilidad, inalienabilidad, imprescriptibilidad, inembargabilidad, irrenunciabilidad e intransmisibilidad [45]. En este apartado hablaremos sobre la perspectiva constitucional de los previstos en el apartado primero del art. 18 de la CE [46], es decir, el derecho al honor, a la intimidad personal y familiar, y a la propia imagen.

Estos derechos son autónomos entre sí, a pesar de que todos deriven de la dignidad de la persona [47] y que aunque se encuentren en un único precepto,

---

[41] PASCUAL MEDRANO, A. *El derecho Fundamental a la Propia Imagen. Fundamento, contenido y límites,* Ed. Aranzadi, Navarra, 2003, p. 24.

[42] F.J.3 de la STC (Sala Segunda)156/2001, de 2 de julio, (RTC\2001\156; ECLI:ES:TC:2001:156).

[43] SIMÓN CASTELLANO, P. *El régimen constitucional del derecho al olvido digital,* Tirant lo Blanch, Valencia, 2012, p. 119.

[44] REBOLLO DELGADO, L., «Derechos de la personalidad y los datos personales», *Revista de Derecho Político*, núm. 44, 1998, p. 146.

[45] *Ib.*, p. 146-147.

[46] El desarrollo legislativo de estos Derechos catalogados como fundamentales y por tanto de protección especial, deben contenerse en una Ley Orgánica de conformidad con lo establecido en el artículo 81.1 de la CE: *«Son leyes orgánicas las relativas al desarrollo de los derechos fundamentales y de las libertades públicas (…)».*

[47] En cuanto a que los derechos de la personalidad derivan de la dignidad, encontramos como ejemplo lo establecido por STC 214/1991 de 11 de noviembre (RTC 1991\214; ECLI:ES:TC:1991:214), en su F.J. 1 que a la letra dice que: *«el derecho al honor y otros de los derechos reconocidos en el art. 18. C.E. aparecen como derechos fundamentales vinculados a la propia personalidad, derivados sin duda de la "dignidad de la persona" que reconoce el art. 10 C.E.».* En este mismo sentido el F.J. 8º de la STC (Pleno) 53/1985, de 11 de abril (RTC\1985\53; ECLI:ES:TC:1985:53), establece que el: «*valor jurídico fundamental la dignidad de la persona, que, sin perjuicio de los derechos que le son inherentes, se halla íntimamente vinculada con el libre desarrollo de la personalidad (art. 10) y los derechos a la integridad física y moral (art. 15), a la libertad de ideas y creencias (art. 16), al honor, a la intimidad personal y familiar y a la propia imagen (art. 18.1). Del sentido de estos preceptos puede deducirse que la dignidad*

HERNÁNDEZ FERNÁNDEZ señala que *«los derechos al honor, a la intimidad y a la propia imagen, a pesar de su estrecha relación en tanto que derechos de la personalidad derivados de la dignidad humana y dirigidos a la protección del patrimonio moral que las personas tienen, no obstante, un contenido propio y específico»* [48]*;* lo anterior también ha sido reconocido por diversas sentencias del Tribunal Constitucional [49]. A continuación, en un epígrafe específico se estudiará cada uno de ellos.

3.1 Derecho al honor

El derecho al honor está recogido en el art. 12 de la DUDH [50], en el art. 17 del PIDCP [51], constitucionalmente en España se contempla en el art. 18.1 [52], y desarrollado por 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.

Este derecho entra en la categoría de los conceptos jurídicos indeterminados, ya que carece de una definición en nuestro ordenamiento jurídico, según las sentencias del Tribunal Constitucional 223/1992, de 14 de diciembre [53] y 139/1995,

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».

[48] HERNÁNDEZ FERNÁNDEZ, A., *El honor, la intimidad y la imagen como derechos fundamentales,* Colex, Madrid, 2009, p. 64.

[49] Cfr. STC (Sala Segunda) 156/2001, de 2 de julio, F.J. 2º (RTC\2001\156; ECLI:ES:TC:2001:156): «*Debe recordarse que los derechos al honor, a la intimidad personal y a la propia imagen son derechos autónomos. De este modo, al tener cada uno de ellos su propia sustantividad, la apreciación de la vulneración de uno no conlleva necesariamente la vulneración de los demás*»; STC (Sala Segunda) 81/2001, 26 de marzo, F.J. 2º (RTC\2001\81; ECLI:ES:TC:2001:81), refiriéndose al derecho a la propia imagen: «*En la Constitución española ese derecho se configura como un derecho autónomo, aunque ciertamente, en su condición de derecho de la personalidad, derivado de la dignidad y dirigido a proteger el patrimonio moral de las personas, guarda una estrecha relación con el derecho al honor y, sobre todo, con el derecho a la intimidad, proclamados en el mismo art. 18.1 del Texto constitucional*»; STC (Sala Segunda) 14/2003, de 28 de enero, F.J. 4º (RTC\2003\14; ECLI:ES:TC:2003:14), que: «*a pesar de su estrecha relación en tanto que derechos de la personalidad, derivados de la dignidad humana y dirigidos a la protección del patrimonio moral de las personas, tienen, no obstante, un contenido propio y específico*»; STC (Sala Primera) 83/2002, de 22 de abril, FJ 4º (RTC\2002\83; ECLI:ES:TC:2002:83), haciendo referencia tanto al derecho a la propia imagen como al derecho a la intimidad, determina que tienen «*un contenido propio y específico*».

[50] Art. 12: *«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».*

[51] Art. 17: *«1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques».*

[52] Art.18.1: «*Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen».*

[53] F.J.3 de la STC (Sala Primera) 223/1992, de 14 de diciembre (RTC 1992\223; ECLI:ES:TC:1992:223).

de 26 de septiembre de 1995 [54], de tal suerte que ese Tribunal: *«se ha referido expresamente a la imposibilidad de encontrar una definición del mismo en el propio ordenamiento jurídico. Se trata de un concepto dependiente de las normas, valores e ideas sociales vigentes en cada momento, que encaja sin dificultad, por tanto, en la categoría jurídica conocida de conceptos jurídicos indeterminados»* [55]. Lo anterior concuerda con la STC de 13 de noviembre de 1989 [56] la cual establece que: *«El contenido del derecho al honor, que la Constitución garantiza como derecho fundamental en su art. 18, apartado 1, es, sin duda, dependiente de las normas, valores e ideas sociales vigentes en cada momento»*. Es decir, que el concepto honor [57] no puede entenderse como estático, sino que va transformándose según la época y la sociedad en la cual se vive, asociándose con la buena reputación que ostenta una persona. Por tanto, debe entenderse que «*El denominador común de todos los ataques e intromisiones ilegítimas en el ámbito de protección de este derecho es el desmerecimiento en la consideración ajena como consecuencia de expresiones proferidas en descrédito o menosprecio de alguien o que fueren tenidas en el concepto público por afrentosas»* [58].

El Diccionario de la lengua española por su parte realiza una aproximación conceptual de lo que debe entenderse como honor, de la cual tomaremos como referencia las primeras dos definiciones. La primera aproximación relaciona al honor con la «*cualidad moral que lleva al cumplimiento de los propios deberes respecto del prójimo y de uno mismo*», mientras que la segunda define al honor como la «*Gloria o buena reputación que sigue la virtud, al mérito o a las acciones heroicas, la cual trasciende a las familias, personas y acciones mismas de quien se las granjea*».

---

[54] F.J. 5 de la STC (Sala Primera) 139/1995, de 26 de septiembre de 1995 (RTC 1995\139; ECLI:ES:TC:1995:139).

[55] *Íd.*

[56] F.J.4 de la STC (Sala Segunda) 185/1989, de 13 de noviembre (RTC 1989\185; ECLI:ES:TC:1989:185).

[57] Para VIDAL MARÍN, T., el derecho al honor consta de dos sentidos el subjetivo y el objetivo: *«En cualquier caso, y a los efectos que ahora interesan, la doctrina ha solido distinguir entre un concepto objetivo y un concepto subjetivo de honor. En su sentido subjetivo, el honor sería el resultado de la valoración que cada hombre hace de sus propias cualidades, en tanto que en sentido objetivo el honor sería el resultado de la valoración que los demás hacen de nuestras cualidades, es decir, sería el aprecio o la estima que una persona recibe en la sociedad en la que vive», vid.* VIDAL MARÍN, T., «Derecho al honor, personas jurídicas y tribunal constitucional» (en línea), *Indret: Revista para el Análisis del Derecho,* núm. 1, 2007, p. 6. Disponible en: http://www.indret.com/pdf/397_es.pdf

[58] F.J.3 de la STC (Sala Primera) 223/1992, de 14 de diciembre (RTC 1992\223; ECLI:ES:TC:1992:223).

Esta definición refleja por la doble protección de este derecho, por una parte, a la estima propia y, por la otra, a injerencias externas, es decir, «*a no ser escarnecido o humillado ante uno mismo o ante los demás*»[59]. De acuerdo con SANCHIS CRESPO, el derecho al honor «*se integra, pues, en dos características: a) El de la inminencia o estimación que cada persona hace de sí misma. b) El de trascendencia o reconocimiento que los demás hacen de nuestra dignidad. Garantiza la no exteriorización por terceros de sentimientos opuestos a la consideración o respeto que tengan respecto de un particular o colectivo*»[60], lo anterior en concordancia con lo establecido por O´CALLAGHAN MUÑOZ, quien determinó también ese doble aspecto de este derecho, pues se ve «*reflejada en la consideración de los demás y el sentimiento de la propia persona*»[61].

La segunda acepción relaciona el derecho al honor con la «buena reputación». En este sentido, el TC ha tomado como referencia esta última para determinar que consiste «*en la opinión que las gentes tienen de una persona, buena o positiva si no van acompañadas de adjetivo alguno. Así como este anverso de la noción se da por sabido en las normas, éstas en cambio intentan aprehender el reverso, el deshonor, la deshonra o la difamación, lo infamante*»[62]. Por consiguiente, «*El denominador común de todos los ataques o intromisiones legítimas en el ámbito de protección de este derecho es el desmerecimiento en la consideración ajena (art. 7.7 LO 1/1982) como consecuencia de expresiones proferidas en descrédito o menosprecio de alguien o que fueren tenidas en el concepto público por afrentosas*»[63]. Las intromisiones de este tipo pueden realizarse a partir de opiniones e informaciones sobre alguien, y en tal caso es menester recordar que ningún derecho fundamental contemplado en nuestra Constitución es absoluto. Es decir, el derecho al honor puede constituir un

[59] F.J. 4 de la STC (Sala Segunda) 85/1992, de 8 de junio (RTC 1992\85; ECLI:ES:TC:1992:85).
[60] SANCHIS CRESPO, C., «La tutela judicial del derecho al honor, Internet y la blogosfera», *Diario La Ley*, núm. 8035, sección Doctrina, 4 de marzo de 2013, p. 2.
[61] O´CALLAGHAN MUÑOZ, X., «Personalidad y derechos de la personalidad (honor, intimidad, imagen) del menor, según la Ley de Protección de Menor», *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía,* núm. 4, 1996, p. 1249.
[62] F.J. 3 de la STC (Sala Primera) 223/1992, de 14 de diciembre (RTC 1992\223; ECLI:ES:TC:1992:223).
[63] F.J. 3 de la STC (Sala Primera) 223/1992, de 14 de diciembre (RTC 1992\223; ECLI:ES:TC:1992:223).

límite a los demás, en especial al derecho a la libertad de expresión e información previstos en el art. 20.1, haciéndose siempre una ponderación de estos.

Como se dijo antes, el contenido del derecho al honor en buena parte depende de los valores vigentes, y comprende de «*un aspecto interno, subjetivo o dimensión individual, por uno mismo, y un aspecto externo, objetivo o dimensión y valoración social, por los demás, siendo tan relativo el concepto de honor , debe compaginarse la inevitable subjetivación con las circunstancias objetivas, con el fin de evitar que una exagerada sensibilidad de una persona transforme en su interés conceptos jurídicos como el honor; y para la calificación de ser atentatorio al honor una determinada noticia o expresión, debe hacerse en relación con el contexto y las circunstancias de cada caso*» [64]. El panorama que se presenta en el siglo XXI viene dado principalmente por el uso de tecnologías como las redes sociales: Facebook, Twitter, Instagram [65], etc., o por cualquier medio de comunicación con página web, blog, que suponga la visualización masiva de una publicación por la cual se realice una intromisión al derecho al honor.

Es pertinente decir en este punto que ningún derecho es absoluto y, por tanto, el hecho de que se realicen publicaciones que contengan expresiones que puedan dañar nuestro honor, implica que debe llevarse a cabo una ponderación de derechos según el caso concreto. Esto implica que el análisis a los posibles daños en el entorno tecnológico no se realice de manera aislada. La STS 534/2016, de 14 de septiembre, enumera los criterios más relevantes en las que se debe basar este juicio de ponderación [66]. El primero de ellos es reconocer el mismo grado de protección a los dos derechos, para poder determinar que se ha realizado una intromisión al derecho al honor por alguna noticia o expresión debe tomarse en cuenta el contexto y las circunstancias del caso concreto.

[64] F.D. 4º de la STS (Sala de los Civil) 534/2016, de 14 de septiembre (RJ 2016\4826; ECLI:ES:TS:2016:4060).

[65] Aunque esta página web perteneciente al grupo de Facebook se relacione con contenido fotográfico, su modalidad de «historias» permite a los usuarios enviar mensajes escritos, cuya durabilidad sea de 24 horas., en cuyo caso puede también ser una herramienta para realizar una intromisión al derecho al honor.

[66] F.D. 4º de la STS (Sala de los Civil) 534/2016, de 14 de septiembre (RJ 2016\4826; ECLI:ES:TS:2016:4060).

El segundo de los parámetros es determinado por el reconocimiento del prestigio profesional dentro de ese «*marco externo de trascendencia en que se desenvuelve el honor, pero se exige que el ataque revista un cierto grado de intensidad para que pueda apreciarse una transgresión del derecho fundamental, de modo que, obviamente, no toda crítica sobre la actividad laboral o profesional de un individuo constituye una afrenta a su honor personal*», por lo que solo son limitativas y trasgreden el derecho al honor aquellos ataques dirigidos a su actividad profesional, consistentes en 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*»[67]. En este punto procede hacer una observación, las personas jurídicas también son titulares del derecho fundamental al honor, por ello se encuentra en una circunstancia similar a la descrita con anterioridad. Continuando con el segundo de los parámetros, conforme a la STS 802/2006, de 19 de julio «*la problemática se centra en la apreciación del aspecto trascendente o exterior –consideración pública protegible*»[68]. El tercero de los parámetros hace referencia al propio comportamiento de la persona *«("propios actos", según el art. 2.1 de la Ley Orgánica 1/1982)*»[69]. El cuarto criterio está relacionado con la colisión misma del derecho al honor y el derecho a la libertad de expresión, en cuyo caso «en abstracto» prevalecerá el derecho a la libertad de expresión, sin embargo, siempre se tendrán en cuenta las circunstancias del caso concreto, «*para lo que deberán tomarse en cuenta dos parámetros o presupuestos esenciales (dejando al margen el requisito de la veracidad, solo exigible cuando está en juego la libertad de información): si las expresiones, opiniones o juicios de valor emitidos tenían interés general y si en su difusión no se utilizaron términos o expresiones inequívocamente injuriosas o vejatorias, innecesarias para lograr transmitir aquella finalidad crítica*». Finalmente, el último criterio en la ponderación de estos dos derechos es la realización de un

[67] F.J. 5 de la STC (Sala Segunda) 180/1999, de 11 de octubre (RTC 1999\180; ECLI:ES:TC:1999:180).
[68] F.D. 2º de la STS (Sala de lo Civil) 802/2006, de 19 de julio (RJ 2006\3991; ECLI: ES:TS:2006:4495).
[69] Inciso c) del F.J. 4 de la STS (Sala de los Civil) 534/2016, de 14 de septiembre (RJ 2016\4826; ECLI:ES:TS:2016:4060).

análisis del contexto en que fueron vertidas las declaraciones y no así un análisis separado de cada expresión empleada o de «su mero significado gramatical», por lo que «*la jurisprudencia mantiene la prevalencia de la libertad de expresión cuando se emplean expresiones que, aun aisladamente ofensivas, al ser puestas en relación con la opinión que se pretende comunicar o con la situación política o social en que tiene lugar la crítica, experimentan una disminución de su significación ofensiva y sugieren un aumento del grado de tolerancia exigible, aunque puedan no ser plenamente justificables*»[70].

La transgresión del derecho al honor en la web se lleva a cabo principalmente por los usuarios de estos servicios y serían responsables de las expresiones utilizadas en sus publicaciones, aunque también podría suponer responsabilidad para los prestadores de servicios de la información. El considerando 45 de la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre comercio electrónico)[71] establece que: «*Para beneficiarse de una limitación de responsabilidad, el prestador de un servicio de la sociedad de la información consistente en el almacenamiento de datos habrá de actuar con prontitud para retirar los datos de que se trate o impedir el acceso a ellos en cuanto tenga conocimiento efectivo de actividades ilícitas. La retirada de datos o la actuación encaminada a impedir el acceso a los mismos habrá de llevarse a cabo respetando el principio de libertad de expresión y los procedimientos establecidos a tal fin a nivel nacional*». El art. 14 de esta Directiva establece el régimen de exención a los servicios de alojamiento de datos siempre y cuando: a) no tengan conocimiento efectivo del carácter ilícito de la actividad o la información, y en el caso de reclamaciones por daños o perjuicios, no tenga conocimiento de los hechos o circunstancias que se

[70] F.D. 4º de la STS (Sala de lo Civil) 217/2015, de 22 de abril (RJ 2015\1358; ECLI:ES:TS:2015:1532).
[71] De acuerdo con la reciente STJUE de 8 de octubre de 2020 se determina que se aplicará lo dispuesto en la Directiva 2002/58 y en el Reglamento 2016/679 (RGPD) «en el ámbito de la protección de la confidencialidad de las comunicaciones y de las personas físicas en lo que respecta al tratamiento de datos personales en el contexto de los servicios de la sociedad de la información», Cfr. Apartado 212 de la STJUE (Gran Sala) de 6 de octubre de 2020 (ECLI:EU:C:2020:791).

desprenda de tal actividad o información ilícita y, b) en caso de tener conocimiento actúe con prontitud para eliminar o impedir el acceso a la información.

La norma de transposición de esta Directiva en España es la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico (LSSI)[72], en esta se define qué se entiende como servicio de intermediación en el apartado b) de su anexo como aquel «*por el que se facilita la prestación o utilización de otros servicios de la sociedad de la información o el acceso a la información. 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*».

Dentro de esta categoría deben considerarse las redes sociales, blogs y cualquier página web que almacene datos de sus usuarios. Las redes sociales también insertan por defecto en su estructura un buscador, herramienta por medio de la cual se obtiene una lista de resultados relacionados según el parámetro buscado, el contenido que se muestra en esta lista es propio de la red social, sin embargo, los resultados pueden contener enlaces externos a otros sitios de Internet. El régimen de responsabilidades según su actividad está previsto también en la LSSI, el art. 13.2 de esta Ley se remite a los artículos siguientes. Para servicios de alojamiento o almacenamiento de datos se estará al contenido del art. 16, y para los servicios que faciliten enlaces a contenidos o instrumentos de búsqueda. Se trata de un régimen de exención de responsabilidades en ambos casos, siempre que los prestadores de servicios de intermediación: «*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*

[72] Es importante señalar que a través de esta ley también se transponen por medio de la modificación de algunos de sus preceptos (arts. 20, 21, y 31) el contenido de la Directiva 2009/136/CE, por medio del Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista (art. 4 del Título II. Modificaciones relativas a la transposición de Directivas en materia de Telecomunicaciones y Sociedad de la información).

diligencia para retirar los datos o hacer imposible el acceso a ellos». El contenido de la propia LSSI entiende como conocimiento efectivo a la determinación de un órgano competente que declare 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*».

En relación con la definición de «conocimiento efectivo», el Tribunal Supremo por sentencia 773/2009, de 9 de diciembre determina que: «*No es conforme a la Directiva -cuyo objetivo es, al respecto, armonizar los regímenes de exención de responsabilidad de los prestadores de servicios - una interpretación del apartado 1 del artículo 16 de la Ley 34/2.002 como la propuesta por la recurrente, ya que reduce injustificadamente las posibilidades de obtención del "conocimiento efectivo" de la ilicitud de los contenidos almacenados y amplía correlativamente el ámbito de la exención, en relación con los términos de la norma armonizadora, que exige un efectivo conocimiento, pero sin restringir los instrumentos aptos para alcanzarlo. Además de que el propio artículo 16 permite esa interpretación favorable a la Directiva - al dejar a salvo la posibilidad de "otros medios de conocimiento efectivo que pudieran establecerse" -, no cabe prescindir de que la misma atribuye igual valor que al "conocimiento efectivo" a 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*»[73]. Por lo tanto, no es necesario esperar a que se determine la ilicitud del contenido por un órgano judicial que ordene su retirada o acceso, pues el conocimiento efectivo puede realizarse por otros medios como la notificación de la persona afectada en su derecho al honor. Esto viene dado por el hecho de que el daño que se genera en las redes sociales, blogs o páginas de internet que albergan contenido de los usuarios resulta mayor al utilizarse este tipo de plataformas debido a la gran cantidad de usuarios que lo pueden visualizar al día, los cuales son

[73] F.D. 4º de la STS (Sala de lo Civil) 773/2009 de 9 diciembre (RJ 2010\131; ECLI:ES:TS:2009:7684).

exponencialmente difusores de estas publicaciones, en concordancia con el contenido de la STS 805/2013, de 7 de enero de 2014 [74].

Otro medio de conocimiento efectivo puede llevarse a cabo a través de herramientas de moderación de contenido, disponibles en casi todas las redes sociales, foros y blogs, utilizadas para eliminar contenido que van en contra de sus condiciones de uso. En las redes sociales se puede eliminar el contenido previa utilización de esta herramienta, ya sea por iniciativa propia del prestador de servicios de intermediación o como consecuencia de la denuncia de una publicación por algún usuario que lo estime contrario a las condiciones de uso. En relación con lo anterior, la STS 805/2013, de 7 de enero, igualmente señala que, si un foro en la web cuenta con sistemas de control, detección o moderación de contenido y no funcionan o no se activan correctamente, es responsable por no reaccionar frente a un ataque prohibiendo el acceso a la página o expulsar a un usuario, pese a conocer la información difundida a través del mismo [75].

Las vulneraciones realizadas por medio de algún servicio de la sociedad a la información tienen una mayor onda expansiva, las publicaciones de esta naturaleza tienen mayor alcance de transmisión por la propia naturaleza del medio. Como consecuencia de ello, la reparación de daño deberá hacerse por el mismo medio en el que se realizó la vulneración. Así, por ejemplo, encontramos la Sentencia 235/2014 del Juzgado de Primera Instancia de Sevilla [76], en el fallo se condena a «*eliminar de un perfil de Twitter los comentarios lesivos*» (en relación con la honorabilidad de la persona demandante) y «*a publicar el fallo de la sentencia a través de la cuenta de Twitter del demandado mediante la Transcripción del fallo en un Tweet usando una herramienta creada al efecto para aumentar el número de caracteres permitidos, publicándolo durante treinta días en el horario de mañana (de nueve a 14 horas) o tarde (de 17 a 22 horas)*» [77].

---

[74] F.J 4º de la STS (Sala de lo Civil) 805/2013, de 7 de enero de 2014 (RJ 2014\773; ECLI:ES:TS:2014:68).
[75] *Íd.*
[76] AC 2014\1875; ECLI:ES:JPI:2014:154.
[77] La Sentencia se recurrió, y la Audiencia Provincial de Sevilla (Sección 8ª) en Sentencia 259/2015 (JUR 2016\231770; ECLI:ES:APSE:2015:3634), confirma íntegramente la sentencia del *«A quo»*

3.2 Derecho a la intimidad

Otro derecho fundamental de gran importancia objeto de este estudio es el derecho a la intimidad. Los instrumentos internacionales hacen referencia a «la vida privada» y reconocen la privacidad del individuo. Así el art. 12 de la DUDH determina que «*Nadie será objeto de inherencias arbitrarias en su vida privada, su familia, su domicilio o a su reputación. Toda persona tiene derecho a la protección de la ley contrátales injerencias o ataques*»; el art. 17.1 del PIDCP se determina que: «*Nadie será objeto de injerencias arbitrarias o ilegales a su vida privada, su familia, su domicilio o su correspondencia, ni ataques ilegales a su honra o reputación*»; y art. 8.1 del Convenio Europeo de Derechos Humanos y de las Libertades Fundamentales (CEDH): «*Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia*». En los mismos términos también se encuentra previsto en el art. 7 de la CDFUE.

Antes de estudiar cómo se configura este derecho en el ordenamiento jurídico español, es imprescindible realizar una distinción entre lo que se entiende como privacidad en relación con el concepto de intimidad. Uno de los primeros estudios realizados al respecto fue el ensayo «*The right to privacy*» de WARREN y BRANDEIS, consistente en una crítica a la publicación de información relacionada con cuestiones personales en los medios de comunicación de la época. Este artículo precisa que el individuo es el único que tiene el derecho a decidir qué desea dar a conocer a los demás sobre sí mismo sin que otros lo hagan por él[78]. Frente a estas injerencias se basa la idea de privacidad, que sitúa la vida de cada persona en una esfera dentro de un ámbito mayor perteneciente o relativo al ámbito público, y que

imponiendo las costas del recurso a los apelantes. Posteriormente se interpuso un recurso de casación, sin embargo, se inadmitió, debido a que incurre en la causa de inadmisión contenida en el art. 483.2.4º de la LEC (si el recurso carece manifiestamente de fundamento o se ha resulto ya el fondo en otros recursos sustancialmente iguales), así pues el Tribunal Supremo, entiende que el recurrente pretende convertir el recurso de casación en una tercera instancia, cuando la ponderación de derechos (libertad de expresión y derechos de la información *vs* derecho al honor) realizado por el Tribunal de instancia se ajusta a la Doctrina, declarándose firme la sentencia recurrida e imponiendo de costas a la parte recurrente por Auto del 11 de octubre de 2016 (recurso 3083/2015) del Tribunal Supremo (sala de lo civil JUR 2016\224928; ECLI:ES:TS:2016:9170A).

[78] Respecto a esta afirmación, WARREN y BRANDEIS determinaron que: «*In every such case the individual is entitled to decide whether that which is his shall be given to the public. No other has the right to publish his productions in any form, without his consent*», *vid.* WARREN, S. Y BRANDEIS, L. D., «The right to privacy», *Harvard Law Review,* Vol. 4, No. 5. (Dec. 15, 1890), p. 196.

sin duda tiene que ver con el libre desarrollo de la personalidad y la autodeterminación de la persona.

Los conceptos de privacidad, vida privada e intimidad como bien apunta el Profesor VILLAVERDE MENÉNDEZ, son distintos, pero no distantes. Él precisa que «*la privacidad-vida privada es el género, la intimidad una de sus especies*» [79]. Para el Profesor CARRILLO cuando hablamos de intimidad nos debemos referir «*a aquel ámbito de la vida privada que resulta inaccesible a los demás salvo que medie su propio consentimiento, es un concepto más restringido del que materialmente sirve para definir el ámbito de lo privado*» [80]. De acuerdo con lo establecido en el numeral 29 la STEDH de 16 de diciembre de 1992, caso *Niemietz* v. Alemania [81] «*el respeto a la vida privada debe incluir también, en cierta medida, el derecho a establecer y desarrollar relaciones con otros seres humanos*». En el numeral 95 de la STEDH, caso Von Hannover v. Alemania (nº2), de 7 de febrero de 2012, se hace una referencia más extensa en relación de cómo debe entenderse esa vida privada, la cual «*comprende elementos que hacen referencia a la identidad de la persona tales como el nombre, su foto, su integridad física y moral; la garantía que ofrece el artículo 8 del Convenio está destinada principalmente a asegurar el desarrollo, sin emergencias externas, de la personalidad de cada individuo en relación con sus semejantes*».

En la CE se protege el derecho a la intimidad personal y familiar en su art. 18.1, derecho que es desarrollado por la Ley Orgánica 1/1982, de 5 de mayo; este derecho al igual que los demás derechos a la personalidad, tiene su base axiológica en la dignidad de la persona [82]. La definición de derecho a la intimidad como derecho fundamental según el Profesor REBOLLO DELGADO [83] contempla diversos rasgos

[79] VILLAVERDE MENÉNDEZ, I., «La intimidad, ese "terrible derecho" en la era de la confusa publicidad virtual» (en línea), *Espaço Jurídico: Joural of Law,* núm. 13, vol. 14, p. 59 Disponible en: https://dialnet.unirioja.es/descarga/articulo/4546679.pdf (consulta: 10 de septiembre de 2019).
[80] CARRILLO, M., «Los ámbitos del derecho a la intimidad en la sociedad de la comunicación», *XX Jornadas de la Asociación de Letrados del Tribunal Constitucional. El derecho a la privacidad en un nuevo entorno tecnológico,* Centro de Estudios Políticos y Constitucionales, Madrid, 2016, p. 13.
[81] STEDH de 16 diciembre de 1992, Caso Niemietz v. Germany (TEDH 1992\77; ECLI:CE:ECHR:1992:1216JUD001371088).
[82] En este sentido, el F.J. 5 de la STC (Sala Primera) 134/1999, de 15 de julio (RTC 1999\134; ECLI:ES:TC:1999:134) establece que «*El derecho a la intimidad salvaguardado en el art. 18.1 CE tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y al conocimiento de terceros, sean éstos poderes públicos o simples particulares, que está ligado al respeto de su dignidad*».
[83] REBOLLO DELGADO, L., *El derecho fundamental a la intimidad,* Ed. Dykinson, Madrid, 2000, pp.75-81.

imprescindibles, es un *derecho subjetivo y de defensa*, es decir, *«el derecho de intimidad ya no es solo la potestad que tenemos de que un tercero conozca o no nuestra vida privada, sino también la posibilidad de controlar los que los otros conocen de nosotros mismos»* [84], constituyéndose, por dos ámbitos: el interno *(ad intra), que* consiste en el derecho que tenemos a defendernos frente a intromisiones, y el externo *(ad extra)* la facultad de controlar lo que los demás saben de nosotros. También es una *garantía institucional de pluralismo y de democracia*, al estar presente en nuestro ordenamiento jurídico se garantiza la individualidad de las personas proyectada en una sociedad democrática.

Otro rasgo imprescindible es el de *garantía de libertad*, dentro de nuestra esfera privada, entendido como *«un ámbito de soberanía interna, entendido por soberanía la facultad última de decisión, se deduce de ello el componente de libertad»* [85]. Por último es importante señalar que este derecho es fundamental en el orden social «*dado que configura unos valores (art. 1.1, justicia, igualdad, libertad, y pluralismo político), que son articulados en la práctica por una serie de principios, y para los cuales, nuestro constituyente establece una finalidad, que no es otra que el contenido del art-10.1 de la propia CE (dignidad de la persona, los derechos inviolables que le son inherentes, libre desarrollo de la personalidad, respeto a la ley y a los derechos de los demás)»* [86].

Conforme a lo determinado por el Tribunal Constitucional español, el derecho a la intimidad *«tiene por objeto garantizar al individuo un ámbito reservado de su vida frente a la acción y al conocimiento de terceros, sean estos poderes públicos o simples particulares, que está ligado al respeto de su dignidad. El derecho a la intimidad atribuye a su titular el poder de resguardar ese ámbito reservado por el individuo para sí y su familia de una publicidad no querida. El art. 18.1 CE no garantiza una "intimidad" determinada, sino el derecho a poseerla, a tener vida privada, disponiendo de un poder de control sobre la publicidad de la información relativa a la persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público. Lo que el art. 18.1 garantiza es un*

[84] *Ib.*, p. 76.
[85] *Ib.*, p. 78.
[86] *Ib.*, p. 79.

derecho al secreto, a ser desconocido, a que los demás no sepan qué somos o lo que hacemos, vedando que terceros, sean particulares o poderes públicos, decidan cuáles sean los lindes de nuestra vida privada pudiendo cada persona reservarse un espacio resguardado de la curiosidad ajena, sea cual sea lo contenido en ese espacio. Del precepto constitucional se deduce que el derecho a la intimidad garantiza al individuo un poder jurídico sobre la información relativa a su persona o a la de su familia, pudiendo imponer a terceros su voluntad de no dar a conocer dicha información o prohibiendo su difusión no consentida lo que ha de encontrar sus límites, como es obvio, en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos» [87].

La anterior delimitación de este derecho constitucional, realizada tanto por la doctrina como por el Tribunal Constitucional [88], precisa una esfera de protección más delimitada que el termino de vida privada usado por el TEDH, tal y como tan acertadamente menciona el Profesor VILLAVERDE MENÉNDEZ, «*la intimidad del artículo 18.1 CE no es, ni necesita ser, sinónimo de privacidad o vida privada al modo anglosajón o de la jurisprudencia del TEDH. La intimidad de la CE es algo más preciso y relativo únicamente a la información sobre la persona y su ámbito familiar*», en esta se «*garantiza la intimidad, entendida no como lo íntimo, sino la decisión sobre qué queda reservado a la mirada ajena. El objeto del derecho a la intimidad del art. 18.1 CE no es la decisión sobre cómo vivir o un espacio que objetiva y materialmente quepa considerar como vida privada, sino la decisión sobre qué de nosotros pueden conocer los demás*» [89].

Las nuevas tecnologías suponen un nuevo entorno donde se desarrollan los derechos fundamentales, entre los que obviamente se encuentra el derecho a la intimidad. Como consecuencia, todos los agentes intervinientes en la prestación del servicio y los usuarios deberán observar este derecho. Uno de los mayores riesgos de intromisión al derecho a la intimidad en el entorno tecnológico viene dado por la forma en que se introduce y gestiona la publicidad en línea. Los responsables de una

[87] F.J. 5 de la STC (Sala Primera)134/1999, de 15 de julio (RTC 1999\134; ECLI:ES:TC:1999:134).
[88] Cfr. *Íd.* y el F.J. 5 de la STC (Sala Segunda)115/2000, de 5 de mayo (RTC 2000\115; ECLI:ES:TC:2000:115).
[89] VILLAVERDE MENÉNDEZ, I., *op. cit.*, p. 61.

posible intromisión en caso de no observar lo previsto por la ley, serían las redes de publicidad, los prestadores de servicios de la información y el editor de la página web donde se alberga la publicidad, también conocidos como *webmaster*. Estos últimos pueden ser también páginas dedicadas a la indexación de resultados o motores de búsqueda. Recientemente el TS ha establecido que también están obligados «*a preservar con la misma intensidad el derecho fundamental a la vida privada de las personas afectadas, impidiendo cualquier interferencia que pueda considerarse ilegítima*» [90].

La publicidad online «*entendida como comunicaciones comerciales que, con la finalidad de promocionar bienes o servicios, alcanzan a los consumidores a través de canales digitales basados en internet (páginas web, aplicaciones, resultados de búsqueda, correos electrónicos, etc.), es un elemento fundamental en el desarrollo de internet*» [91]. Casi todas las páginas web en la actualidad tienen algún tipo de espacio publicitario. Sin duda esta nueva forma de hacer marketing en las empresas haciendo uso de las nuevas tecnologías trae más rendimientos de los imaginables, sin embargo, no hay que olvidar que los prestadores de servicios de la sociedad de la información deben observar el cumplimiento del orden jurídico español y comunitario. El uso de *cookies* en este tipo de publicidad es crucial. Gracias a estas, las redes de publicidad se encargan de gestionar y analizar nuestras preferencias de navegación para mostrarnos lo que queremos ver, y es así, como normalmente se financian los servicios «gratuitos» que prestan al usuario. Pero habrá que pagar un coste a cambio por esa relativa gratuidad, la respuesta es simple, datos e invasión a la intimidad de las personas. Sin embargo, este derecho nos da la potestad de desarrollarnos libremente como personas y compartir nuestra vida privada o familiar con quien nos apetezca y, a defendernos frente a intromisiones a la misma.

Los usuarios normalmente no se detienen a pensar qué información quieren compartir y con quién en el ámbito digital, de esta manera resulta sencillo aceptar las políticas de privacidad o las *cookies,* con tal de poder acceder a un servicio de la

[90] F.D. 3 de la STS (Sala de lo Contencioso-Administrativo, Sección 3ª) 12/2019 de 11 de enero (RJ 2019\8; ECLI:ES:TS:2019:19).
[91] PÉREZ BES. F., *La publicidad comportamental online*, UOC, Barcelona, 2012, p. 7.

sociedad de la información, aunque retirar esa aceptación y sus efectos puede resultar complicado.

Existen muchos tipos de publicidad en línea, por ejemplo, la publicidad conceptual «*es la que selecciona con base en el contenido que está viendo el sujeto en un momento determinado. En el caso de un buscador, el contenido puede derivarse de las palabras clave de la búsqueda, de la búsqueda anterior o de la dirección IP del usuario si esta indica su probable ubicación geográfica*» [92], o la publicidad seleccionada realizada «*con base en las características conocidas del sujeto (edad, sexo, ubicación geográfica, etc.) proporcionadas por el usuario al inscribirse o registrarse*» [93], que es la utilizada en las redes sociales. Quizás la más lesiva para la vida íntima del usuario sea la comportamental, que está basada en técnicas de segmentación de mercado. De acuerdo con la Real Academia Española, un segmento de mercado, en términos económicos es «*uno de los grupos homogéneos diferenciados a los que se dirige la política comercial de una empresa*» [94]. Actualmente, uno de los parámetros para segmentar la publicidad es el comportamiento de los usuarios en línea, llevado a cabo por medio de cookies.

Este tipo de publicidad ha sido definida por el GT29 como aquella *«basada en la observación continuada del comportamiento de los individuos. La publicidad comportamental busca estudiar las características del comportamiento a través de sus acciones (visitas repetidas en un sitio concreto, interacciones, palabras clave, producción de contenidos en línea, etc.) para desarrollar un perfil específico y proporcionar así a los usuarios anuncios a medida de los inferidos de su comportamiento (…) la publicidad comportamental puede dar a los anunciantes un cuadro detallado de la vida en línea del usuario, con muchos de los sitios y de las páginas concretas que ha visitado, cuánto tiempo ha durado la visita, durante cuánto tiempo ha visitado determinados artículos, en qué orden, etc.»* [95].

---

[92] GT29, Dictamen 2/2010 sobre publicidad comportamental en línea, adoptado el 22 de junio de 2010 (consulta y descarga: 10 de diciembre de 2019), p. 5.
[93] *Íd.*
[94] Cfr. DLE, *segmento:* https://dle.rae.es/segmento?m=form (consulta: 10 de diciembre de 2019).
[95] Literalmente establece: «*is based on the observation of the behaviour of individuals over time. Behavioural advertising seeks to study the characteristics of this behaviour through their actions*

Sin embargo, matizaría la definición dada por el GT29 en el sentido de que la técnica empleada en la publicidad comportamental permita el envío de publicidad a un usuario concreto identificado. Siendo precisos, la indagación que caracteriza a la publicidad comportamental se refiere al rastreo de la actividad llevada a cabo por navegadores (a través de las *cookies* instaladas en estos) que, efectivamente, estarán instalados en concretos terminales; pero no se refiere a la actividad desarrollada por un concreto usuario identificado. Así pues, cuando hablamos de publicidad comportamental nos referimos a aquella publicidad online dirigida a un concreto navegador instalado en un terminal electrónico que, evidentemente, es utilizado por un usuario durante su navegación.

La regulación a la publicidad en línea viene dada por 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 (Directiva sobre privacidad y comunicaciones electrónicas), pues supone extraer información de los equipos terminales de los usuarios, relacionada con su actividad y su uso puede vulnerar la esfera privada de los mismos. El considerando 25 de esta Directiva reconoce el uso legítimo de las cookies en relación con la publicidad en la web. Sin embargo, también establece que los usuarios deben tener información clara y precisa sobre su uso conforme a la hoy extinta Directiva 96/46/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.

El art. 5.3 de la Directiva 2002/58/CE es el que regula específicamente este tipo de publicidad, a tenor literal determina que «*Los Estados miembros velarán por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva*

(repeated site visits, interactions, keywords, online content production, etc.) in order to develop a specific profile and thus provide data subjects with advertisements tailored to match their inferred interests», GT29, Dictamen 2/2010, p. 3.

95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento. La presente disposición no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado». Posteriormente, el apartado 3 del art. 5 se modificó por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009. Dicho cambio consistió en establecer como condición el consentimiento del usuario previa información clara y completa para poder permitir el almacenamiento o en su caso el acceso a la información almacenada en el equipo terminal del usuario. Sin embargo, se establecen dos excepciones a esta condición. La primera es que el almacenamiento o el acceso a la información deberá realizarse con fines técnicos para que pueda efectuarse la transmisión de una comunicación a través de una red de comunicaciones electrónicas. La segunda es que se podrán realizar cualquiera de estas dos opciones siempre y cuando sea para prestar un servicio de la sociedad de la información expresamente solicitado por el usuario. Por lo que todas aquellas cookies insertadas en cualquier servicio de la sociedad de la información deberán contar con el consentimiento de los usuarios cuando estos hayan obtenido previamente una información clara y precisa de su funcionamiento. El segundo supuesto de excepción está revestido de cierta singularidad, ya que casi todos los servicios de la sociedad de la información en la navegación web son mayoritariamente solicitados por los usuarios. Pensemos en un motor de búsqueda, su utilización por el usuario supone la prestación de un servicio de intermediación solicitado por el usuario, por lo que se podrán insertar *cookies* en el ordenador o equipo terminal del usuario sin que previamente se expliquen sus usos y fines. Cabe destacar que estos servicios de motor de búsqueda son económicamente viables gracias a la publicidad que se visualiza en la lista de resultados, por lo que es evidente que se insertaran cookies con esa finalidad y, por tanto, sujetos al régimen de responsabilidad de la Sección segunda del Capítulo II del Título II de la LSSI.

El artículo 22.2 de la LSSI en relación con este tema establece que «*Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y*

recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones. Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario»[96]. El contenido de este artículo fue introducido en la LSSI por la Disposición Final Segunda de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, que transpone al ámbito nacional la Directiva 2009/136/CE.

En el año 2016 fue sustituida la Directiva 95/46/CE por el Reglamento 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 (Reglamento general de protección de datos -RGPD-). A nivel nacional en 2018 se aprueba la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, por la que se deroga la LO 15/1999, de 23 de diciembre.

Los principales cambios introducidos por este nuevo marco jurídico y que tienen relación con las *cookies* son los referentes al consentimiento de los usuarios y al diseño de estas tecnologías. El consentimiento pasa de ser tácito a ser explícito e inequívoco para cada una de las finalidades del tratamiento. En el RGPD se contempla en el apartado de definiciones que debe entenderse como «elaboración de perfiles» a «*toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos*

[96] Aunque se hace referencia a la LO 15/1999, de 13 de diciembre, ahora se debe estar a lo dispuesto en la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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»; esto es básicamente lo que vienen a hacer las *cookies*. En el artículo 25 del RGPD se establece que debe tenerse «*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*», por lo que técnicamente por diseño y por defecto estas *cookies* deberán ser respetuosas con lo establecido el RGPD. A nivel estatal estos cambios son introducidos por los artículos 6 y 73.d) de la LO 3/2018.

Sin embargo, el marco jurídico descrito con anterioridad establecido en la Directiva 2002/58/CE y en la LSSI parece tener fecha de caducidad. Actualmente se está gestando mediante procedimiento ordinario [97] la Propuesta de Reglamento del Parlamento europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas por el que se deroga la Directiva 2002/58/CE (Reglamento sobre privacidad y comunicaciones electrónicas). Este tiene como objetivo, al igual que la normativa anterior, complementar la regulación en materia de protección de datos personales (RGPD) de conformidad con su considerando 5 y su art. 1.3. En el considerando 20 de la Propuesta del Reglamento denominado *e-Privacy*, también se reconoce que las *cookies* pueden «*recopilar a distancia información relacionada con el dispositivo del usuario final a efectos de identificación y seguimiento utilizando técnicas tales como la "huella digital de dispositivo", con frecuencia sin el conocimiento del usuario final,*

[97] De conformidad con lo establecido en el art. 294 del TFUE.

lo cual puede suponer una grave intromisión en la vida privada de esos usuarios finales».

En relación con las cookies la propuesta también prevé en su art. 8 la protección de la información almacenada en los equipos terminales de los usuarios finales y relativa a dichos equipos en los siguientes términos: «*1.El uso de las capacidades de tratamiento y almacenamiento de los equipos terminales y la recopilación de información del equipo terminal de los usuarios finales, incluida la relativa a su soporte físico y lógico, excepto por parte del usuario final, estarán prohibidos, salvo por los motivos siguientes: a)cuando sean necesarios con el fin exclusivo de efectuar la transmisión de una comunicación electrónica a través de una red de comunicaciones electrónicas, o b)cuando el usuario final haya dado su consentimiento, o c)cuando sean necesarios para la prestación de un servicio de la sociedad de la información solicitado por el usuario final, o d)cuando sean necesarios para medir la audiencia en la web, siempre que esa medición corra a cargo del proveedor del servicio de la sociedad de la información solicitado por el usuario final*». Por lo que se añaden dos supuestos de excepción, el de consentimiento y el de medición de la audiencia, esta última deberá realizarla el propio servicio de la sociedad de la información que provea el servicio al usuario, es decir que empresas dedicadas a esta actividad que no cumplan este requisito tendrán que recabar el consentimiento del usuario[98].

Respecto al consentimiento, hasta ahora se otorga por medio del aviso de utilización de cookies, que aparece de manera emergente en la página web que se vista. En esta propuesta de reglamento inicialmente se preveía que se podría llevar a cabo en el momento de instalar el navegador o aplicación por la que se navegue por internet o cuando se actualizase el mismo, como respuesta a la ineficacia que suponían los avisos de cookies, pues los usuarios los aceptaban con tal de acceder al

[98] Hasta diciembre de 2020, estos supuestos seguían siendo los mismos. En relación con el inciso c) su redacción ha cambiado a: «*sea estrictamente necesario desde el punto de vista técnico para prestar el servicio solicitado específicamente por el usuario final*», Cfr. Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 4 November 2020 (OR. en) 9931/20. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017PC0010 (consulta: 20 de diciembre de 2020).

contenido de la página web, de conformidad con el considerando 22 y al art. 10 de la propuesta. Lo que colocaba a los navegadores como agentes coadyuvantes «*en hacer cumplir esta nueva normativa en pro de un consentimiento informado*», de tal manera que «*la información que se dará a los usuarios consistirá en hacerles saber cuáles son las opciones con las que cuentan en relación con la confidencialidad. De esta manera, se cumplirá con los parámetros establecidos en los arts. 4.11 y 7 del RGPD, evitando así la instalación de cookies de terceros*»[99]. Sin embargo, el contenido del art. 10 se ha eliminado por haber suscitado preocupaciones «*con respecto a la carga para los navegadores y las aplicaciones, el aspecto de la competencia, el vínculo con las multas por incumplimiento, pero también las repercusiones para los usuarios finales y la capacidad de esta disposición para abordar, por ejemplo, la cuestión de la fatiga del consentimiento, lo que suscita dudas sobre su valor añadido. 10 y los respectivos considerandos*»[100].

Existen empresas relacionadas principalmente al servicio de red social que suministran a sus usuarios como: *Facebook Messenger, Instagram, Snapchat,* etc. que también deber ser consideradas como prestadores de servicios de comunicaciones electrónicas, ya que ofrecen al usuario servicios como telefonía vocal y mensajería, como bien determina el considerando 10 de la Directiva 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas (versión refundida): «*Determinados servicios de comunicaciones electrónicas regulados por la presente Directiva podrían entrar también en el ámbito de la definición de "servicio de la sociedad de la información" que figura en el artículo 1 de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo. Las disposiciones de dicha Directiva que regulan los servicios de la sociedad de la información se aplican a esos servicios de comunicaciones electrónicas en la medida en que la presente Directiva u otros actos jurídicos de la Unión no contengan más disposiciones específicas aplicables a los*

[99] GONZÁLEZ MENDOZA, D.P., «Panorama jurídico actual sobre la elaboración de perfiles a partir de *cookies* y dirección IP», BUENO DE MATA, F. (Dir.), *Fodertics 7.0 Estudios sobre derecho digital,* Comares, Granada, 2017, p. 78-79.

[100] Cfr. Council of the European Union, Brussels, 10 July 2018 (OR. en) 10975/18, Interinstitutional File: 2017/0003(COD), p.3. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10975_2018_INIT&from=EN (consulta: 21 de diciembre de 2020).

servicios de comunicaciones electrónicas. No obstante, los servicios de comunicaciones electrónicas como la telefonía vocal, la mensajería y los servicios de correo electrónico están cubiertos por la presente Directiva». Por lo que, entrarían plenamente en la definición dada por el art. 2.4 de esta Directiva. Consecuentemente, tendrá que aplicarse en cuanto salga a la luz el Reglamento *e-privacy,* al contenido de las comunicaciones electrónicas: «como texto, voz, vídeos, imágenes y sonidos» [101], remitidos por este tipo de medios.

Los que también tendrán que estar al contenido del futuro Reglamento *e-Privacy,* serán todas aquellas empresas que, sin ser su actividad principal la prestación de servicios de la sociedad de la información, den acceso a internet a los usuarios en sus establecimientos a través de su actividad comercial. La recogida de datos se realiza principalmente con usos comerciales, lo que puede suponer en algunos casos también una intrusión a la privacidad de sus usuarios, y afectar su derecho a la protección de datos personales.

Otro tipo de acción que puede llegar a afectar al derecho a la intimidad de los usuarios se deriva de las publicaciones realizadas por estos. Cuando realizamos cualquier tipo de publicación en nuestro muro o *timeline* se puede verter información de los demás sin su consentimiento. Este tipo de publicaciones normalmente se realizan sin tener una especial diligencia hacia quienes pueden visualizarlas o, mejor dicho, este tipo de publicaciones se realizan en perfiles abiertos, lo cual supone una mayor audiencia y con ello mayor efecto multiplicador en relación con perfiles que se mantienen cerrados a la «lista de amigos». Las publicaciones por su contenido pueden afectar cualquiera de los derechos de la personalidad consagrados en el art. 18.1 CE [102].

[101] Art. 4.3.b) de la Propuesta de Reglamento *e-Privacy*.

[102] En este sentido FROSINI, V.: «*Los derechos humanos en la era tecnológica*» establece que «*Ciertamente, el progreso tecnológico puede ser portador de beneficios o de perjuicios, según como lo encause la voluntad humana; ciertamente, ha dado origen a nuevas situaciones que han provocado la necesidad de nuevas elecciones y decisiones, en ocasiones incluso angustiosas*», *vid.* FROSINI, V., «Los derechos humanos en la era tecnológica», PÉREZ LUÑO, A. (Coord.), *Derechos humanos y constitucionalismos ente el tercer milenio*, Ed. Marcial Pons, Madrid, 2006, p. 91.

3.3 Derecho a la propia imagen

También, dentro de los denominados derechos de la personalidad, encontramos al derecho fundamental a la propia imagen, de forma que partiremos del concepto de imagen para después definirlo. De acuerdo con lo establecido en el Diccionario de la Lengua Española, se define imagen en su primera acepción como *«Figura, representación, semejanza y apariencia de algo»*, por tanto, podría atreverme a decir que la imagen individual de las personas son el signo o representación más distintivo de los individuos, ya que la hace única e irrepetible. Este derecho entonces, protege reconoce la facultad *«para decidir y controlar el uso de su propia imagen y, por ende, el deber de los demás de respetar dicha decisión»* [103], o dicho en otras palabras «*se configura como un derecho de la personalidad, que atribuye a su titular la facultad de disponer de la representación de su aspecto físico que permita su identificación, lo que conlleva tanto el derecho a determinar la información gráfica generada por los rasgos físicos que le hagan reconocible que puede ser captada o tener difusión pública*» [104], y protege a las personas en un sentido negativo contra injerencias externas [105], «*consiste en esencia en impedir la obtención, reproducción o publicación de la propia imagen por parte de un tercero no autorizado, sea cual sea la finalidad –informativa, comercial, científica, cultural, etc.- perseguida por quien la capta o difunde*» [106] sin su autorización.

No está de más decir que, *«el hecho de que la Constitución haya considerado el derecho a la propia imagen merecedor de su reconocimiento como derecho fundamental queda, por tanto, justificado a partir de su vinculación con la dignidad humana»* [107]. Este derecho pese a ser autónomo guarda estrecha relación con los demás derechos a la personalidad, protege a la imagen pero no su aspecto íntimo [108], el cual queda salvaguardado por el derecho a la intimidad, que también corresponde a la categoría de derechos a la personalidad, y se encuentra contemplado también en el art, 18.1 de la CE, y desarrollado por la Ley Orgánica 1/1982, de 5 de mayo, de

[103] *Ib.*, p. 21.
[104] F.J. 3 de la STC (Sala Primera) 158/2009, de 29 de junio (RTC 2009\158; ECLI:ES:TC:2009:158).
[105] PASCUAL MEDRANO, A., *El derecho Fundamental …op. cit*. p.,20.
[106] F.J. 2 de la STC 81/2001, de 26 de marzo (RTC 2001\81; ECLI:ES:TC:2001:81).
[107] PASCUAL MEDRANO, A. *El derecho Fundamental …op. cit*., p. 25.
[108] F.J. 3 del ATC 28/2004, de 6 de febrero (RTC 2004\28 AUTO; ECLI:ES:TC:2004:28A).

protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen.

Respecto a lo anterior, el Tribunal Constitucional se pronuncia en los siguientes términos: *«El derecho a la propia imagen, reconocido por el art. 18.1 de la Constitución a la par de los del honor y la intimidad personal, forma parte de los derechos de la personalidad y como tal garantiza el ámbito de libertad de una persona 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 persona. En la medida en que la libertad de ésta se manifiesta en el mundo físico por medio de la actuación de su cuerpo y las cualidades del mismo, es evidente que con la protección de la imagen se salvaguarda el ámbito de la intimidad y, al tiempo, el poder de decisión sobre los fines a los que hayan de aplicarse las manifestaciones de la persona a través de su imagen, su identidad o su voz»* [109].

Como ya mencionamos anteriormente, ningún derecho fundamental tiene carácter absoluto, estos encuentran su límite en los demás. En el caso de los derechos de la personalidad, las personas cuentan con un mecanismo para su protección y en su caso resarcimiento del daño en caso de alguna injerencia contemplados en la LO 1/1982, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen. Estos nos dan la posibilidad frente a intromisiones ilegitimas de llevarse a cabo la reclamación por la vía ordinaria o por el recurso de amparo ante el Tribunal Constitucional, y en el caso de que estemos frente a daño moral la reclamación de un importe en concepto de indemnización por el daño [110].

[109] F.J. 3 de la STC (Sala Segunda)117/1994, de 25 de abril (RTC 1994\117; ECLI:ES:TC:1994:117). Otra sentencia relevante que nos sirve para identificar en qué consiste la vulneración de este derecho es la STS 241/2003, de 14 de marzo (Sala 1ª RJ 2003\2586; ECLI:ES:TS:2003:1750), la cual establece en su F.D.3º que *«el derecho a la propia imagen es el derecho que cada individuo tiene a que los demás no reproduzcan los caracteres esenciales de su figura sin consentimiento del sujeto, de tal manera que todo acto de captación. reproducción o publicación por fotografía, filme u otro procedimiento, de la imagen de una persona en momentos de su vida privada o fuera de ellos supone una vulneraci6n o ataque al derecho fundamental a la imagen»*.

[110] Arts. 9º.1 y 4 de la LO 1/1982, de 5 de mayo, y art. 53.2 de la CE.

En relación con la posible colisión entre el derecho a la propia imagen con alguno de los derechos contemplados en el art. 20.1, es decir, con los derechos de expresión e información (que más adelante se estudiarán), es importante tener en cuenta que en el momento de realizarse la ponderación de estos dos derechos debe tenerse en cuenta que la captación de figuras públicas en lugares públicos no se reputará una intromisión al derecho a la propia imagen, debido a que estas ayudan a la formación de una opinión sobre la vida democrática del país, sin embargo, el contenido del art. 8 de la LO 1/1982, se ha matizado por el TC, ya que si las imágenes de los personajes públicos han sido obtenidas de un ámbito propio y reservado como el de su vida familiar, de manera clandestina, y publicadas sin su consentimiento estas acciones suponen una intromisión al derecho a la propia imagen [111].

Otra cuestión relacionada con la colisión de los derechos de la personalidad contenidos en el art. 18.1 respecto a los contenidos en el art. 20.1 de la CE, es la relativa al denominado derecho de rectificación, contemplado en la Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación, este derecho podrá ejercerse por los individuos en caso de que se dé difusión de información que pueda causarle algún perjuicio.

Otra ley que prevé la protección del derecho a la propia imagen y demás derechos de la personalidad, es la LO 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las fuerzas o cuerpos de seguridad en lugares públicos, esta tiene por objeto regular el uso de los medios de grabación de imágenes y sonido utilizados por las Fuerzas y Cuerpos de Seguridad introduciendo garantías para el ejercicio de los derechos y libertades reconocidas en la Constitución [112].

Las nuevas tecnologías basadas en el uso de Internet, específicamente los servicios de la sociedad de la información suponen un nuevo marco de desenvolvimiento de los derechos de la personalidad. Facebook, Instagram y casi todas las redes sociales, así como los servicios de almacenamiento de vídeo como YouTube son nuevas plataformas por las que los usuarios se pueden expresar. Sin

[111] FJ 6 (in fine) de la STC (Sala Segunda) 176/2013, de 21 de octubre (RTC 2013\176; ECLI:ES:TC:2013:176).
[112] Preámbulo tercer párrafo de la LO 4/1997, de 4 de agosto.

embargo, la publicación de imágenes en este tipo de servicios puede generar una coalición entre los derechos contenidos en el art. 18.1 de la CE y los del art. 20.1 a) y d). por lo que habrá que hacerse una ponderación en cada caso concreto.

El Tribunal Supremo en su sentencia 91/2017, de 15 de febrero, ha determinado que si un medio de comunicación publica una imagen sustraída de un perfil de *Facebook* esta es una intromisión ilegítima a este derecho, pues esta se ha realizado sin el consentimiento del mismo y la fotografía no fue obtenida del lugar donde se produjeron los hechos, establece al tenor literal: «*Que en la cuenta abierta en una red social en Internet, el titular del perfil haya "subido" una fotografía suya que sea accesible al público en general, no autoriza a un tercero a reproducirla en un medio de comunicación sin el consentimiento del titular, porque tal actuación no puede considerarse una consecuencia natural del carácter accesible de los datos e imágenes en un perfil público de una red social en Internet. La finalidad de una cuenta abierta en una red social en Internet es la comunicación de su titular con terceros y la posibilidad de que esos terceros puedan tener acceso al contenido de esa cuenta e interactuar con su titular, pero no que pueda publicarse la imagen del titular de la cuenta en un medio de comunicación. El consentimiento del titular de la imagen para que el público en general, o un determinado número de personas, pueda ver su fotografía en un blog o en una cuenta abierta en la web de una red social no conlleva la autorización para hacer uso de esa fotografía y publicarla o divulgarla de una forma distinta, pues no constituye el "consentimiento expreso" que prevé el art. 2.2 de la Ley Orgánica 1/1982 como excluyente de la ilicitud de la captación, reproducción o publicación de la imagen de una persona. Aunque este precepto legal, en la interpretación dada por la jurisprudencia, no requiere que sea un consentimiento formal (por ejemplo, dado por escrito), sí exige que se trate de un consentimiento inequívoco, como el que se deduce de actos o conductas de inequívoca significación, no ambiguas ni dudosas*» [113].

Tal y como se ha establecido en esta sentencia, las intrusiones al derecho a la propia imagen sacadas de redes sociales o alguna plataforma en donde el titular del perfil haya subido por *motu proprio* imágenes, y estas se suban a la web, ya sea en

[113] F.D. 5 de la STS (Sala de lo Civil) 91/2017, de 15 de febrero (RJ 2017\302; ECLI: ES:TS:2017:363).

un perfil público o cerrado, debido a que las formas para ambos tipos de perfiles de descargar las mismas, no autorizan cualquier medio ya sea escrito o digital para que se asocien a una nota periodística, si estas no reflejan el hecho noticiable [114] y no se haya dado consentimiento expreso, de conformidad con lo establecido en la ley 1/1982, específicamente conforme a los artículos 2.2 y 8.2. Este hecho confiere a la persona afectada por tal intromisión a que se le indemnice de conformidad con el apartado 3 del art. 8 de la Ley 1/1982, por los daños causados. Otras sentencias en este mismo sentido son STC núm. 139/2001, de 18 de junio (FJ 5) [115]; SAP de Alicante núm. 366/2014, de 4 de diciembre [116]; SAP de León núm. 254/2017, de 27 de octubre [117]; SAP de A Coruña núm. 88/2017, de 10 de marzo (F.D. 3) [118].

También se puede realizar una intromisión al derecho de imagen si la persona afectada en un principio dio su consentimiento para aparecer en imágenes subidas a la web por otros usuarios, pero de manera posterior retira el mismo. De conformidad con el art. 2.3 de la LO 1/1982, en este sentido la SAP de Asturias núm. 233/2017, de 10 de mayo, el F.D. 2º determina que: «*En el caso de autos, consta acreditado que en las redes sociales de Facebook y Twitter en las que participa la demandada, se difundían algunas fotografías con la imagen del actor constante el matrimonio de las partes, presumiblemente con consentimiento del actor. Ahora bien, disuelto el matrimonio por causa de divorcio el 25 de noviembre de 2014 y habiendo sido requerida la demandada mediante correo electrónico de fecha 13 de noviembre de 2015, para que procediese a su retirada, correo cuya recepción no se discute, no cabe duda que la permanencia de algunas de ellas en la red, como lo demuestra las capturas de pantalla presentadas con la demanda (....) y una de ellas a la fecha de celebración de la audiencia previa, constituyen una intromisión legítima al derecho fundamental de la propia imagen del actor, en cuanto claramente inconsentida, como se apreció en la recurrida*» [119].

[114] Cfr. F.D. 3 de la STS (Sala de lo Civil) 397/2019, de 5 de julio (RJ 2019\2673; ECLI:ES:TS:2019:2255).
[115] RTC 2001\139; ECLI:ES:TC:2001:139.
[116] AC 2015\401; ECLI:ES:APA:2014:4043.
[117] JUR 2017\292938; ECLI:ES:APLE:2017:1040.
[118] AC 2017\838; ECLI: ES:APC:2017:535.
[119] F.D. 2ºde la SAP de Asturias 233/2017 de 10 mayo (JUR 2017\174442; ECLI:ES:APO:2017:1675).

4. LOS DERECHOS A LA LIBERTAD DE EXPRESIÓN Y A LA INFORMACIÓN.

Estos derechos están recogidos en el art. 20.1 incisos a) y d) de la CE a nivel nacional, a tenor literal establecen que: «*se reconocen y protegen los derechos a) A expresar y difundir libremente los pensamientos, ideas y opiniones mediante la palabra, el escrito o cualquier otro medio de reproducción (…) d) A comunicar o recibir libremente información veraz por cualquier medio de difusión. La ley regulará el derecho a la cláusula de conciencia y al secreto profesional en el ejercicio de estas libertades*». También están recogidos en Convenios y Tratados como en la DUDH artículo 19: «*Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, el de difundirlas, sin limitación de fronteras, en cualquier medio de expresión*»; en el art. 10.1 del CEDH: «*Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas, sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa*»; en el Pacto Internacional de los Derechos Civiles y Políticos, art. 19.2 se establece que: «*este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección*». A nivel comunitario se recoge en el art. 11 de la CDFUE: «*1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras*».

Pero ¿en qué consiste o cuál es el objeto de protección de este derecho o de estos dos derechos? Primero debemos aclarar que hay varias posturas acerca de si el contenido de estos dos incisos del art. 20.1 de la CE contemplan una pluralidad de derechos o si por el contrario hablamos de un solo derecho fundamental. El Tribunal Constitucional en el F.J. 4 de la Sentencia 6/1981, de 16 de marzo, dicta que: *«La libertad de expresión que proclama el art. 20.1 a) es un derecho fundamental del que gozan por igual todos los ciudadanos y que les protege frente a cualquier injerencia de*

los poderes públicos que no esté apoyada en la Ley, e incluso frente a la propia Ley en cuanto ésta intente fijar otros límites que los que la propia Constitución (arts. 20.4 y 53.1) admite. Otro tanto cabe afirmar respecto del derecho a comunicar y recibir información veraz (art. 20.1 d), fórmula que, como es obvio, incluye dos derechos distintos, pero íntimamente conectados. El derecho a comunicar que, en cierto sentido, puede considerarse como una simple aplicación concreta de la libertad de expresión y cuya explicitación diferenciada sólo se encuentra en textos constitucionales recientes, es derecho del que gozan también; sin duda, todos los ciudadanos, aunque en la práctica sirva, sobre todo, de salvaguardia a quienes hacen de la búsqueda y difusión de la información su profesión específica; el derecho a recibir es en rigor una redundancia (no hay comunicación cuando el mensaje no tiene receptor posible), cuya inclusión en el texto constitucional se justifica, sin embargo, por el propósito de ampliar al máximo el conjunto de los legitimados para impugnar cualquier perturbación de la libre comunicación social» [120]. Estos dos derechos como bien apunta el Tribunal Constitucional en la sentencia 107/1988, de 8 de junio, además de tener la consideración de derechos fundamentales de las personas, también constituyen al «*reconocimiento y garantía de la opinión pública libre, que es una institución ligada de manera inescindible al pluralismo político, valor esencial del Estado democrático*» [121]. Al comunicarnos con otros, y expresar nuestra opinión o juicios de valor en relación con nuestro entorno, ayuda a formar de manera crítica el debate de cuestiones de orden público. Por otro lado, recibir información relacionada con hechos de relevancia pública, ayuda a formar una opinión relacionada con el tema, lo cual genera una participación activa y toma de decisiones responsables e informadas en un entorno de pluralismo ideológico.

Para diferenciar uno de otro, es necesario como señala BUSTOS GISBERT atender a la «estructura última de toda comunicación», la cual presenta cinco elementos básicos: «*emisor, receptor, mensaje, canal y contexto. Trasladando estos elementos a términos jurídicos para el análisis de estas libertades, entenderíamos que el emisor es el sujeto activo del derecho (la persona que lo ejerce); el receptor sería el sujeto pasivo del derecho (entendiéndolo como la persona que recibe un beneficio del*

[120] RTC 1981\6; ECLI:ES:TC:1981:6.
[121] F.J. 1 de la STC (Sala Primera) 107/1988, de 8 de junio (RTC 1988\107; ECLI:ES:TC:1988:107).

ejercicio de este derecho); al referirnos a mensaje hablaríamos del objeto del derecho ("lo transmitido"); el canal sería el medio utilizado para ejercer el derecho; y finalmente, el contexto sería la situación que rodea la comunicación tutelada» [122].

Conforme a lo establecido por el TC, se trata de dos derechos completamente diferenciados y con contenido propio «*es posible señalar también que sean diferentes sus límites y efectos, tanto ad extra como ad intra*» [123]. Esta confusión suele darse cuando una persona cuya profesión es la de informar, publica alguna nota periodística cuyo contenido se basa en unos hechos ciertos y veraces, pero también en la opinión del autor. En estos casos podría decirse que la información es una manifestación del derecho de expresión, en cuanto que el artículo periodístico contiene el juicio subjetivo acerca de los hechos por parte del autor. Sin embargo, como bien apunta BUSTOS GISBERT «*pese a que exista este ejercicio conjunto, no debemos confundir conceptualmente ambos derechos, ya que sus efectos, límites y contenido no son los mismos*» [124].

La libertad de expresión «*es el fundamento de una sociedad democrática, marcada por el pluralismo, la tolerancia y el espíritu de apertura*» [125] y «*una de las condiciones previas para el funcionamiento de la democracia*» [126]. Este derecho fundamental según el contenido de la temprana STC 6/1988, de 21 de enero, nos permite manifestar todo tipo de pensamientos, ideas, opiniones o juicios de valor [127], sin que prime una autorización previa de algún poder del Estado, pudiendo

[122] BUSTOS GISBERT, R., «El concepto de libertad de información a partir de su distinción de la libertad de expresión», *Revista de estudios políticos,* núm. 85, 1994, pp. 270-271.
[123][123] F.J. 5 de la STC (Sala Primera) 6/1988, de 21 de febrero (RTC 1988\6; ECLI:ES:TC:1988:6). GUICHOT establece conforme al contenido de esta sentencia que deben ser considerados dos derechos los contenidos en este art. Constitucional: el de expresión y de la información, Cfr. GUICHOT, E., «Aspectos constitucionales del derecho de la comunicación», GUICHOT, E. (Coord.) *Derecho de la Comunicación,* Ed. Iustel, España, 2011, pp. 28 y ss.
[124] BUSTOS GISBERT, R., *op. cit*., p. 262.
[125] Numeral 34 de la STEDH de 10 de julio de 2008. Caso Soulas y otros contra Francia (TEDH 2008\42; ECLI:CE:ECHR:2008:0710JUD001594803): «*la liberté d'expression est l'un des fondements essentiels d'une société démocratique, caractérisée par le pluralisme, la tolérance et l'esprit d'ouverture*».
[126] *Íd.*
[127] Conforme con el contenido del F.J. 5 de la STC (Sala Primera) 6/1988, de 21 de febrero (RTC 1988\6; ECLI:ES:TC:1988:6).

realizarse en un entorno público o privado, cuyo límite es el contenido de los demás derechos fundamentales de otras personas [128].

El derecho a la información sería sin embargo aquel «*derecho a comunicar y recibir libremente información veraz, en cambio, sobre hechos o, tal vez más restringidamente, sobre aquellos hechos que pueden considerarse noticiables*» [129]. En palabras de GÓMEZ SÁNCHEZ, el derecho a la información «*se refiere al acto de transmitir información, con el requisito de que esta sea veraz*» [130]. Para este último autor tiene una «doble dirección», por un lado, está protegido el comunicar hechos noticiables y por otra la recepción de estos. En este sentido los profesionales dedicados a comunicar deberían cumplir con el requisito principal de veracidad en lo que publican, además de cumplir el deber de diligencia en lo que transmite asegurando y asegurándose de que son hechos contrastados con datos objetivos [131]. Las personas receptoras de la información son titulares del derecho a recibir información veraz sobre hechos noticiables resultado de una labor periodística. Son elementos exclusivos de la libertad de información, según BUSTOS GISBERT: «*la llamada prueba de la verdad, la relevancia pública de determinadas informaciones o la existencia de una necesaria labor preparatoria de la información*» [132].

Como se ha dicho con anterioridad los profesionales que se dedican a la difusión de hechos noticiables y que ejercen este derecho a diario, gozan «*de un derecho preferente atribuido en virtud de la función que cumplen, en aras del deber de información constitucionalmente garantizado*» [133]. Resulta necesario aclarar que no solo el derecho a la información es de titularidad de los informadores, toda persona que tenga conocimiento de manera directa a un hecho noticiable y de relevancia pública [134], y que lo transmita a la colectividad debe entenderse como sujeto activo de este derecho. En cambio, el derecho a la libertad de expresión no conoce de ningún tipo de profesión, los sujetos activos son todas las personas que lo ejercen.

[128] De acuerdo con el art. 20.4 CE.
[129] F.J. 5 de la STC (Sala Primera) 6/1988, de 21 de febrero (RTC 1988\6; ECLI:ES:TC:1988:6).
[130] GÓMEZ SÁNCHEZ, Y., *op. cit.*, p. 466.
[131] *Ib.,* p. 468.
[132] BUSTOS GISBERT, R., *op. cit.,* p. 262.
[133] F.J. 4 de la STC (Sala Segunda) 30/1982, de 1 de junio (RTC 1982\30; ECLI:ES:TC:1982:30).
[134] GÓMEZ SÁNCHEZ, Y., *op. cit.,* p. 474.

En relación con el canal, en el derecho a la información es aquel por el cual se recibe la información, el TC los denominó como «medios de comunicación social» [135]. Sin embargo, la evolución de los «vehículos habituales de la formación de la opinión pública» [136], se han transformado debido a los avances tecnológicos, ya sea en formato (*web*) o por que han emergido de herramientas para difundir (*Twitter*) o informar los hechos de naturaleza pública *(Periscope*). Aún se utilizan los medios escritos como diarios de circulación nacional y los medios televisivos para transmitir la información, a estos actualmente se les suman los medios de carácter digital, en los que entrarían las versiones web de estos dos medios. Las vías para ejercer nuestro derecho de libertad de expresión también se han visto modificados, además de expresarla de manera verbal o escrito (en papel), también puede darse y cada vez más frecuente la utilización de las redes sociales, blogs, plataformas de vídeo como YouTube, *Tik-Tok*, etc.

En cuanto al contenido, el TC haciendo referencia al derecho a la información establece que para que una noticia se vea plenamente protegida por este, se requiere (como se ha dicho antes) que la noticia refleje un hecho veraz [137] y que además, presente relevancia pública, «*elemento decisivo para la información (…)por razón de una persona o del propio hecho*» [138], siempre que verse en el caso de que se trate de personas de relevancia pública y personajes públicos, sobre cuestiones relacionadas con su cargo o actividad. De manera contraria el derecho a la libertad de expresión requiere una manifestación por parte del sujeto activo sobre cualquier tema del ámbito público o privado y sobre cualquier tipo de persona.

---

[135] F.J. 4 de la STC (Sala Segunda) 30/1982, de 1 de junio (RTC 1982\30; ECLI:ES:TC:1982:30).
[136] GÓMEZ SÁNCHEZ, Y., *op. cit.,* p. 276.
[137] F.J. 5 de la STC (Sala Primera) 6/1988, de 21 de enero (RTC 1988\6; ECLI:ES:TC:1988:6).: «*Cuando la Constitución requiere que la información sea «veraz» no está tanto privando de protección a las informaciones que puedan resultar erróneas -o sencillamente no probadas en juicio- cuanto estableciendo un específico deber de diligencia sobre el informador, a quien se le puede y debe exigir que lo que transmita como "hechos" haya sido objeto de previo contraste con datos objetivos, privándose, así, de la garantía constitucional a quien, defraudando el derecho de todos a la información, actúe con menosprecio de la veracidad o falsedad de lo comunicado. El ordenamiento no presta su tutela a tal conducta negligente, ni menos a la de quien comunique como hechos simples rumores o, peor aún, meras invenciones o insinuaciones insidiosas, pero si ampara, en su conjunto, la información rectamente obtenida y difundida, aun cuando su total exactitud sea controvertible. En definitiva, las afirmaciones erróneas son inevitables en un debate libre, de tal forma que, de imponerse "la verdad" como condición para el reconocimiento del derecho, la única garantía de la seguridad jurídica sería el silencio*».
[138] F.J. 3 de la STC (Sala Segunda) 219/1992, de 3 de diciembre (RTC 1992\219; ECLI:ES:TC:1992:219).

A lo largo de esta tesis ya se ha hecho referencia a estos dos derechos y se han relacionado con los contenidos en el art. 18 (honor, propia imagen, intimidad personal y familiar, y protección de datos personales), ya que todo derecho fundamental no denota carácter absoluto. Los límites de estos derechos fundamentales son otros derechos fundamentales, conforme a lo establecido así en el art. 20.4 CE. Motivo por el cual cuando dos o más derechos fundamentales colisionen debe realizarse una ponderación sobre la prevalencia de uno u otro. La doctrina del TC resulta bastante consolidada en el sentido de hacer prevalecer el derecho a la información respecto a los derechos de la personalidad contenidos en el art. 18.1 CE, siempre que se trate de hechos noticiables y de relevancia pública que puedan ayudar a la formación de una opinión sobre la vida democrática del país, ya sea *per se* por el hecho o por la persona involucrada en el mismo. En relación con el derecho a la libertad de expresión no se requiere que los hechos sean veraces, sin embargo, se requiere esta manifestación de ideas o juicios de valor se realicen con ausencia de «*expresiones injuriosas, ultrajantes y ofensivas sin relación con las ideas u opiniones que se expongan, y por tanto, innecesarias a este propósito, pues no reconoce un pretendido derecho al insulto*»[139]. Quedando fuera de la protección del derecho a la libertad de expresión «*las expresiones indudablemente injuriosas o sin relación con las ideas u opiniones que se expongan y que resulten innecesarias para la exposición de las mismas. Es decir, las que, "en las concretas circunstancias del caso sean ofensivas u oprobiosas"*»[140]. Otras expresiones que trasgredan la línea de lo lícito previstos así por el derecho penal para tipos penales del orden privado: injurias (arts. 208-210 CP) y calumnias (arts. 205-207 CP), así como en otros delitos de carácter público: enaltecimiento del terrorismo (art. 578 CP), o el discurso del odio (art. 510 CP), etc. Igualmente quedan fuera de protección otras expresiones por constituir tipos penales de orden privado, por ejemplo, injurias y calumnias, casi como otros delitos de carácter público como el enaltecimiento del terrorismo y el discurso del odio.

[139] F.D.3 de la SAN (Sala de lo Contencioso-Administrativo, Sección1ª) de 3 de diciembre de 2013 (RJCA 2014\496; ECLI:ES:AN:2013:5414).
[140] F.J. 2 de la STC (Pleno) 177/2015, de 22 de julio (RTC 2015\177; ECLI:ES:TC:2015:177).

Dicho lo anterior, también ha de recordarse como bien apunta IGLESIA PRADOS que «*a la hora de apreciar el carácter ofensivo, insultante o vejatorio de las palabras o términos empleados para expresar una idea u opinión crítica, o un juicio de valor sobre la conducta ajena, se ha de prescindir del análisis separado de cada término o de su mero significado gramatical, para optar por su contextualización*» [141]. La STS 554/2014, de 20 de octubre, en este mismo sentido determina que se necesita el contexto mismo en el que tuvieron lugar las expresiones de este tipo, determinándose que prevalecerá el derecho a la libertad de expresión cuando se empleen expresiones «*que, aun aisladamente ofensivas, al ser puestas en relación con la información que pretende comunicar o con la situación política o social*» en que tengan lugar estas, «*experimentan una disminución de su significación ofensiva y sugieren un aumento del grado de tolerancia exigible, aunque puedan no se plenamente justificables*» [142].

La posición de preeminencia frente a los derechos de la personalidad procederá *«en los casos siguientes: a) cuando la información verse sobre asuntos en los que por razón de su objeto sea relevante o resulte de interés general. O en terminología que emplea el TC, los hechos resulten "noticiables". b) O bien cuando la información se refiera a personas que, en razón de su dimensión pública, determinada por el cargo que ocupan, la función representativa que ejercen (personajes públicos) o la actividad profesional que habitualmente desarrollan personajes de notoriedad pública), también resulten de interés público (SSTC 171/1990 y 134/1999, FJ 7)»* [143]

Estos dos derechos como bien apunta RODRÍGUEZ-AMAT no están «*en peligro en la ley fundamental sino más bien allí dónde la ley ha crecido con los cambios*» [144]. El art. 20 de la CE además de establecer estos dos derechos fundamentales como bien apunta la STC 9/2007, de 15 de enero, en su F.J. 4, «*garantiza un interés constitucional: la formación y existencia de una opinión pública libre, garantía que reviste una especial trascendencia ya que, al ser una condición previa y necesaria para*

141 IGLESIA PRADOS, E. DE LA., *op. cit.,* p. 205.
142 F.D. 4 de la STS 217/2015, de 22 de abril (RJ 2015\1358; ECLI:ES:TS:2015:1532).
143 CARRILLO, M., *op. cit.,* p. 57.
144 RODRÍGUEZ-AMAT, J. R., *et al.*, «Gobernanza de Internet y libertad de expresión», CORREDOIRA Y ALFONSO, L. y COTINO HUESO, L. (Dirs.), *Libertad de expresión e información en Internet: amenazas y protección de los derechos personales*, Centro de Estudios Políticos y Constitucionales, 2013, p.75.

el ejercicio de otros derechos inherentes al funcionamiento de un sistema democrático, se convierte, a su vez, en uno de los pilares de una sociedad libre y democrática. Para que el ciudadano pueda formar libremente sus opiniones y participar de modo responsable en los asuntos públicos, ha de ser también informado ampliamente de modo que pueda ponderar opiniones diversas e incluso contrapuestas».

Tal y como lo establece el art. 10.2 del CEDH, el ejercicio de estas libertades entraña: «*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*» [145]. El TEDH por sentencia de 4 de diciembre de 2003 (caso Müslüm Gündüz contra Turquía) en relación con el contenido del apartado segundo del art. 10 del CEDH «*subraya principalmente que la tolerancia y el respeto de la igual dignidad de todos los seres humanos constituyen el fundamento de una sociedad democrática y pluralista. De ello resulta que en principio se puede juzgar necesario, en las sociedades democráticas, sancionar o prevenir todas las formas de expresión que propaguen, inciten, promuevan o justifiquen un odio basado en la intolerancia (incluida la intolerancia religiosa), si se quiere que las "formalidades", "condiciones", "restricciones" o "sanciones" impuestas sean proporcionadas al fin legítimo perseguido*» [146], inclusive cuando el desarrollo de estos derechos se realice en un entorno digital.

Este nuevo espacio de expresión e información suponen «*la recepción y la posibilidad de acceso a los contenidos por tal vía es directa y sin necesidad de espera a un momento temporal determinado, al ser la red un medio de transmisión de datos*

[145] Art. 10.2 del CEDH

[146] Apartado 40 de la STEDH de 4 diciembre 2003. Caso Müslüm Gündüz contra Turquía (TEDH 2003\81; ECLI:CE:ECHR:2003:1204JUD003507197): «*emphasise, in particular, that tolerance and respect for the equal dignity of all human beings constitute the foundations of a democratic, pluralistic society. That being so, as a matter of principle it may be considered necessary in certain democratic societies to sanction or even prevent all forms of expression which spread, incite, promote or justify hatred based on intolerance (including religious intolerance), provided that any "formalities", "conditions", "restrictions" or "penalties" imposed are proportionate to the legitimate aim pursued*».

que podríamos calificar como abierto para difundir opiniones, informaciones e imágenes las 24 horas del día»[147]. Las publicaciones realizadas por los usuarios en el entorno digital por ejemplo, en un blog o en una red social, en un espacio específico dentro de la misma o en forma de microblogging como ocurre en las redes sociales de Twitter o Tumblr, deben ser consideradas como una manifestación de la libertad de expresión. Los servicios de la sociedad de la información constituyen un nuevo espacio virtual donde manifestar nuestras opiniones o cualquier juicio de valor relacionado con cualquier tema por medio de palabras, fotografías y/o vídeos. Sin embargo, estas manifestaciones no siempre son bienintencionadas y puede, como en otros medios de comunicación, que los derechos de la personalidad colisionen bien con el derecho a la libertad de expresión o con el derecho a la información.

En la Web 1.0 por sus características era más fácil controlar el contenido de la información, tanto para los medios como para los gobiernos. Sin embargo, con la llegada de la denominada *Web* semántica, en todo el mundo se encuentran millones de potenciales informadores los cuales podrían compartir imágenes, vídeos y cometarios al respecto con ayuda de diferentes aplicaciones informáticas, eliminando cualquier tipo de filtro de la información, lo cual, nos ayuda a ser más conscientes de la realidad actual, ejemplo de ello está el uso de *Periscope*[148]. Sin embargo, como bien apunta el TEDH «*los sitios web son instrumentos de información y comunicación que se diferencian de la prensa especialmente en su capacidad para almacenar y difundir información, y en que las comunicaciones en línea y su contenido tienen más probabilidades de vulnerar el ejercicio y el disfrute de los derechos y libertades fundamentales, en particular, el derecho al respeto de la vida privada*»[149].

Tanto en este mundo virtual como en el mundo analógico, el límite de estos dos derechos se encuentra en los demás derechos fundamentales, principalmente

---

147 IGLESIA PRADOS, E. DE LA., *op. cit.,* p. 207.

148 *Pericope* es una red social que puede estar asociada a una cuenta de *Twitter*, la cual nos permite transmitir en directo desde cualquier parte del mundo en formato vídeo, lo que está ocurriendo a nuestro alrededor, desde nuestra vida cotidiana hasta algún hecho noticiable, en el siguiente link se podrá consultar más al respecto sobre esta aplicación Cfr. Verne, El País, Así es Periscope, la app de Twitter para transmitir tu vida en directo. Disponible en: http://verne.elpais.com/verne/2015/03/28/articulo/1427564916_014554.html (consulta: 15 de junio de 2017).

149 Numeral 91 de la STEDH de 28 de junio de 2018. Caso M.L. et W.W. contra Allemagne (TEDH 2018\67; ECLI:CE:ECHR:2018:0628JUD006079810).

en los derechos de la personalidad, que ante ataques dentro del mundo real o virtual se pueden ejercer acciones para hacer cesar las conductas lesivas y en su caso reparar el daño que pudo haber ocasionado la publicación u opinión [150]. Los ejercicios de estos dos derechos pueden estar condicionados por el contenido de la opinión o juicio de valor realizado en cualquier medio de comunicación o por el contenido de una noticia.

Como se dijo anteriormente estos dos derechos deberán prevalecer frente a los previstos en el art. 18.1, siempre y «cuando la noticia difundida por medios digitales sea veraz y se refiera «*a hechos con relevancia pública, que son de interés general*» [151] y que el contenido de la misma relacione el hecho noticiable con una persona de notoriedad pública, en el caso del derecho a la libertad de información. La prevalencia del derecho a la libertad de expresión, quedará condicionada al contenido del juicio de valor, en tanto no contenga expresiones innecesarias «*para exteriorizar una crítica por muy rigurosa que se quiera y, por tal, instrumentos de una inadmisible extralimitación*» [152].

En principio, las mismas deben ser consideradas como una manifestación de la libertad de expresión. Constituyen un nuevo espacio virtual donde manifestar nuestras opiniones o cualquier juicio de valor relacionado con cualquier tema, y puede tener cualquier formato permitido por las mismas, como de palabras, fotografías y/o vídeos. Es conveniente recordar que «*ni el ejercicio de la libertad ideológica ni la de expresión pueden amparar manifestaciones o expresiones destinadas a menospreciar o a generar sentimientos de hostilidad contra determinados grupos étnicos, de extranjeros o inmigrantes, religiosos o sociales, pues en un Estado como el español, social, democrático y de Derecho, los integrantes de aquellas colectividades tienen el derecho a convivir pacíficamente y a ser plenamente*

[150] En este caso, se pueden ejercer acciones como el derecho de rectificación, contemplado en la LO 2/1984, de 26 de marzo, reguladora del derecho de rectificación, la vía contemplada 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, lo contenido en el código penal por la comisión de algún delito como injurias, que solo puede ser perseguible mediante denuncia de la persona agraviada o de su representante legal (art.173.4 CP) o la acción de responsabilidad extracontractual derivada de un daño prevista el Código Civil (art. 1902 y 1903 del CC).

[151] F.D. 2º de la STS (Sala de lo Contencioso) 12/2019, de 11 de enero (RJ 2019\8; ECLI:ES:TS:2019:19).

[152] F.D. 3º de la STS (Sala de lo Civil) 805/2013, de 7 de enero (RJ 2014\773; ECLI:ES:TS:2014:68).

respetados por los demás miembros de la comunidad social»[153], lo cual, es extensivo a este entorno digital. Por lo que, las opiniones que contengan un «*ánimo subjetivo que conduce al autor a la comisión del hecho agresivo*»[154], de ninguna forma estarán amparados por el derecho a la libertad de expresión pues incitan o realzan el rechazo a lo que el sujeto entiende como diferente y por tanto contrario a la pluralidad e igualdad, y que pueden lesionar «*la dignidad de los colectivos contra los que se actúa*»[155]. Esta animadversión como lo evidencia la STC 177/2015, de 22 de julio, «*se proyectan sobre las condiciones étnicas, religiosas, culturales o sexuales de las personas. Pero lo cierto es que el discurso fóbico ofrece también otras vertientes, siendo una de ellas, indudablemente, la que persigue fomentar el rechazo y la exclusión de la vida política, y aun la eliminación física, de quienes no compartan el ideario de los intolerantes*». Estas conductas tipificadas como delitos en diversos artículos el Código Penal español (CP). Pensemos en opiniones que supongan un discurso al odio, previsto en el CP en su art. 510, o que supongan enaltecimiento del terrorismo, conducta también prevista como un delito en el art. 578 del CP.

Las redes sociales también pueden servir de manera instrumental para hacer eco o secundar la opinión de otros usuarios a través de iconos de «compartir» o «*retweet*». Es decir, que pueden ser consideradas como un medio de difusión entendido en términos de la STS 259/2011, de 11 de abril como «*trasladar, hacer saber, propagar, divulgar, descubrir o comunicar algo a terceros. Puede hacerse públicamente o de forma privada*». Por ejemplo, por la STS 706/2017, de 27 de octubre de 2017, se determinó que, para la configuración del tipo penal de enaltecimiento del terrorismo, no se exige que «*el acusado asuma como propio, razone o argumente la imagen y su mensaje, ni tampoco que sea el recurrente el que lo haya creado, basta que de un modo u otro accedan a él, y les de publicidad, expandiendo el mensaje a gran cantidad de personas*», tal como sucede con un «*retweet*», pues mediante esta plataforma la información puede ser difundida a terceros, quienes a su vez pueden difundirla en sus perfiles, lo cual facilita que otros

[153] F.J. 8 de la STC (Sala Primera) 214/1991, de 11 de noviembre (RTC 1991\214; ECLI:ES:TC:1991:214).
[154] STS (Sala de lo Penal) 646/2018, de 14 de diciembre, F.D. Único (RJ 2018\5588; ECLI:ES:TS:2018:4133).
[155] *Íd.*

a su vez puedan darle difusión. Es decir que esta acción permite «*el acceso a lo difundido por parte de un número plural de personas, que puede ser también indeterminado*» [156].

Los prestadores de servicios de intermediación deben guardar diligencia y control en relación con los posibles agravios a derechos fundamentales «*para evitar que la misma sirva de vehículo para la comisión de comportamientos ilícitos, no siendo adecuada su exoneración en caso de adopción de las medidas pertinentes para evitar que la difusión se produzca, más cuando ésta es de contenidos flagrantemente ilícitos. De este modo, el titular de la red social no puede ampararse en la generalidad y amplitud de los sujetos intervinientes y contenidos alojados, o en el incumplimiento de las pautas de uso existentes, pues debe establecer las medidas adecuadas para limitar estas conductas, las cuales no podrán ser disminuidas o erradicadas únicamente por medidas represivas, sino también por actuaciones preventivas de las mismas, a llevar a cabo por el titular de la red social mediante la previsión de los filtros previos pertinentes que las eviten y, entre ellos, los que permitan en todo caso determinar la identidad del usuario de la red social, por lo que si ello no es posible, la misma debiera ser quien asuma las consecuencias del ilícito*» [157]. No solo las redes sociales, todos los prestadores de servicios de intermediarios de la sociedad de la información, estarán sujetos al régimen de responsabilidad contenido en la Directiva 2000/31/CE (arts. 12-15) y en la LSSI (arts. 13-17).

Esta situación queda patente con el contenido de la STS 805/2013, de 7 de enero de 2014, donde se establece que si bien es cierto que el responsable de una página web «*no podía filtrar a priori la información que a través de sus foros de internet (…) contaba en su página web con sistemas de control, detección o moderación de su contenido, así como que, en el caso de autos, no funcionaron o no se activaron correctamente, (…) de manera que debió reaccionar frente al mismo y prohibir el acceso a la página, así mediante una expulsión de usuario, etc., nada de lo cual hizo, pese a ser conocedora de la información difundida*» [158]. Otro ejemplo nos lo

[156] F.D. 2º de la STS (Sala de lo Penal) 259/2011, de 12 de abril (RJ 2011\5727; ECLI:ES:TS:2011:3386).
[157] IGLESIA PRADOS, E. DE LA., *op. cit.*, p. 219.
[158] F.D. 4º STS (Sala de lo Civil) 805/2013, de 7 de enero de 2014 (RJ 2014\773; ECLI:ES:TS:2014:68).

da el contenido del F.D. 4º STS 128/2013, de 26 de febrero, que establece en este sentido que el titular de una página web «*y creadora del foro de debate abierto, debió extremar las precauciones y ejercer un mayor control sobre las opiniones y comentarios alojados, cuyas connotaciones despectivas y peyorativas para el demandante no podían pasarle inadvertidas»*, por lo que este debe procurar *«la pronta retirada de aquellos que manifiesta e inequívocamente aparecían como gravemente injuriosos o incitadores a la violencia. No puede pasar inadvertido el papel desempeñado por el titular de la página que no solo alberga un contenido externo, sino que genera la posibilidad de realizar comentarios, incorporándolos a la noticia y permite que se consideren como elemento de valoración de la misma*» [159].

Otra cuestión que entraña especial preocupación en este mundo digital son las «*fakenews*» por las cuales los medios de comunicación valiéndose de la inmediatez de los servicios de la sociedad de la información, principalmente por medio de las redes sociales, se pueden divulgar información falsa o darle mal uso a la misma, de ahí que *«Los peligros de una utilización abusiva, incontrolada o criminal de este espacio plantean ahora, de forma apremiante, la necesidad de su ordenación»* [160], ya que *«Internet ha supuesto un factor de incremento de formas de criminalidad, al potenciar la difusión de sabotajes, virus y abordajes a los sistemas por parte de un número imprevisible e incontrolable de piratas informáticos (Hackers)»*, de esta forma «*Internet implica, por tanto, el riesgo de un efecto multiplicador de los atentados contra derechos, bienes e intereses jurídicos»* [161].

La veracidad es uno de los elementos esenciales que debe contener una nota informativa para quedar amparada por el art. 20.1.d) CE. Los medios de información o personas dedicadas a la labor informadora o periodística deben tener especial diligencia al hacer eco de cualquier tipo de información. En las redes sociales muchas veces son lanzadas noticias falsas por los usuarios, en su carácter de generadores de contenido, noticias que pueden hacerse virales por los propios

[159] F.D. 4º STS (Sala de lo Civil) 128/2013, de 26 de febrero (RJ 2013\2580; ECLI:ES:TS:2013:1441).
[160] PÉREZ LUÑO, A., *La tercera generación de Derechos Humanos,* Ed. Aranzadi, Navarra, 2006, p. 103.
[161] *Ib.*, p. 93.

usuarios o gracias a la ayuda de *bots*[162]. Lo que no pueden hacer los medios de comunicación frente a este tipo de contenido que circula en la red, es difundirla como si estas noticias fuesen veraces y vigilar si tal contenido es contrastable.

Además de que muchas veces estas «*fakenews*» pueden resultar injuriosas, sin embargo, su propagación por medios de información, como bien apunta GARCÍA PÉREZ «*sólo hacen responsable al sujeto declarante, pero no al redactor y difusor de las declaraciones, salvo que el informador y el medio a través del cual se difunde hagan noticiable (y, por tanto, den publicidad) manifestaciones de terceros ofensivas contra el honor que no tengan relevancia o interés público, que manifiestamente carezcan de verosimilitud o tergiversen dichas declaraciones de forma desproporcionada, pues en tal caso, sí son responsables*» [163].

[162] Según la Fundéu actualmente puede ser utilizado para referirse a aquel «*programa que sirve principalmente para efectuar tareas simples y repetitivas en internet o simular la conducta humana*», Cfr. Fundéu, https://www.fundeu.es/recomendacion/bot-acortamiento-valido-en-espanol/ (consulta: 19 de diciembre de 2019).

[163] GARCÍA PÉREZ, C.L., «La responsabilidad civil de los medios de comunicación por vulneración del derecho al honor» (en línea), *Revista Doctrinal Aranzadi Civil-Mercantil*, núm. 1/2015, p. 9 (consulta: 15 de enero de 2020). Ref: BIB 2015\716.

CAPÍTULO II

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

1. PRIMEROS PASOS EN LA CONFIGURACIÓN DE LA PROTECCIÓN DE DATOS.

El primer antecedente del derecho a la protección de datos a nivel europeo data de 1950, año en que fue adoptado por el Consejo de Europa, el CEDH. En su art. 8 se contempla el derecho de toda persona al respeto de su vida privada, familiar, de su domicilio y de su correspondencia, estableciéndose que no podrá haber injerencias por parte de particulares o autoridades públicas a menos de que este establecido legalmente o por motivos tasados. Ello implica el respeto a los derechos y libertades fundamentales, particularmente al respeto a la vida privada a nivel europeo

Treinta años más tarde con el Convenio 108 del Consejo de Europa de 28 de enero de 1981 [164], se cristaliza el esfuerzo por parte del Consejo de Europa de crear un texto que fuera referente en materia de protección de datos compatible con los avances tecnológicos. Su principal finalidad aparece recogida en el art. 1, la cual es *«garantizar, en el territorio de cada parte, a cualquier persona física sean cuales fueren su nacionalidad o residencia, el respeto de sus derecho 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")».* El Profesor SERRANO PÉREZ establece que: *«La pretensión del Convenio es equilibrar dos derechos fundamentales - en el sentido de importantes- necesarios en toda sociedad democrática y que se situaban, en su punto de partida, en direcciones opuestas: por un lado, la protección de datos relativos a las*

[164] Según se establece en su artículo 1, el objeto y el fin del mismo es *«garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")»*.

personas y por otro, la libre circulación de las informaciones a través de las fronteras. Hacia la consecución de esa armonización se dirige el conjunto del Texto» [165].

Este Convenio fue ratificado por España el 27 de enero de 1984 y entró en vigor de forma general el 1 de octubre del mismo año, conforme a lo establecido en su artículo 22.2 [166]. Actualmente es un instrumento de gran relevancia a nivel internacional, pues además de ser parte los miembros del Consejo de Europa, son parte en la actualidad: Argentina, Burkina Faso, Cabo Verde, República de Mauricio, México, Marruecos, Senegal, Túnez y Uruguay [167], gracias a que el Comité de Ministros del Consejo de Europa puede invitar a cualquier Estado no miembro del Consejo de Europa a que se adhiera a dicho Convenio [168].

Consta de un número de veintisiete artículos, por los cuales se establecen pautas para el mejor tratamiento de los datos personales, para que esto sea eficaz primeramente se debe tener en cuenta una serie de definiciones, las cuales resultan fundamentales para el entendimiento entre los Estados parte (art. 2). El campo de aplicación serán los ficheros y los tratamientos automatizados de datos de carácter personal en los sectores público y privado (art. 3), pudiendo indicar en el momento de su aceptación, aprobación, adhesión o en un acto posterior a qué ficheros no les será aplicable; se señala también si el Convenio será aplicable a informaciones relativas a agrupaciones, asociaciones, fundaciones, sociedades, compañías o cualquier otro organismo y en su caso si será aplicable a ficheros no automatizados (art. 3.2). En este instrumento por primera vez se establecen los principios básicos para la protección de datos personales, estos últimos deben ser observados durante todo el tratamiento, incluso desde su recogida. Los datos serán obtenidos de forma

[165] SERRANO PÉREZ, M. M., *El derecho fundamental a la protección de datos. Derecho español y comparado,* Thomson Civitas, Madrid, 2003, p. 93.
[166] El art. 22.2 del Convenio 108 del Consejo de Europa, establece lo siguiente: *«El presente Convenio entrará en vigor el día primero del mes siguiente a la expiración de un periodo de tres meses después de la fecha en que cinco Estados miembros del Consejo de Europa hayan expresado su consentimiento para quedar vinculados por el Convenio, con arreglo a las disposiciones del párrafo anterior»*.
[167] Cuadro de firmas y ratificaciones del Convenio 108 para la protección de las personas con respecto al tratamiento automático de sus datos personales: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=BaeKoI48 (consulta: 6 de octubre de 2020).
[168] De conformidad con lo establecido en el artículo 23.1 del Convenio 108 del Consejo de Europa. Para poder invitar a un Estado no miembro deberá tomarse un acuerdo adoptado por la mayoría prevista en el art. 20 del Estatuto del Consejo de Europa, es decir, se adoptará por mayoría de dos tercios de los votos emitidos y por unanimidad de los representantes de los Estados contratantes que tengan derecho a formar parte del Comité.

leal y legitima, se utilizarán solo para las finalidades del tratamiento para los cuales fueron recogidos, los datos deberán ser adecuados pertinentes y no excesivos en relación con las finalidades, también deberán ser exactos y actualizados, y que los datos deberán ser conservados durante un periodo de tiempo que no exceda el requerido para las finalidades por las cuales hayan sido registrados [169].

De igual manera por primera vez, se les da a los datos la categoría de especiales a aquellos que denoten una ideología política, sus preferencias sexuales, el origen racial, los relativos a la salud y de índole religiosa. En principio el Convenio establece que este tipo de datos no serán automatizados salvo, que el derecho interno de la parte firmante prevea *garantías apropiadas* para su tratamiento (art. 6). Todas las medidas previstas para el tratamiento de los datos personales contenidas en el Convenio antes aludido se entenderán como limitativas, cada Estado parte podrá establecer medidas más robustas que las previstas en el mismo (art. 10). Entre otras cosas destaca el Convenio 108 que, también regula por primera vez los flujos transfronterizos de datos entre los Estados parte (art. 12).

A este Convenio se le han incorporado dos Protocolos, el de fecha de 8 de noviembre de 2001, relativo al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos [170], ratificado por 44 Estados [171] y en vigor desde el 1 de julio de 2004 [172]; y recientemente el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal, de 18 de mayo de 2018 (Convenio 108+), del cual hablaremos posteriormente.

Actualmente este instrumento ha sido firmado por 33 países de los cuales 30 son Estados parte del Consejo de Europa y 3 que no lo son; conforme con el art. 26

[169] De conformidad con lo contenido en el artículo 5 del Convenio 108.
[170] Cfr. Protocolo adicional al Convenido 108 de 8 de noviembre de 2001. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/8588474 (consulta: 24 de septiembre de 2019).
[171] Cfr. Lista de firmas y ratificaciones del Protocolo adicional del Convenio 108 de 8 de noviembre de 2001. Disponible en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/181/signatures?p_auth=XqFDzyr8 (consulta: 24 de septiembre de 2019).
[172] España lo ha firmado el día 24 de septiembre de 2009, ratificado el 3 de junio de 2010 y con vigencia desde el 1 de octubre de 2010.

entró en vigor a partir del día siguiente a la expiración de un periodo de tres meses, contados a partir de la fecha en que cinco Estados parte del Consejo de Europa se obligaron a su cumplimiento.

Ahora bien, en el marco de la legislación emitida por la Unión Europea, posterior a el Convenio 108, se presentó una propuesta de Directiva por parte del Consejo de las Comunidades Europeas, relativa a la protección de las personas en lo referente al tratamiento de datos personales, publicada el 5 de noviembre de 1990 en el Diario Oficial de las Comunidades Europeas y que finalmente se aprobó como 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, publicada en el Diario Oficial de las Comunidades Europeas el día 23 de noviembre de 1995.

Esta Directiva hace referencia a una serie de conceptos que también se incluían en el Convenio 108 [173], sin embargo, los perfeccionaba e incluía alguno más para el adecuado entendimiento de la Directiva, de igual forma clarifica el qué, el quién y el cómo se lleva a cabo el tratamiento de datos de carácter personal. Uno de los motivos fundamentales de su existencia, se atañe a las NTIC todo por la introducción y métodos automatizados para el tratamiento de los datos personales, como el uso de la informática, la cual facilitaba enormemente esta labor, así como la transmisión de los mismos. El objetivo de esta Directiva era la protección de las libertades y de los derechos fundamentales de las personas físicas y, en particular, el derecho a la intimidad, en lo que respecta al tratamiento de los datos personales (art. 1.1) y se aplicará al tratamiento total o parcialmente automatizado y al no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero (art. 3.1).

Al tratarse de una Directiva Europea precisaba de una ley de carácter nacional para la transposición de los principios y obligaciones contenidos en la

[173]En el Convenio se definen términos como «datos de carácter personal», «fichero automatizado», tratamiento automatizado y autoridad controladora del fichero

misma [174]. La Directiva 95/46/CE establecía que debía aplicarse el derecho nacional de algún Estado miembro cuando el tratamiento se llevase a cabo en el establecimiento de un responsable situado en la Unión Europea. También era de aplicación esta Directiva al tratamiento de datos personales cuando el responsable no estuviera establecido en algún país de la Unión, pero se le aplicaba la legislación nacional de un Estado miembro debido al Derecho internacional público. Igualmente se aplicaba aun cuando el responsable del tratamiento no estuviese establecido en territorio de la Unión siempre que recurriese a medios para llevar a cabo tratamientos de datos localizados en el territorio de un Estado miembro, salvo que fueran utilizados solamente con fines de tránsito (art. 4).

El consentimiento debía ser informado y anterior al inicio del tratamiento se tenían que señalar qué datos se tratarían, sus finalidades, la identidad del responsable, y los derechos de los interesados (art. 7. a y art. 10). El consentimiento podía ser retirado cuando la persona afectada lo estimara oportuno, sin embargo, se requería la manifestación explícita del mismo cuando se trataran datos de alguna de las categorías especiales, en esta Directiva, se incluían las previstas en el Convenio 108 y además se incluían a este tipo de categorías los datos que revelarán el origen étnico, las convicciones filosóficas, y la pertenencia a sindicatos (art. 8.1).

En esta Directiva se completan los principios básicos para la protección de datos establecidos en el Convenio 108, en cuyo caso dichos principios siempre debían ser aplicables a cualquier información relativa a persona identificada o identificable, ya sea en el tratamiento automatizado de datos o en su tratamiento analógico; así pues, los datos debían ser recogidos de manera lícita, con fines determinados, explícitos y legítimos, adecuados, pertinentes, no excesivos en relación con los fines para los cuales fueron recogidos, exactos y conservados solo durante el tiempo no superior al necesario (art. 6). Con esta Directiva se instauran

[174] De conformidad con lo establecido en el art. 288 (antiguo artículo 249 TCE) de la Versión consolidada del Tratado de Funcionamiento de la Unión Europea, el cual dicta a tenor literal que: «*La directiva obligará al Estado destinatario en cuanto al resultado que deba conseguirse, dejando, sin embargo, a las autoridades nacionales la elección de la forma y de los medios*». También se menciona este método para introducir a las legislaciones nacionales el contenido de la Directiva 95/46/CE, lo establecido en su considerando 69 y su relación con el art. 4 de la Directiva.

los derechos de acceso, rectificación, cancelación y oposición, que podían ser ejercidos por el interesado (art. 12 y 14).

Los flujos transfronterizos de información y de datos dentro de la UE son necesarios para el desarrollo del comercio internacional. Estos estaban contemplados y permitidos en la Directiva 95/46/CE, siempre y cuando dichos flujos fuesen respetuosos con los principios contemplados en la misma. En el caso de la transferencia de datos personales se llevase a cabo a terceros países, éstos debían garantizar un nivel de protección adecuado, de lo contrario debía prohibirse la transferencia de los mismos, sin embargo, en el caso de que se verificase que efectivamente se cumpliese con un adecuado nivel de protección, ya sea por su legislación interna o por los compromisos internacionales que hayan suscrito a tales efectos, se podían realizar transferencias a dichos países sin ningún requisito adicional, sin perjuicio de lo que establecieran las legislaciones nacionales de los países miembros.

Con la transposición de la Directiva 95/46/CE, los países miembros debían crear una autoridad de control, cuya función principal era la de vigilar la aplicación en su territorio de las disposiciones en materia de protección de datos. De acuerdo con esta Directiva también los países miembros debían establecer un recurso administrativo y un recurso judicial, a fin de que se garantizaran las disposiciones del derecho nacional en el tratamiento de datos. Así pues, se establecía que toda persona que sufriera algún perjuicio por el tratamiento de sus datos podía solicitar la reparación del daño o perjuicio sufrido al responsable del tratamiento. Cada país miembro debía establecer sus sanciones con motivo del incumplimiento de las disposiciones adoptadas en ejecución de la Directiva 95/46/CE. La referida Directiva creó el Grupo de Trabajo del art.29 (*Article 29 Data Protection Working Party*-GT29-) con carácter consultivo e independiente para la protección de datos y derecho a la intimidad. Las funciones de este grupo entre otras eran las de estudiar todas las cuestiones relativas a la aplicación de las disposiciones adoptadas por los Estados miembros a fin de que su aplicación fuese homogénea, emitir dictámenes destinados a la Comisión sobre el nivel de protección dentro de la Comunidad y en los países terceros, asesorar a la Comisión sobre cualquier proyecto de modificación

de la Directiva 95/46/CE y, emitir dictámenes sobre los códigos de conducta elaborados a escala comunitaria [175].

Posteriormente este derecho también se incluye en el art. 8 de CDFUE [176], proclamada en Niza el mes de diciembre del año 2000 por el Parlamento Europeo, el Consejo y la Comisión, y publicada el 18 de diciembre de 2000 en el Diario Oficial de la Unión Europea. Esta reafirma de manera general los derechos contenidos en las diversas constituciones de los Estados miembros en un instrumento que les es aplicable a todos ellos. Como no puede ser de otra manera, también reafirma el contenido del CEDH, el de la Carta social europea del Consejo y los principios emanados por la Jurisprudencia del Tribunal de Justicia de las Comunidades Europeas [177]. Con la entrada en vigor del Tratado de Lisboa, esta adquiere el mismo carácter jurídico vinculante que los Tratados (el Tratado de la Unión Europea -TUE- y el Tratado del Funcionamiento de la Unión Europea-TFUE-). Incluso el art. 16 del Tratado del Funcionamiento de la Unión Europea determina el derecho de toda persona a la protección de datos de carácter personal.

Después de la Directiva 95/46/CE se aprueban otras que tienen relación con distintos aspectos del tratamiento de datos personales, una de ellas fue la hoy derogada 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, que posteriormente fue sustituida por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre privacidad y las comunicaciones electrónicas), la cual se encarga de armonizar en los Estados miembros de la UE, en el sector de las comunicaciones electrónicas, la protección de las libertades y de los derechos fundamentales y, en particular, del

[175] Las funciones se encuentran detalladas en el art. 30 de la Directiva 95/46/CE.
[176] Art. 8: *«1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».*
[177] Con la entrada en vigor en España del Tratado de Lisboa en 2009 cambia su denominación a la de Tribunal de Justica de la Unión Europea (TJUE).

derecho a la intimidad y del derecho a la protección de datos personales. Como su nombre indica, el sector de las comunicaciones electrónicas es marco del intercambio de datos, por lo que se trata de dar cabida a una mejor y eficaz protección de los datos personales y de la intimidad, principalmente en Internet.

Con posterioridad se aprobarán otras Directivas encargadas de regular algunos aspectos relativos a la Protección de Datos de Carácter Personal como la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, cuyo objeto era garantizar que los datos estuviesen disponibles con fines de investigación, detección y enjuiciamiento de delitos graves, definidos así por los Estados miembros [178]. Esta dejó de tener validez desde el 8 de abril de 2014, por Sentencia del Tribunal de Justicia de la Unión de esa misma fecha, asuntos acumulados C-293/12 y C-594/12 [179]; en la que señala que la misma no garantizaba un nivel óptimo de protección del contenido de los derechos establecidos en los arts. 7 y 8 de la CDFUE (privacidad y protección de datos), ya que por una parte se aplicaba de manera general a todos los usuarios abonados de los servicios de comunicaciones electrónicas en la Unión Europea, sin que hubiese un indicio de haber cometido un delito grave, y por otra parte, no fijaba ningún criterio objetivo *para delimitar el acceso de las autoridades nacionales competentes a los datos y utilización posterior con fines de prevención, detección o enjuiciamiento de delitos que, debido a su magnitud y la gravedad de la injerencia en los derechos fundamentales reconocidos en los artículos 7 y 8 de la carta* [180], remitiéndose así a la legislación de cada país miembro, tampoco establecía un procedimiento específico, se remitía a las legislaciones nacionales de los Estados miembros. En cuanto a las categorías de datos, esta Directiva establecía un plazo de conservación mínimo de 6 meses (art. 6)

[178] Art. 1.1 de la Directiva 2006/24/CE, del Parlamento Europeo y del Consejo, de 15 de marzo.
[179] STJUE de 8 de abril de 2014, Digital Rights Ireland Ltd (asunto C-293/12) y Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síovhána, Irlanda, The Attorney General, con intervención de Irish Human Rights Commission y Kärntner Landesregierung (asunto C-594/12), Michael Seitlinger, Christof Tschohl y otros (TJCE\2014\104; ECLI:EU:C:2014:238).
[180] Numeral 60, *íd.*

para todas las categorías de datos del art. 5 de la misma Directiva sin ninguna distinción, lo cual resultaba excesivo pues no tomaba en cuenta «su posible utilidad para el objetivo perseguido» [181] o a las personas afectadas. Finalmente, no tenía criterios objetivos para el lapso temporal de conservación de los datos, ni medios para comprobar su efectiva destrucción después del periodo de conservación [182].

En relación con la conservación de datos para la investigación en el año 2008, el Consejo de la Unión Europea adoptó la Decisión Marco 2008/977/JAI , de 27 de noviembre, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, la cual se aplicaba únicamente a los datos recogidos o tratados por las autoridades competentes para la prevención, investigación, detección o el enjuiciamiento de infracciones penales y la ejecución de sanciones de esta naturalez [183]. Sin embargo, esta decisión marco fue sustituida años más tarde por 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo [184]. Esta Directiva debió de ser transpuesta a nuestro sistema jurídico antes del 6 de mayo de 2018, sin embargo, a falta de una ley específica en la materia, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) en su D.T. 3ª ha determinado que los tratamientos de datos sometidos a la Directiva antes aludida deberán continuar rigiéndose por la LOPD de 1999, específicamente por el contenido de su art. 22, hasta que no entre en vigor una norma que la transponga. El art. 22 de la LOPD en sus primeros dos apartados hace una clara diferenciación del alcance de la norma en relación con los distintos tipos de ficheros según su finalidad creados por las Fuerzas y Cuerpos de Seguridad: 1) para fines administrativos y, 2) para fines

[181] Apartado 63.
[182] Cfr. Numeral 50 y ss., *íd.*
[183] Considerando 6 de la Decisión marco 2008/977/ JAI del Consejo, de 27 de noviembre de 2008.
[184] En el RGPD se prevé como una limitación a los derechos de los interesados contenidos en este instrumento jurídico, siempre y cuando «*respete en lo esencial los derechos y libertades fundamentales*» contenidos en la CDFUE, conforme a lo previsto en el art. 23.1.d).

policiales. El primero de ellos estaba sujeto al régimen general vigente, por tanto, estará sometido en la actualidad a la LOPDGDD y al RGPD. Los segundos al régimen específico, es decir, quedarán sometidos al contenido del art. 22 de la LOPD, en tanto no haya norma de transposición.

Otro instrumento que también regulaba a nivel europeo la protección de datos personales era el Reglamento (CE) núm. 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y organismos comunitarios y a la libre circulación de estos, sin embargo, este se vio desplazado por el contenido del Reglamento 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento nº45/2001 y la Decisión 1247/2002/CE, publicada en Diario Oficial de la Unión Europea el día 21 de noviembre de 2018.

2. MARCO CONCEPTUAL DE LA NORMATIVA VIGENTE.

El 25 de enero de 2012, la Comisión Europea, presenta al Parlamento Europeo la Propuesta de Reglamento [185], relativo a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de protección de Datos -RGPD-). De conformidad con la exposición de motivos, al tiempo de presentación de esta iniciativa se estimaba que lo establecido en la Directiva 95/46/CE, aun resultaba adecuado, sin embargo, no se había evitado con ella *«la fragmentación de cómo se aplica en la Unión la protección de datos de carácter personal, la inseguridad jurídica y la percepción generalizada de la opinión pública de que existen riesgos significativos, especialmente por lo que se refiere a la actividad en línea»* [186]. Por el año de gestación y publicación se puede inferir que se trataba de derecho derivado parco en relación con los avances tecnológicos, específicamente los desarrollados a partir de la web y posteriormente

[185] Cfr. Comisión Europea 2012. Disponible en http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf (consulta: 15 de junio de 2017).
[186] Exposición de motivos de la propuesta del RGPD, p. 2.

la tecnología móvil, teniendo en cuenta que en todas estas se realiza un tratamiento ingente de datos personales. Por todo ello la Comisión estimó que había llegado el momento de establecer un marco más sólido y coherente en la materia dentro de la UE, con una aplicación estricta que permitiese el desarrollo de la economía digital en el mercado interior, otorgase a los ciudadanos el control de sus propios datos y reforzara la seguridad jurídica y práctica de los operadores económicos y las autoridades públicas [187]. La propuesta surge como resultado de una amplia consulta [188] sobre la revisión del marco jurídico para la protección de datos de carácter personal, donde la gran mayoría de los participantes estaban de acuerdo en que los principios seguían siendo válidos pero era necesario *« adaptar el marco vigente para responder mejor a los retos que plantea el rápido desarrollo de las tecnologías (especialmente en línea) y la globalización creciente, al tiempo que se mantiene la neutralidad tecnológica del marco jurídico. La actual fragmentación de la protección de datos personales en la Unión ha sido blanco de duras críticas, especialmente por parte de los operadores económicos, que solicitaron una mayor seguridad jurídica y la armonización de las normas relativas a la protección de los datos de carácter personal. Se considera que la complejidad de las normas en materia de transferencias internacionales de datos personales constituye un impedimento sustancial a su funcionamiento, ya que se necesita transferir con regularidad datos personales de la UE a otras partes del mundo»* [189]. Debido a su falta de homogenización y fragmentación en la aplicación de la regulación en materia de protección de datos, se considera que el Reglamento es el instrumento jurídico más apropiado para definir el marco de protección de datos personales en la Unión, y así lo argumentaba la Comisión: *«La aplicabilidad directa de un reglamento, de conformidad con el artículo 288 del TFUE, reducirá la fragmentación jurídica y ofrecerá una mayor seguridad jurídica merced a la introducción de un conjunto armonizado de normas básicas, la mejora de la protección de los derechos*

[187] *Íd.*
[188] El procedimiento de todas las consultas realizadas a diversas instituciones de la Unión se detalla en la exposición de motivos, en su apartado dos, de la propuesta de RGPD, p. 3.
[189] Exposición de motivos de la propuesta del RGPD, p. 4.

fundamentales de las personas y la contribución al funcionamiento del mercado interior» [190]*.*

El Reglamento (EU) 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 (Reglamento general de protección de datos-RGPD-). Supone un cambio en el modelo europeo de protección de datos es de gran envergadura, por una parte, como establece el art. 288 del TFUE, este instrumento tiene alcance general dentro de la Unión y es «*obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro»,* lo cual, implica que su aplicación sea homogénea en toda la UE garantizándose así un elevado nivel de protección respetando de manera igualitaria el derecho a la protección de datos personales, pero también con arreglo al principio de proporcionalidad, considerando también otros derechos fundamentales contenidos en la CDFUE como el respeto de la vida privada y familiar, del domicilio y las comunicaciones, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística y, el respeto a la vida [191]. El RGPD también faculta a los Estados miembros para «*mantener o adoptar disposiciones nacionales a fin de especificar en mayor grado la aplicación de las normas del presente Reglamento»* [192]*.*

Como se mencionó anteriormente la actualización del marco normativo europeo en materia de protección de datos también se debe a los cambios tecnológicos y a la globalización. La tecnología global por excelencia es la web, por medio de esta se realizan gigantescas transmisiones de datos a cada segundo, la necesidad de regular estas transferencias a países no comunitarios no es nada baladí, es por ello que se incluyen en este RGPD del art. 44 al 50 una serie de criterios a fin de asegurar que el nivel de protección de las personas físicas no se vea menoscabado [193]; lo cual podrá realizarse mediante un acto de ejecución previa de

[190] Exposición de motivos de la propuesta del RGPD, p. 6.
[191] Considerando 4 del RGPD.
[192] Considerando 10 del RGPD.
[193] Art. 44 *in fine* del RGPD.

evaluación de la adecuación del nivel de protección realizada por la Comisión[194], la prestación de garantías adecuadas[195] ,o por normas corporativas vinculantes[196] las cuales asegurarán el nivel de protección incluso a las transferencias ulteriores de datos personales entre responsables y encargados desde el tercer país u organización internacional a otro tercer país u organización internacional[197]. En cuanto a los acuerdos celebrados con anterioridad a la aplicación del RGPD, cuyo fundamento sea el art. 25 de la Directiva 95/46/CE, estos seguirán vigentes hasta que en su caso sean modificados, sustituidos o derogados por una decisión de la Comisión y estarán sujetos a su supervisión y revisión periódica por lo menos cada cuatro años[198]. Por ejemplo, la Decisión de ejecución 2016/1250 de la Comisión de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de privacidad UE-EE.UU, la cual fue publicada en el DOUE el 1 de agosto de 2016[199], meses después de que haya entrado en vigor el RGPD.

---

[194] Conforme a lo establecido en el art 45 del RGPD, teniendo en cuenta: «*a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial(…);b)la existencia y funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional(…); 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 su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales*».

[195] En caso de que no hubiese una decisión se podrán prestar las garantías establecidas en el art. 46 para que se puedan realizar este tipo de transferencias a países terceros.

[196] Conforme a lo establecido con el art. 47, en relación con el contenido del art 63 del RGPD.

[197] Para un estudio en mayor profundidad *vid.* PIÑAR MAÑAS, J. L., «XXV. Transferencias de datos personales a terceros países u organizaciones internacionales», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad,* Reus, Madrid, 2016, pp. 427-460.

[198] Apartados 3, 4, 5 y 9 del art. 45 del RGPD.

[199] Esta Decisión de la Comisión se realizó de manera posterior a que la STJUE de 6 de octubre de 2015(TJCE 2015\324; ECLI:EU:C:2015:650), declarará invalida la Decisión de la Comisión 2000/520/CE, pues entre otras cosas, no se garantizaba la protección de los derechos contenidos en los arts. 7 y 8 de la CDFUE, establece numeral 73 de esta sentencia que el término de «adecuado» que se establecía en la Directiva 95/46/CE en su art. 25.6 «*significa que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión (…) debe entenderse la expresión «nivel de protección adecuado» en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta*», además del hecho de que la Decisión 2000/520 reconocía «*la primacía de las "exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]" sobre los principios de puerto seguro, primacía en virtud de la cual las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión*

El art. 2.3 del RGPD establece que el entonces Reglamento 45/2001, del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, y demás actos jurídicos de la Unión aplicables a ese ámbito de aplicación debía adaptar sus principios y normas al contenido del RGPD al art. 98, en el cual se contempla la revisión de otros actos jurídicos de la Unión en materia de protección de datos, llevado a cabo por la Comisión. Como se ha referido anteriormente El Reglamento 45/2001 ha sido sustituido recientemente por el Reglamento 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y organismo de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento 45/2001 y la Decisión nº1247/2002/CE. El cual a diferencia que Reglamento 45/2001, protege los datos personales tratados por las instituciones, órganos y organismos de la Unión en cualquier contexto total o parcialmente automatizado, así como al tratamiento no automatizado contenidos y destinados a ser incluidos en un fichero [200].

Siguiendo con lo establecido en el RGPD, este se aplicará al tratamiento total, parcial y no automatizado de datos personales (art. 2.1); en cuanto a su aplicación territorial, se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento o del encargado en la Unión, independientemente que tengan lugar en la Unión o no, cuando se traten datos de los interesados que se encuentren en la UE siempre que el tratamiento esté relacionado con la prestación u oferta de algún bien o servicio, o con motivo del control del comportamiento de los usuarios (art. 3).

Se introducen nuevos términos que ayudan a entender este nuevo modelo de protección de datos, que no estaban contemplados en la Directiva anterior, como seudonimización, elaboración de perfiles, datos genéticos, datos biométricos, datos relativos a la salud, grupo empresarial, normas corporativas vinculantes,

están obligadas sin limitación a dejar de aplicar esos principios cuando éstos entren en conflicto con esas exigencias y se manifiesten por tanto incompatibles con ellas» (*vid.* numeral 86 de la citada sentencia).

[200] Cfr. Considerando 6 y 8 del Reglamento 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre, y conforme a lo establecido en el art. 2 del mismo.

tratamiento trasfronterizo, objeción pertinente y motivada u organización internacional (art. 4). Además de lo anterior, se introducen modificaciones sustanciales que mejoran el nivel de protección de datos, como el principio de transparencia (art. 5.1 y 12), el principio de minimización de datos (art. 5.c), los de integridad y confidencialidad (art. 5.f), la responsabilidad proactiva del responsable del tratamiento (art. 5.2) traducida en la obligación de cumplir los principios relativos al tratamiento y ser capaz de demostrarlo, lo que supone que estos principios «*están constituidos por un conjunto de reglas que determinan cómo se deben recoger, tratar y ceder los datos de carácter personal, a los efectos de garantizar la intimidad y demás derechos fundamentales de los titulares de los datos*»[201].

En cuanto al consentimiento, este deberá ser explícito, libre, específico, informado e inequívoco (art. 4.11) el cual puede manifestarse por escrito, por medios electrónicos, incluso por medio de una declaración oral siempre que conste de manera clara su sentido positivo para cada uno de los tratamientos de datos[202], pudiéndose retirar en cualquier momento, sin que este afecte la licitud previa a su retirada[203]. El consentimiento forma parte de una de las seis condiciones para que el tratamiento resulte lícito (art. 6.1.a). El RGPD también prevé condiciones especiales al consentimiento de menores en relación con los servicios de la sociedad de la información, el cual resultará lícito cuando se ha concedido por un menor cuya edad mínima sea de 16 años, contrariamente se requerirá la autorización del titular de la patria potestad o tutela del menor, sin embargo, se da la potestad a los Estados miembros a que señalen una edad inferior, cuyo límite estará en los 13 años[204].

En fin, se realizan otras modificaciones sustanciales como la introducción del Derecho de supresión («el derecho al olvido») contenido en el art. 17, y del que hablaremos posteriormente; se introduce también el derecho de portabilidad (art. 20); la obligación de adoptarse medidas técnicas y organizativas desde el diseño y por defecto (art. 25); la figura del corresponsable del tratamiento en caso de que dos o más responsables determinen los objetivos y medios del tratamiento (art. 26); la

[201] PUYOL MONTERO, J., «IX. Los principios del Derecho a la protección de datos», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad,* Reus, 2016, p. 135.
[202] Considerando 32 del RGPD.
[203] Art. 7.3 del RGPD.
[204] Art. 8 del RGPD.

obligación del registro de actividades del responsable y en su caso, su representante, siempre y cuando la empresa u organización no emplee a más de 250 trabajadores, siempre que el tratamiento no suponga riesgo para los derechos y libertades de los interesados, no sea ocasional o que incluya categorías especiales (art. 30); la introducción de la figura del Delegado de protección de datos, el cual deberá ser designado por responsables y encargados (art. 37); la previsión de creación de códigos de conducta (art. 40) y certificaciones (arts. 42-43); un marco más sólido para la transferencias de datos a terceros países u organizaciones internacionales e incluso cuando estas sean ulteriores a una transferencia previa, basadas en decisiones de adecuación tomadas por la Comisión, mediante la provisión de garantías adecuadas o bien la sujeción a normas corporativas vinculantes (arts. 44-50); la creación del Comité Europeo de Protección de Datos (CEPD) el cual viene a sustituir al Grupo de trabajo del art. 29 previsto en la normativa anterior (art. 68)[205]; el derecho a la tutela judicial efectiva en contra de una autoridad de control y en contra de un responsable (arts. 78 y 79), así como un derecho de indemnización y responsabilidad frente al responsable y al encargado, como consecuencia de una infracción al RGPD (art. 82). Estos cambios descritos de manera enunciativa y escueta merecen un estudio individualizado de cada uno de ellos[206].

[205] De acuerdo con lo establecido por NEIRA BARRAL «*es uno de los pilares sobre los que se asienta el nuevo marco legal de protección de datos en la Unión Europea y esto es así porque se le confiere algunas funciones que ya tenía atribuida el Grupo de Trabajo del artículo 29 de la Derogada Directiva 95/46/CE*», Cfr. NEIRA BARRAL, D., «Autoridades de control en el nuevo Reglamento General de Protección de Datos 2016/679 y la Ley Orgánica 3/2018», CAMPOS ACUÑA, C. (Dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local,* Segunda edición, Wolters Kluwer, 2019, p. 688.

[206] Para un estudio más pormenorizado *vid.* PIÑAR MAÑAS, J. L. (Dir), *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad,* Reus, 2016; *Derechos humanos y nuevas tecnologías. XXI Cursos de verano en San Sebastián. XIV Cursos Europeos- UPV/EHU 2002*, Ararteko, 2003, D.L. VI-73/2003; APARICIO VAQUERO, J. P., «La protección de datos que viene: el nuevo Reglamento General europeo», *Ars Iuris Salamanticensis. Tribuna actualidad.* Vol. 4, diciembre 2016, 27-34; BIURRUN ABAD, F.J., «"Accountability" o responsabilidad activa en el Reglamento General de Protección de Datos», *Actualidad jurídica,* Aranzadi, núm. 927/2017 (BIB 2017\732); BOTANA, G.A., Crónica anunciada de un Reglamento de Protección de Datos en la Unión Europea, *Actualidad civil,* Wolters Kluwer, nº 6, 1 de junio de 2016; FERNÁNDEZ DE MARCOS, E., «La evaluación de impacto en protección de datos: aspectos de interés», *Actualidad Administrativa,* Wolters Kluwer, nº 4, marzo, 2018; DÍAZ DÍAZ, E., «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones», *Revista Aranzadi Doctrinal,* nº 6 (parte Estudio), 2016; DOPAZO FRAGUÍO, P., «La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente (Novedades del Reglamento General de Protección de Datos», *Revista Española de Derecho Europeo,* nº 68 (parte Estudios), 2018; DURÁN CARDO, B., *La figura del responsable en el Derecho a la Protección de datos.* Wolters Kluwer España, Madrid, 2016; entre otros.

El 12 de marzo de 2019[207] el Parlamento Europeo *dio su aprobación a la ratificación por parte de los Estados miembros, en interés de la Unión Europea* del Protocolo modificativo del Convenio 108 por parte de los Estados miembros [208]. Este adapta el Convenio 108 a las disposiciones en materia de protección de datos a los establecido en Reglamento 679/2016, 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 (RGPD) del cual de manera posterior se hablará en este epígrafe. También las modificaciones al Convenio 108 por este último protocolo son compatibles con lo establecido en 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 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.[209]

La modernización de este Convenio supone el flujo de datos personales seguro con un alto grado protección tanto entre los países de la Unión como con los extraeuropeos y quizás lo más importante sea la internacionalización de los principios y el nivel de protección del derecho a la protección de datos personales fuera de sus fronteras. El objeto del Convenio 108+, es proteger a toda persona, cualquiera que sea su nacionalidad o residencia, en lo que respecta al tratamiento de sus datos personales, contribuyendo al respeto de sus derechos humanos y de

[207] Cfr. Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2019, sobre la propuesta de Decisión de Consejo por la que se autoriza a los Estados miembros a firmar, en interés de la Unión Europea, el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal [10923/2018 – C8-0440/2018 – 2018/0238(NLE)]. http://www.europarl.europa.eu/doceo/document/TA-8-2019-0142_ES.html (consulta: 24 de septiembre de 2019).

[208] Cfr. Propuesta de Decisión del Consejo por la que se autoriza a los Estados miembros a ratificar, en interés de la Unión Europea, el Protocolo que modifica el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CONSIL:ST_7772_2019_INIT&from=EN (consulta: 24 de septiembre de 2019).

[209] *Vid.* Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Disponible en: https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32016L0680 (consulta: 24 de septiembre de 2019).

sus libertades fundamentales, y en particular del derecho a la privacidad (art. 1), dicho Convenio será aplicado tanto al sector público como al sector privado, y excluye de su aplicación al uso con fines domésticos o personales de los datos (art. 3).

Los cambios en las legislaciones de los Estados que se adapten al Convenio deberán efectuarse antes de la ratificación o adhesión al mismo, y será el Comité de la Convención quien se encargue de vigilar su plena adaptación al mismo. Se añade el principio de transparencia en el tratamiento de los datos personales (art. 8). En el art. 6 ahora no solo están previstos los datos que revelen las creencias religiosas, de origen racial, las opiniones políticas, los relativos a la salud o a la vida sexual, como categorías especiales de datos, con la modificación, también se incluyen los relativos a la comisión de delitos, procedimientos penales y condenas, los datos biométricos y los datos genéticos dentro de esta categoría de datos (art. 6), estableciendo que en su tratamiento se deberán guardar la debida seguridad para asegurar salvaguardarlos. Se prevé también la gratuidad de las solicitudes de rectificación o supresión, y que los interesados cuenten con un medio para defender sus derechos si estos han sido violados (art. 9). También se prevé que los encargados de tratamiento o en su caso los responsables, realicen una evaluación de impacto antes del inicio del tratamiento de datos personales (art. 10). En cuanto a los flujos transfronterizos de datos personales entre Estados parte se realizará de manera libre y no se le requerirán requisitos adicionales y solo se realizará transferencia de datos a un Estado u organización que no sea parte siempre que se garantice un nivel adecuado de protección en materia de protección de datos (art. 14). Se añade el art. 17 el cual regula las formas de cooperación entre las autoridades de supervisión. La asistencia que deberá proporcionar cada Estado parte a los interesados se realizará sin importar su nacionalidad o residencia, a fin de que puedan ejercer los derechos contenidos en el art. 9 de dicho convenio. Quizás uno de los cambios más relevantes que ha supuesto este Convenio 108+, es la posibilidad que ofrece a las organizaciones internacionales de adherirse al mismo, de conformidad con lo establecido en su art. 27.

A nivel nacional, el art. 18.4 de la CE establece que «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», sin embargo, debido a su redacción, solían haber ciertas confusiones del alcance y de la independencia del este derecho. En un primer momento, tanto Doctrina como Jurisprudencia tenían dudas sobre su carácter de fundamental y autónomo, e incluso se generó polémica respecto a su inclusión en la Constitución por parte del Constituyente[210]. Se han acuñado diversos conceptos alrededor de este derecho como «libertad informática» [211], «autodeterminación informativa» [212], o referirse a este simplemente como «protección de datos».

---

[210] El anteproyecto de la Constitución Española publicado en el Boletín Oficial de las Cortes el día 5 de enero de 1978, contemplaba de manera casi idéntica el derecho a la protección de datos de la siguiente manera *«La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos»*, sin embargo es gracias a la Minoría Catalana la incorporación los límites de la informática: *«el pleno ejercicio de los derechos por parte de los ciudadanos»* en el texto constitucional vigente (DSCD, Comisión de Asuntos Constitucionales y libertades públicas, nº 7, de 19/05/1978, pp. 2526-2590). Es importante mencionar, que la Constitución Española fue la segunda (después de Portugal en 1974, art. 35 *Utilização da informática*) a nivel europeo en incorporar a su Constitución el derecho fundamental a la protección de datos de carácter personal limitando así el uso de la informática.

[211] Como se cita en la obra *La nueva generación de derechos humanos* de RODRÍGUEZ PALOP sobre el concepto de libertad informática de FROSINI, el cual consiste en *«el derecho de poner disponer de los datos de información personal propios, y por tanto, permitir o rehusar, su uso por parte de las agencias de información que manejan los bancos de datos; derecho a controlar la veracidad de los datos, acceso a su conocimiento por parte de terceros, el uso que de ellos se hiciere con finalidades sociales, económicas y políticas. La libertad informativa (…) representa una nueva forma de desarrollo de la libertad personal; no consiste únicamente en la libertad negativa del right to privacy, de custodiar celosamente una visa reservada (…) consiste también en la libertad de informarse, de ejercer un control autónomo sobre la propia identidad informática»* en RODRÍGUEZ PALOP, M.A., *La nueva generación de Derechos Humanos.,* Ed. Dykinson, Madrid, 2002, p. 57 (nota a pie 90). Por su parte, el Tribunal Constitucional por Sentencia 254/1993, de 20 de Julio (RTC 1993\254; ECLI:ES:TC:1993:254) en el Fundamento Jurídico 7, nos estableció por primera vez una definición en la jurisprudencia española de este término: *«la llamada "libertad informática" es, así, también, derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)»* para este efecto también se pueden consultar las siguientes sentencias STC 94/1998, de 4 de mayo (RTC 1998\94; ECLI:ES:TC:1998:94) y STC 202/1999, de 8 de noviembre (RTC 1999\202; ECLI:ES:TC:1999:202).

[212] Tal y como se establece PÉREZ LUÑO en LOSANO, M., PÉREZ LUÑO, A. Y GUERRERO MATEUS, M., *Libertad Informática y Leyes de Protección de Datos Personales,* Centro de Estudios Políticos y Constitucionales, Bilbao, 1989, p. 140: *«La doctrina y la jurisprudencia germanas han elaborado una categoría paralela a la libertad informática denominada "derecho a la autodeterminación informativa" (Recht auf informationelle Selbstbestimmum). Según las tesis del Tribunal Constitucional (Bunderverfassungsgericht) de Karlsruhe, en su célebre sentencia de 15 de diciembre de 1983 sobre la ley del censo de población (Volkszählungsgesetz), el principio básico del ordenamiento jurídico establecido en la ley Fundamental (Grundgesetz) de la República Federal de Alemania es el valor y la dignidad de la persona, que actúa con libre determinación al formar parte de una sociedad libre. De la dignidad y de la libertad, entendida como libre autodeterminación, deriva la facultad de la persona de "deducir básicamente por sí misma cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida"»*. Esta sentencia, parte de los derechos de la dignidad humana y del derecho general de la personalidad, ambos protegidos por la Ley Fundamental de Bonn, el problema se plantea cuando en la Ley del Censo de 1983, en sus artículos 1, 2, 3, 4, 5, 7 y 9 principalmente,

Poco a poco este derecho fue perfilado por diversas sentencias del TC, en un primer momento se determinó que «*nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona, de forma en último término no muy diferente a como fueron originándose e incorporándose históricamente los distintos derechos fundamentales*» [213]. Posteriormente se le reconoce como un derecho fundamental autónomo, de la siguiente forma: «*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 desarrollado el derecho fundamental a la protección de datos (art. 81.1 CE), bien regulando su ejercicio (53.1 CE). La peculiaridad de este 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»*[214], y también aclara que debe entenderse como dato de carácter personal no solo a aquellos *«relativos a la*

---

contenían la obligación a los particulares de dar sus datos personales como nombre, apellidos, dirección, número de teléfono, estado familiar, pertenencia o no a una asociación religiosa, nacionalidad, etc., supuestamente para fines estadísticos, pero sin las garantías suficientes de que estos serían transferidos a otras autoridades, pues la propia ley legitimaba el tráfico de datos justificándolos en la mejor planeación económica y social que proporcionaban los mismos, por lo tanto se determina en el apartado C II *«la facultad del individuo, derivada de la idea de autodeterminación, de decidir básicamente por sí mismo cuándo y dentro de qué límites procede revelar situaciones referentes a la propia vida […] esta facultad requiere en las condiciones actuales y futuras de la elaboración automática de datos una medida especial de protección[…]la autodeterminación del individuo presupone- también en las condiciones de las técnicas modernas de tratamiento de la información- que se conceda al individuo la libertad de decisión sobre las acciones que vaya a realizar o, en su caso a omitir, incluyendo la positividad de obrar de hecho en forma consecuente con la decisión adoptada»*, de lo anterior se deduce que se toma en cuenta ya en esa época, el riesgo que supone el almacenamiento y la transmisión de los datos personales por medios automatizados haciendo uso de la informática y que la posible transmisión de datos para los fines que fueron recogidos es una infracción dentro del sistema jurídico alemán a la autodeterminación informativa. Facultad de Derecho, Universidad de Chile Disponible en: https://www.u-cursos.cl/derecho/2008/0/DIPDERINFO/1/material_docente/bajar?id_material=163485 (consulta: 15 de junio de 2017) y para la consulta de la versión original en OpenJur, BVerfG, Urteil vom, 15 de diciembre de 1983. Disponible en: https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/1983/12/rs19831215_1bvr020983.html (consulta: 15 de junio de 2017).

[213] STC (Primera Sala) 254/1993, de 20 de julio, F.J. 6 (RTC 1993\254; ECLI:ES:TC:1993:254).

[214] F.J.5 de la STC 292/2000, de 30 de noviembre, (RTC 2000\292; ECLI:ES:TC:2000:292).

vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo»[215]. Por tanto, el abanico de posibilidades se amplía, pudiendo ser su dirección IP, su email, su número telefónico, su orientación política, sus preferencias sexuales, sus antecedentes penales y hasta su perfil de ADN, entre otros.

De acuerdo con lo anterior se puede afirmar que el derecho a la protección de datos es un derecho fundamental que tienen todos los individuos, y que se traduce en el poder de controlar sus datos personales, su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad del afectado; es decir, otorga un poder de disposición de los datos de carácter personal. No solo se constriñe a los datos relativos a la intimidad de las personas, sino que abarca cualquier tipo de dato personal sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales y que hagan al individuo perfectamente identificable o que permitan su identificación. Por su parte, DÁVARA RODRÍGUEZ, establece que *«surge, de este modo, la expresión protección de datos entendida como la protección jurídica de las personas en lo que concierne al tratamiento automatizado de sus datos personales, o, expresado de forma extensa, el amparo debido a los ciudadanos contra la posible utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento automatizado, para confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad»*[216]. De este modo, sabemos que el derecho a la protección de datos personales forma parte de *«un importante criterio de legitimación política de los sistemas democráticos desarrollados»*[217], que desde mi perspectiva tiene una doble función, por una parte

[215] F.J. 6, *íd.*
[216] DÁVARA RODRÍGUEZ, M.A., *La protección de datos en Europa,* Ed. Asnef, Madrid, 1998, p. 17.
[217] En LOSANO, M., *et al.*, *op. cit.,* pp. 138-139: «*La protección de datos personales constituye, por tanto, un importante criterio de legitimación política de los sistemas democráticos desarrollados. Su reconocimiento supone una condición del funcionamiento del propio sistema democrático, es decir, se trata de una garantía básica para cualquier comunidad de ciudadanos libres e iguales. La protección*

se encarga de proteger los datos personales del individuo cuando estos son tratados o almacenados en sistemas automatizados que hacen uso de la informática para ello, y en una segunda concepción del mismo, este derecho puede ser instrumental para la protección de los derechos de la personalidad principalmente, así como el pleno ejercicio de los derechos de las personas.

El objeto de protección es cualquier dato personal que identifique a una persona o lo haga identificable, por lo que «*atribuye a su titular un haz de facultades consistente en diversos deberes jurídicos cuyo ejercicio impone a terceros deberes jurídicos, que no se contienen en el derecho fundamental a la intimidad, y que sirven a la capital función que desempeña este derecho fundamental: garantizar a las personas un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer. A saber: el derecho a que se requiera un previo consentimiento para la recogida y uso de los datos personales, el derecho a saber y ser informado sobre el destino y uso de esos datos y el derecho a acceder, rectificar y cancelar dichos datos. En definitiva, es el poder de disposición sobre los datos personales*»[218].

3. EVOLUCIÓN NORMATIVA EN ESPAÑA.

La primera Ley en España en desarrollar el contenido del art. 18.4 CE, fue la LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, la cual ya en ese entonces preveía «*El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos*»[219], su objeto era «*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*

de datos personales y las libertades en relación con el uso de la informática han pasado a formar parte del conjunto de derechos que, en opinión de Erhard Denninger, "definien el status constituens" del ciudadano, su posición jurídica de formar parte activa y constituyente del Estado».

[218] STC 292/2000, de 30 de noviembre, F.J. 6 (RTC 2000\292; ECLI:ES:TC:2000:292).

[219] Esta ley hace una mención especial al contenido diferenciado de la intimidad y la privacidad en su exposición de motivos, establece que los avances tecnológicos han «*expuesto a la privacidad (…) nótese que se habla de privacidad y no de intimidad. Aquélla es más amplia que ésta (…) la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un relato de la personalidad del individuo que éste tiene derecho a mantener reservado*», *vid.* Apartado 1 de la exposición de motivos de la LO 5/1992, de 29 de octubre.

personal y familiar de las personas físicas y el pleno ejercicio de sus derechos»[220]. Posteriormente, con motivo de la transposición de la Directiva 95/46/CE, y el desarrollo del propio art. 18.4 de la CE, se publica en el BOE de 14 de diciembre de 1999, la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, cuyo desarrollo reglamentario corría a cargo 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.

Esta LO tenía como finalidad garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas. Respecto al tratamiento de datos personales se regulaba el tratamiento de datos personales efectuado tanto en territorio español como en el extranjero, en este último caso era aplicable la LOPD en dos circunstancias, la primera, si el responsable no estuviese establecido en territorio español, se le aplicaba la ley en razón del Derecho Internacional Público, y en la segunda, si el responsable no estuviese establecido en territorio español pero realizara un tratamiento de datos utilizando medios situados en territorio español siempre que no fuesen con fines de tránsito[221].

En la LO 15/1999 también se contemplaban los derechos ARCO (por sus siglas), es decir, los derechos al Acceso, la Rectificación, la Cancelación y la Oposición a los afectados. Estos derechos estaban contemplados del art. 15 al 17 de esta ley. El derecho de acceso, se definía como aquel a *«obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos»* y a saber *«la finalidad del tratamiento»*[222]; el derecho de rectificación, se consideraba como aquel que tenían los interesados a que se modificaran sus datos «*inexactos o incompletos*»[223]; el derecho de cancelación, era aquel que tenían los titulares de los datos a que se eliminasen los mismos siempre que estos no se ajustasen a la

[220] Art. 1 de la LO 5/1992, de 29 de octubre. En concordancia con lo establecido en su exposición de motivos, pues con la misma se pretendía «*hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos*».
[221] La propia LOPD daba una serie de definiciones para mejorar el entendimiento de la normativa.
[222] Art.15.1 de la LO 15/1999, de 13 de diciembre y 27.1 del Real Decreto 1720/2007, de 21 de diciembre.
[223] Art. 16.1 de la LO 15/1999, de 13 de diciembre y 31.1 del Real Decreto 1720/2007, de 21 de diciembre.

normativa en la materia, y específicamente cuando resultasen inexactos o incompletos[224]; y finalmente el derecho de oposición, consistía en que el afectado podía oponerse al tratamiento de sus datos y que en su caso solicitar que cese el mismo[225]; que junto con el derecho de información[226], conformaban los derechos de esta LO.

Por otro lado, en la Ley también se contemplaba una serie de principios a cumplir en el tratamiento de datos personales, como los relativos a la calidad de los datos (art. 4 LO 15/1999) que debían cumplirse en la recogida de los mismos, durante y hasta la finalización del tratamiento. También se encontraba el principio de información, que consistía en la obligación de informar de modo expreso, preciso e inequívoco a los interesados en el momento en el que se recabase sus datos personales sobre la existencia de un fichero o tratamiento de datos de carácter personal, sobre la finalidad y los destinatarios de la información, sobre el carácter obligatorio o facultativo de las respuestas que se les plantea al recabar la información, sobre las consecuencias de la obtención de los datos o la negativa a suministrarlos, así como de la posibilidad de ejercitar sus derechos de acceso, rectificación, cancelación y oposición, y sobre la identidad y dirección del responsable del tratamiento o en su caso del representante[227]; el principio de consentimiento, como su propio nombre indica era aquel por el cual se requería que el tratamiento de los datos contase con el consentimiento del afectado de manera tácita y general, para el tratamiento de cierto tipo de datos se requería que fuese explicito[228]; y principio de seguridad de los datos, que exigía tratar los datos de manera diligente llevando a cabo medidas de índole técnica y organizativa necesarias para evitar la alteración, pérdida, tratamiento o acceso no autorizado por parte de terceros[229]. Junto con el cumplimiento de estos principios, los responsables

[224] Art.16.2 de la LO 15/1999 y art. 32.2 de su reglamento.
[225] Arts. 17.1 de la LO 15/1999 y 34 de su reglamento. Específicamente los supuestos para solicitar el cese de este se establecían en art. 34 a) a c) del reglamento.
[226] El derecho de información contemplado en el art. 13.3 de la ley 15/1999, de 13 de diciembre, consiste en que el afectado tiene *«derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto».*
[227] Art. 5 de la LO 15/1999, de 13 de diciembre.
[228] Del art. 6 al 8 de la LO 15/1999, de 13 de diciembre.
[229] Art. 9 de la LO 15/1999, de 13 de diciembre.

y los encargados del tratamiento, también tenían el deber de preservar los datos, su seguridad y el secreto profesional sobre los mismos.

La autoridad a nivel nacional en la materia continuó siendo la Agencia Española de Protección de Datos[230], un ente de derecho público con personalidad jurídica propia y plena capacidad pública y privada,[231] cuyo deber principal se traducía en actuar con plena independencia para asegurar la observancia de sus funciones, entre las que se encontraba velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación, en especial en lo relativo a los derechos de acceso, rectificación, cancelación y oposición (ARCO)[232], y ejercía conforme a esta LO como autoridad sancionadora, en caso de que se cometiese alguna de las infracciones por el responsable del tratamiento o en su caso por el encargado del mismo, en cualquiera de sus tres escalas de gravedad[233].

Hasta diciembre de 2018 el derecho a la protección de datos personales estaba desarrollado principalmente por la LO 15/1999, de 13 de diciembre[234] y su Reglamento[235], como consecuencia de la publicación del RGPD, se aprueba la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y garantía de los derechos digitales (LOPDGDD). La cual desarrolla el art. 18.4 CE, pero también según sus propios considerandos, esta LO se realiza para «*la depuración del ordenamiento nacional*», y más que incorporar el derecho de la Unión al nacional

[230] Sin embargo, durante la vigencia de esta ley se van creando autoridades autonómicas en la materia como la Agencia Vasca de Protección de Datos regulada por la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos; y la Autoridad Catalana de Protección de Datos regulada por la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.
[231] Art. 35.1 de la LO 15/1999, de 13 de diciembre. Su estatuto es anterior a la LO 15/1999, y está regulado por el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.
[232] Art. 37.1.a) de la LO 15/1999, de 13 de diciembre. Así también se encarga de llevar a cabo la instrucción de los procedimientos con motivo reclamaciones relacionadas con los Derechos ARCO.
[233] Este régimen de infracciones y sanciones estaba contemplado del art. 43 al 46 de la LO 15/1999, de 13 de diciembre.
[234] Existen otras Leyes y Reglamentos a nivel nacional que prevén aspectos relacionados con el Derecho a la protección de datos personales, por ejemplo, la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones y el Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios.
[235] 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.

esta LO desarrolla o complementa el Derecho de la UE. Su objeto conforme su art. 1 es «*Adaptar el ordenamiento jurídico español*» al RGPD, así como completar sus disposiciones, y «*Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el art. 18.4 de la Constitución*».

Esta nueva LO consta de noventa y siete artículos, veintidós disposiciones adicionales, seis disposiciones transitorias, una disposición derogatoria y dieciséis disposiciones finales [236]. Es importante señalar que la LOPDGDD tiene carácter orgánico, sin embargo, la disposición final primera de esta establece que tendrá carácter de ley ordinaria lo relativo al Título IV concerniente a disposiciones aplicables a tratamientos concretos; el Título VII relativo a las autoridades de protección con excepción del deber de colaboración de la AEPD y las Administraciones públicas, con inclusión de las tributarias y la Seguridad Social (SS) para llevar a cabo su actividad de investigación [237], así como su alcance de esa labor investigadora; el Título VIII referente a los procedimientos en caso de posible vulneración de la normativa de protección de datos ; también al régimen sancionador previsto en el Título IX; y finalmente lo relativo a los derechos en la era digital (art. 79), el derecho a la neutralidad en la red (art. 80), el derecho de acceso universal a Internet (art. 81), el derecho a la seguridad digital (art. 82), el derecho a la desconexión digital en el ámbito laboral (art. 88), el derecho de portabilidad de

[236] Es menester señalar que de acuerdo con el contenido de la D.A. 14ª y con la D.T. 4ª de la LOPDGDD en las que se contemplan la vigencia de las normas que desarrollan el art. 13 de la derogada Directiva 95/46/CE que establece la posibilidad de los Estados miembros de limitar las obligaciones y derechos relacionados con los principios de calidad de los datos (art. 6.1), la información proporcionada a los interesados (art. 10 y 11.1), el derecho de acceso (art. 12) y la publicidad de los tratamientos (art. 21), siempre y cuando fuese necesario para salvaguardar la seguridad y defensa del Estado, la prevención e investigación de delitos o infracciones a la deontología de las profesiones reglamentadas, por ser de interés económico y financiero del Estado miembro, para llevar a cabo funciones de control o inspección en relación con los motivos antes descritos o en su caso si fuese necesario para la protección del interesado o de los derechos y libertades de terceros. Siguen estando vigentes, específicamente el contenido del art. 22 de la LOPD hasta que no se transponga lo establecido en 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo para el caso de investigaciones de delitos. En el caso de restricción a los derechos antes descritos que obren en ficheros públicos cuyos responsables sean la Hacienda Pública y los cuerpos de policía, seguirán siendo de aplicación los apartados 2 y 3 del art. 23 de la LOPD, que aplican restricciones a los derechos de acceso, rectificación y cancelación de los interesados.

[237] Como se comenta en la nota a pie de página anterior, se sigue aplicando el art. 23 de la LOPD.

redes sociales y servicios equivalentes (art. 95), lo relativo al derecho al testamento digital (art. 96) y las políticas de impulso de los derechos digitales (art. 97), todos ellos del Título X, al igual que la mayoría de disposiciones adicionales, todas las transitorias y algunas de las finales[238]. De hecho, el art. 2 hace una referencia específica al ámbito de aplicación de esta LO, excluyendo su aplicación de los ámbitos no previstos en el RGPD, por ejemplo, los datos personales de las personas fallecidas. Al hilo de lo anterior, el Profesor TOLIVAR ALAS se ha establecido sobre la compatibilidad de las leyes orgánicas con las leyes ordinarias que «*La reserva de ley orgánica tampoco es incompatible con la complementación por ley ordinaria, que puede ser llamada por aquella a integrar en algunos extremos sus disposiciones a modo "de desarrollo", siempre y cuando no se efectúe "un reenvío en blanco o en condiciones tan laxas que viniesen a defraudar la reserva constitucional en favor de la ley orgánica.."*»[239]. En el caso del desarrollo de derechos fundamentales y de acuerdo con la STC de 137/1986, la inclusión de estas dos categorías normativas en una sola ley constituye «*una técnica sustitutiva de la igualmente constitucional consistente en la inclusión en la propia ley orgánica de normaciones ajenas al ámbito reservado*»[240].

A lo largo del texto de la LOPDGDD se hacen referencias exactas a lo establecido en el RGPD, especificando si es necesario acudir al contenido de lo establecido en el mismo, por lo que su contenido es complementario. En relación con la edad para emitir válidamente el consentimiento por menores, LOPDGDD fija en su art. 7 la edad de 14 años para que este sea válido y no se requiera también el de la persona que ejerza la patria potestad o la tutela del menor, atendiendo al art. 8.1 del RGPD que permite a los Estados miembros fijar una edad inferior a los 16 años.

---

[238] Casi todas las disposiciones adicionales tienen carácter de ley ordinaria con excepción de la segunda (protección de datos y transparencia y acceso a la información pública), y la decimoséptima (tratamiento de datos de salud), las transitorias igualmente tendrán carácter de ordinarias y las finales con excepción de la primera a la cuarta, la octava, décima y decimosexta, las que tienen carácter de orgánicas.

[239] Haciendo referencia in fine a GARCÍA ESCUDERO MÁRQUEZ, P., en Cfr. TOLIVAR ALAS, L., «Leyes Orgánicas», PENDÁS, B. (Dir.), *España Constitucional (1978-2018) Trayectorias y perspectivas*, Tomo III, Centro de Estudios Políticos y Constitucionales, Madrid, 2018, p. 2039.

[240] GARCÍA-ESCUDERO MÁRQUEZ, P., «Sinopsis artículo 81» (en línea), *Constitución española,* disponible en: https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=81&tipo=2 (consulta: 4 de enero de 2021).

Existen otras leyes que mantienen relación con el tratamiento de datos personales previsto tanto en el RGPD y la LOPDGDD, de indudable envergadura como Ley 34/2002 la cual versa sobre los servicios de la información y de comercio electrónico (LSSI), esta ley pretende la coordinación en el sector de la sociedad de la información con diversas normativas entre las que se encuentra la de la protección de los datos de carácter personal estableciéndose un régimen de responsabilidad de los diversos prestadores de servicios de la sociedad de la información, cuando se lleve a cabo el tratamiento de datos. También la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones, la cual tiene por objeto conforme a su art. 1 «*la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales*», sin perjuicio, del contenido de las leyes sectoriales que prevean el tratamiento de datos, como por ejemplo la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP)[241] o la Ley 33/2011, de 4 de octubre, General de Salud Pública[242], las cuales tendrán que aplicarse conforme a los dispuesto en este nuevo marco jurídico en la materia.

La responsabilidad en el tratamiento de datos personales no sólo se constriñe al mundo fáctico, sino a lo contenido en el web y específicamente en la web semántica, tiene una gran relevancia en el ámbito de las relaciones personales y en el comercio electrónico. En el contenido de las páginas *Web* pueden verterse datos personales de alguna persona física que la identifique o la haga identificable. El tratamiento, almacenamiento y la transmisión de los datos personales con el uso de las tecnologías suele ser mucho más cómoda, rápida y de bajo coste, lo que hace que los usuarios sean inconscientes del tipo de datos personales que proporcionan, a quiénes se les proporciona esa información y los peligros que supone cualquiera de

[241] Disposición adicional vigésima quinta de la LCSP.
[242] Art. 41.2 Ley General de Salud Pública.

estas actividades. Para PUENTE «*el individuo debería regirse en todas sus relaciones, dentro y fuera de Internet, por un código basado primordialmente en la autocensura, planteándose siempre, al interactuar con terceros, cuáles podrían ser las consecuencias de esa interactuación en un futuro indeterminado y en un entorno digital y globalmente accesible. En consecuencia, el libre desarrollo de la personalidad, basado en la posibilidad de tomar decisiones que no influyan el futuro devenir de la persona en sus relaciones con la sociedad o en la posibilidad de rectificar nuestras acciones pasadas o modificar nuestras opiniones con el paso de los años se difumina absolutamente, dado que el individuo debería, desde las primeras etapas de su desarrollo, tener conciencia de que cualquier actitud podrá ser tenida en cuenta permanentemente para valorar su personalidad o el modo en que el mismo podrá ser percibido en el futuro*»[243], en busca de una mayor protección de los datos personales.

Las vulneraciones al derecho a la protección de datos en el ámbito tecnológico se producen principalmente por los prestadores de servicios de la sociedad de la información, así como otros agentes intervinientes en la prestación de los servicios, debido a la gran cantidad de datos introducidos por los propios usuarios acerca de su vida privada o por las acciones que realizan en la web. La responsabilidad de todos los prestadores de servicios se refuerza con las nuevas definiciones principalmente las de datos personales (art. 4.1), tratamiento (art. 4.2), elaboración de perfiles (art. 4.4), y seudonimización (art. 4.5). Desde la entrada de aplicación del RGPD, se considera persona física identificable a «*toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, psíquica, económica, cultural o social de dicha persona*». Ahora todos los intervinientes en el tratamiento automatizado de datos incluidas las empresas que se dediquen a elaborar perfiles a partir de *cookies* y direcciones IP serán responsables del tratamiento de datos.

[243] PUENTE, A., «El derecho al olvido», PÉREZ BES, F. (Coord.), *El derecho de Internet,* Atelier libros jurídicos, 2016, p. 191.

Ahora todas las tecnologías diseñadas para la prestación de servicios de la sociedad de la información conforme a lo establecido en el art. 25 tendrán que tener 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 la 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*». Solo podrán ser tratados los datos necesarios para las finalidades específicas de cada tratamiento (art. 25.2 RGPD).

Las páginas web normalmente utilizan iconos de las diversas redes sociales y profesionales consistentes en hiperenlaces para facilitar la difusión del contenido de la propia página web. Lo cierto es que muchas veces no somos conscientes de las consecuencias que tiene en nuestros datos personales y tampoco si este tipo de iconos por el solo hecho de haberlos colocado en la página web supone un tratamiento de datos de los usuarios visitantes. Recientemente el TJUE en la sentencia de 29 de julio de 2019, caso *Fashion ID* & Co. KG y *Verbraucherzentrale NRW eV*, con intervención de *Facebook Ireland Ltd*, *Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen*, ha resuelto un asunto que tiene que ver con los hiperenlaces en forma de icono insertos en las páginas web [244]. Fue resuelto a la luz de la antigua Directiva 95/46/CE ya que esta era aplicable en el momento en que sucedieron los hechos. También está relacionado con el contenido del art. 5.3 de la Directiva 2002/58/CE en donde se establece que los prestadores de servicios deben recabar el consentimiento de los usuarios previa información clara y precisa sobre los fines del tratamiento de los datos personales recabados, en este caso en la página web de *Fashion ID*, una empresa dedicada a la

[244] STJUE de 29 de julio de 2019 (TJCE 2019\148; ECLI:EU:C:2019:629).

venta de prendas de vestir. El botón de «me gusta» que aparece en la página web de esta empresa remite contenido de manera externa a *Facebook.*

En este caso el TJUE, determina por una parte que *Fashion ID* es responsable del tratamiento, en cuanto a que «*las operaciones de tratamiento de datos personales cuyos fines y medios puede determinar Fashion ID, conjuntamente con Facebook Ireland, son, a la luz de la definición del concepto de "tratamiento de datos personales" que figura en el artículo 2, letra b) , de la Directiva 95/46 , la recogida y la comunicación por transmisión de datos personales de los visitantes de su sitio de Internet*»[245]. Ya que la empresa era consciente que el icono de «me gusta», servía de herramienta de recogida y de transmisión de datos personales de los usuarios visitantes del sitio web «*sean miembros o no de la red social Facebook*»[246]. Es decir, que influye en la recogida y la transmisión de los datos de los usuarios que visualizan su página web a favor de *Facebook.* Por lo que ambos agentes determinan los fines y los medios del tratamiento «*que originan las operaciones de recogida y de comunicación por transmisión de datos personales de los visitantes del sitio de Internet de Fashion ID*». Sin embargo, los fines de ambos agentes intervinientes en el tratamiento de datos son distintos, por una parte para la empresa *Fashion ID* tal inserción le permite optimizar la publicidad que se muestra en dicha red social y al insertar este botón de manera consciente «*parece haber consentido, al menos implícitamente, la recogida y la comunicación por transmisión de datos personales de los visitantes de su sitio, ya que esas operaciones de tratamiento se efectúan en interés económico tanto de Fashion ID como de Facebook Ireland, para quien el hecho de poder disponer de esos datos para sus propios fines comerciales constituye la contrapartida de la ventaja ofrecida a Fashion ID*»[247]. La responsabilidad de la empresa *Fashion ID* «*se limita a la operación o al conjunto de las operaciones de tratamiento de datos personales cuyos fines y medios determina efectivamente, a saber, la recogida y la comunicación por transmisión de datos en cuestión*»[248]. En cuanto al consentimiento se determina por el Tribunal que debe realizarse de manera anterior a «*la recogida y a la comunicación por transmisión de datos del*

[245] Numeral 76 de la STJUE de 29 de julio de 2019 (TJCE 2019\148; ECLI:EU:C:2019:629).
[246] Ib., numeral 77.
[247] Ib., numeral 80.
[248] Ib., numeral 85.

interesado» le corresponde a *Fashion ID* «*en la medida en que es el hecho de que un visitante consulte ese sitio de Internet lo que desencadena el proceso de tratamiento de datos personales*»[249], además de que este consentimiento solamente se refiere «*únicamente a la operación o al conjunto de las operaciones de tratamiento de datos personales cuyos fines y medios determina efectivamente dicho administrador*»[250].

Por otra parte, las páginas web de naturaleza públicas o privadas pueden llegar a contener datos personales de los usuarios que los identifiquen o los hagan identificables, dicha información puede llegar a lesionar el proyecto vital de la persona. Es por lo que se le debe reconocer al afectado, un derecho a la supresión cuando sus datos personales hayan cumplido la finalidad para la cual fueron recabados, retire su consentimiento, se oponga al tratamiento, cuando los datos hayan sido tratados ilícitamente o cuando hayan sido obtenidos siendo menor con motivo de la oferta de servicios de la sociedad de la información, conforme al nuevo art. 17.1 del RGPD.

Las redes sociales en la actualidad cuentan con gran efervescencia, sobre todo entre la juventud, dónde en muchos casos el suministrar una mayor cantidad de información relacionada con la persona a la red social (mayormente *Facebook*) puede ayudar a tener un cierto *status* de popularidad, principalmente entre los usuarios. La información suministrada puede consistir en fotos, vídeos, notas, preferencias, que sirvan para elaborar un perfil, por lo que si toda esta información suministrada, es descontextualizada y difundida de manera posterior, puede llegar a afectar el contenido del derecho a la protección de datos. Las redes sociales tal y como están estructuradas, requieren para prestar este servicio la elaboración de un perfil, en el cual el usuario deberá aportar información como su nombre, apellidos, mail, número de móvil, fecha de nacimiento, sexo, etc. Posteriormente, de manera progresiva se podrán aportar otro tipo de informaciones de manera voluntaria, como una breve descripción del usuario, su ubicación o lugar de residencia, formación o empleo, colegio o universidad, familia, relaciones, sitio web, idiomas, etc. La información sobre los usuarios también puede ser aportada por terceros, por

[249] Ib., numeral 102.
[250] *Íd.*

ejemplo, cuando se realiza alguna publicación en un perfil (ya sea en el propio o de un tercero) en donde se detalla si han visitado de manera conjunta algún sitio, alguna imagen o simplemente un mensaje, gracias al sistema de etiquetas que casi todas las redes sociales tienen. Otra forma de obtener información acerca de las personas dentro de una red social tiene que ver con la cantidad de «me gusta» o «*retweets*», las páginas que se visiten, etc., es decir que las acciones dentro de la red social arrojan también datos como la dirección IP, de manera que se puede realizar perfectamente un perfil detallado; siempre y cuando la actividad que se realiza en las redes sociales corresponda con la identidad de los individuos, puede que se elabore un perfil detallado a partir de los metadatos de una persona y que en realidad no sea quien dice ser. La suplantación de identidades en el entorno tecnológico está a la orden del día, y aunque las políticas de uso de las redes sociales determinen que la información aportada a tales efectos sea verídica y personal, la realidad apunta en sentido contrario. La dificultad de saber si lo que se publica es cierto o quien lo publica es quien dice ser es otra de las complejidades que entraña la web.

Otra cuestión no menos importante es la perennidad de los datos en los SRS, de conformidad con el artículo 5.1.e) del nuevo RGPD los datos podrán ser mantenidos de forma que se permita la identificación de los usuarios durante el tiempo que sea estrictamente necesario en relación con su finalidad. Teniendo en cuenta que algunos datos personales pueden implicar el tratamiento de distintos fines, debe recabarse el consentimiento de manera separada para cada uno de ellos, conforme a los establecido en el art. 6.1. a) del RGPD. Cuando una persona se borra de cualquier red social, se obliga al SRS como responsable a que elimine cualquier tipo de información provista por el propio usuario o derivada de su actividad dentro de la misma. Lo cual podría ser extensivo incluso a periodos de inactividad, aunque no se realice de esta manera en la actualidad, ya lo estableció en su momento GT 29: *«Cuando un usuario no utiliza el servicio durante un período determinado, el perfil debería desactivarse, es decir, dejar de ser visible por otros usuarios o por el mundo exterior y, después de otro período, los datos de la cuenta abandonada deberían*

suprimirse. Los SRS deberían informar a los usuarios antes de proceder a estos trámites a través de los medios de que dispongan»[251].

En relación con el diseño de los servicios de la sociedad de la información, actualmente existen aplicaciones y páginas *Web* como *WeTransfer*[252], *Periscope*[253] y *Snapchat*[254], a las que denomino *DataFriendly* o empáticas con la normativa de protección de datos, ya que debido a sus propias características y por defecto, hacen que las publicaciones realizadas por los usuarios tengan una temporalidad de

[251]Dictamen 5/2009 sobre las redes sociales en línea. Grupo de Trabajo sobre Protección de datos del art. 29, adoptado en fecha 12 de junio de 2009, p. 13.

[252] Está disponible en versión *Web* o en aplicación móvil, se trata de una plataforma de envío de archivos a gran escala, cuyo peso de estos puede alcanzar los dos GB (los *GigaBytes*, es una unidad de almacenamiento de información) si contamos con la versión gratuita, sin embargo, con la versión *Plus* (de pago), se pueden enviar hasta veinte GB de información en cualquier formato. Funciona de la siguiente manera, escribes el mail del destinatario (hasta veinte destinatarios), tu mail, y el mensaje que quieras enviar, se pueden también enviar documentos o cualquier tipo de imagen, vídeo o documento en cualquier tipo de formato con tan solo arrastrarlo al mensaje; después, se tiene que clicar el botón de hacer transferencia; cuando terminen de cargar los archivos se envían al destinatario. Al remitente se le envía un mail de confirmación de envío y otro cuando el destinatario haya descargado los archivos que le fueron enviados. Este tipo de tecnología supone grandes ventajas, ya que los usuarios no tienen que crear un usuario para poder acceder a este servicio, lo que implica que tus datos personales como nombre, apellidos, y número de móvil no se agreguen a un fichero de usuarios por parte de la página web. Otra ventaja es que la información a descargar solo está disponible por un tiempo limitado, para ser exactos siete días para su versión gratuita y cuatro semanas para su versión Plus. Creo que la desventaja, más evidente se encuentra en el envío de información cuyo contenido pueda suponer un ilícito o que la transferencia lo suponga. Al no tener un usuario para acceder al servicio, o verificar el usuario, se puede usar por cualquier persona que sepa tu correo electrónico y mandar archivos a tu nombre a cualquier persona, aunque el mail de conformación lo recibas tú, lo cual complica las cosas sobre todo si la información como mencionamos anteriormente supone un ilícito.

[253] *Periscope*, es una página Web y una aplicación móvil, que está asociada mayoritariamente a una cuenta de *Twitter,* donde se puede transmitir en formato vídeo lo que está sucediendo alrededor del mundo de manera directa, el vídeo inicialmente solo permanecía disponible para su visualización dentro de las veinticuatro horas. siguientes, después el contenido era eliminado por defecto. Ahora los usuarios pueden escoger entre almacenar de manera indefinida su contenido o por el contrario eliminar sus transmisiones después de veinticuatro horas, con la posibilidad de guardar esas transmisiones, *vid.* Periscope, How to save a Periscope broadcast: https://help.twitter.com/en/using-twitter/save-broadcast (consulta: 17 de diciembre de 2019).

[254] *Snap* según el *Cambridge Dictionary* en Reino Unido de manera informal se utiliza para denominar a las fotografías, *vid.* http://dictionary.cambridge.org/es/diccionario/ingles-espanol/snap (consulta: 17 de diciembre de 2019), lo cual tiene sentido ya que *Snapchat* se autodefine como una aplicación para compartir momentos a partir de fotografías o vídeos, con la posibilidad de enviar estos archivos a alguno de los contactos del usuario remitente e incluso el contenido puede ser visualizado por toda su lista de amigos. Su diseño implica que «*la mayoría de los mensajes que se envían mediante Snapchat se eliminarán automáticamente una vez que se han visto o han vencido*». Se eliminan después de veinticuatro horas: los *snaps* enviados a un chat grupal aun si no han sido vistos y las historias; se eliminan en treinta días los *snaps* que no fueron visualizados. Pero el contenido también puede eliminarse antes incluso de este plazo por el usuario de manera manual o cuando los archivos han sido visualizados por todos los destinatarios por defecto. Los vídeos y fotografías tienen una duración máxima de diez segundos, y no se almacenan los dispositivos de los usuarios, solo en los servidores de la empresa.

almacenamiento en la web bastante limitada. Dicha caducidad permite al usuario tener el control y certeza de que los datos personales que le hacen potencialmente identificable o identificables serán eliminados, reduciendo así su huella digital.

El mayor problema que presentan los servicios consistentes en la provisión de instrumentos de búsqueda, acceso y recopilación de datos o enlaces a otros sitios web, como bien señala PUENTE, tiene que ver con el «efecto multiplicador» que generan, ya que permiten que «*cualquier opinión de una persona o sobre una persona, cada "post" que pueda referirse a aquélla, cada fotografía o cada vídeo en que aparezca (incluso accidentalmente) o cualquier hecho del pasado sea accesible de forma sencilla, rápida y permanente por cualquier persona en cualquier lugar del mundo y pueda ser empleado para efectuar una valoración de esa persona, en cualquier entorno y para cualquier finalidad, con independencia de que la información recabada sea cierta, relevante, actualizada o completa, simplemente por el hecho de que esa información se contiene en la lista de resultados de esa persona obtenida a partir de su nombre*»[255].

Los motores de búsqueda o buscadores tienen un papel importante en el tratamiento de los datos, de conformidad con lo establecido por la AEPD en varias resoluciones[256]. Estos facilitan al usuario de *Internet* el acceso a determinadas páginas web y ponen a su disposición una lista de resultados relacionada con los parámetros de búsqueda utilizados por los mismos, es decir, *«Los motores de búsqueda indexan información que está disponible en la Web, y por lo tanto, ponen al alcance de los ciudadanos un sistema para acceder, recoger, conservar y modificar información que eventualmente contiene datos personales»*[257]*.* De acuerdo con la Directiva 2015/1535 del Parlamento Europeo y del Consejo, de 9 de diciembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información, los motores de búsqueda tienen que ser considerados como servicios, pues como señala su art.1.b) se considera como servicio a todo aquel «*prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a*

[255] PUENTE, A., *op. cit.,* p. 188.
[256] Resoluciones en los procedimientos TD/01335/2008 y TD/00463/2007.
[257] SIMÓN CASTELLANO, P., *op. cit.,* p. 140.

petición individual de un destinatarios de servicios». Específicamente como prestadores de servicio de intermediación, ya que proveen al usuario de «*instrumentos de búsqueda, acceso y recopilación de datos o enlaces a otros sitios de internet*»[258]. Por lo tanto, están sujetos al régimen de responsabilidades establecido por 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 (Directiva sobre el comercio electrónico). También a lo establecido en la norma de transposición española, la LSSI.

Algunos buscadores tienen la opción de crear un perfil o registrarse con información del usuario con la finalidad de ofrecer un mejor servicio, además, de ofrecer otras herramientas relacionadas con la prestación de servicios de la sociedad de la información, como red social, *blogs*, etc. Es por lo que este tipo de empresas pueden tener acceso de muchas maneras a las preferencias de los usuarios e insertar publicidad acorde con su perfil y a la información almacenada en el mismo, lo que puede acarrear un mayor tratamiento y almacenamiento de datos. Como bien señala HERNÁNDEZ RAMOS *«muchas veces la retención de estos datos deja de tener justificación con el paso del tiempo, ya que aunque en un principio su recogida estaba legitimada, su conservación indefinida y sin motivo que la sustente deja de tener sentido»*[259].

Los datos personales de los usuarios que son tratados por los prestadores de servicios de intermediación, específicamente por los motores de búsqueda, conforme al Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda del GT29, son: los datos contenidos en los ficheros de registro [260] (los cuales integran una gran y diversa cantidad de datos), las

[258] Letra b) del Anexo de la LSSI.

[259] HERNÁNDEZ RAMOS, M., «El Derecho al olvido digital en la web 2.0» (en línea), *Cuaderno de Red de Cátedras Telefónica,* núm. 11, 2013, p. 29 Disponible en: https://dialnet.unirioja.es/descarga/articulo/4498471.pdf (consulta y descarga: 26 de junio de 2017).

[260] Los ficheros de registro de conformidad con lo establecido por el Grupo sobre protección de datos del artículo 29, en su Dictamen 1/2008 sobre cuestiones de protección de datos relacionados con motores de búsqueda son: -suponiendo que no se hagan anónimos-los datos personales más importantes tratados por los proveedores de motores de búsqueda. Los datos que describen la

direcciones IP, *Cookies* de red y *cookies flash*[261]. Lo anterior supone la elaboración de perfiles detallados de los usuarios de este tipo de servicios.

4. ESPECIAL REFERENCIA AL DERECHO AL OLVIDO DIGITAL.

A partir de los cambios en las tecnologías y específicamente en la *Web*, la fácil y numerosa transferencia de datos en la misma, el bajo coste y fácil almacenamiento de datos de las personas por parte del responsable del tratamiento de los datos, así como la perennidad en este tipo de plataformas, especialmente los motores de búsqueda han hecho surgir el derecho al olvido digital.

El derecho al olvido en Europa tiene sus primeras manifestaciones en Francia y Bélgica a finales del siglo XX[262]. Este derecho según ROUVROY[263], se puede desglosar en dos, por una parte encontramos el derecho a olvidar, el cual se refiere al proceso natural e involuntario de las personas que con el paso del tiempo olvidan cosas, y por otro lado, tenemos el derecho a hacerse olvidar o a hacernos olvidar, el cual

utilización de los servicios pueden dividirse en distintas categorías: los registros de consultas (contenido de consultas, fecha, hora, fuente (dirección IP y *cookie*), preferencias del usuario y datos relativos a su ordenador); los datos relativos al contenido propuesto (vínculos de publicidad resultante de cada consulta) y datos relativos a los lugares visitados a continuación por el usuario (*clicks*). Los motores de búsqueda también pueden tratar datos operativos relativos a los datos del usuario, datos relativos al usuario registrados, y datos de otros servicios y fuentes como el correo electrónico, la búsqueda en el ordenador del usuario (*desktop search*) y la publicidad en sitios Internet de terceros.

[261] De conformidad con lo establecido por el Grupo sobre protección de datos del artículo 29, en su Dictamen 1/2008 sobre cuestiones de protección de datos relacionados con motores de búsqueda, establece que: las *cookies red* son aquellas que proporciona el motor de búsqueda y se almacenan en el ordenador, contienen generalmente información relativa al sistema operativo y al navegador del usuario, así como un número de identificación único para cada cuenta de usuario y las *cookies flash,* son aquellas con las que cuentan algunas empresas de motores de búsqueda se utilizan por ejemplo como copia de seguridad de las *cookie*s normales o para almacenar información detallada sobre las búsquedas efectuadas por los usuarios.

[262] En Bélgica se regula por la Ley relativa a la protección de la vida privada y tratamiento de datos personales (Trad. *«Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)* específicamente en el art. 12, sin que se encuentre literalmente el termino Derecho al olvido. Por su parte Francia, tiene en marcha una propuesta de Ley que data de 2009 *(Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique*) y que aún está inmersa en el proceso legislativo para su aprobación, lo cual se puede corroborar en la página del Senado Francés, Cfr. Disponible en: https://www.senat.fr/dossier-legislatif/ppl09-093.html (consulta: 19 de junio de 2017).

[263] Para ROUVROY el Derecho al olvido tiene una doble acepción, por una parte, es *«el derecho o más bien el interés legítimo de olvidar y hacerse olvidar»* trad. Del francés: *«intérêt légitime à oublier et à se faire oublié», vid.* ROUVROY, A., «Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?» (en línea), *La sécurité de l'individu numérisé. Réflexions prospectives et internationales,* 2008, p. 25. Disponible en: https://works.bepress.com/antoinette_rouvroy/5/(consulta: 19 de junio de 2016).

consiste en que no aparezcan nuestros datos personales en la web, ya que la perennidad de la información, hace que se tenga un recuerdo constante de la información proporcionada principalmente por motores de búsqueda y páginas de web, que hacen que el proceso natural del olvido se vea modificado, al estar siempre disponible en la *Web*, no se permite olvidar la información que no es relevante para las personas. DE TERWANGNE es otra autora que concibe el derecho al olvido de la misma manera que ROUVROY, establece que «*contrariamente a lo que sucede en la vida física, la eliminación de datos en el mundo digital exige tomar una decisión al respecto. Se trata de un proceso consciente y voluntario. Hay que tener la voluntad de eliminar los datos*»[264].

4.1 La Sentencia del TJUE, de 13 de mayo de 2014.

El derecho al olvido tiene su origen a nivel comunitario en la Sentencia del TJUE (Gran Sala) de 13 de mayo de 2014, caso *Google Spain, S.L., Google Inc*. y AEPD, Mario Costeja[265]. Esta Sentencia encuentra su origen en la reclamación de una persona de nacionalidad española efectuada ante la AEPD el 5 de marzo de 2010, por la que ejerce su derecho de oposición, contra el periódico «La Vanguardia», y su derecho de cancelación en cuanto a *Google Spain, S.L.*, y *Google Inc.,* pues si se realizaba una búsqueda por su nombre en *google.es*, se obtenía una lista de resultados que contenía enlaces a noticias realizadas por este periódico, en donde se anunciaba la subasta de inmuebles relacionados con deudas a la Seguridad Social, mencionando su nombre; dicha subasta era un hecho pasado acontecido hacía más de dos años respecto a la fecha de la reclamación y, por lo tanto, el reclamante estimaba que esa información ya carecía de relevancia[266]. Ante esta afirmación se le

[264] TERWANGNE, C. DE, «Privacidad en Internet y el derecho a ser olvidado/derecho al olvido» (en línea), *IDP: Revista de Internet, Derecho y Política,* núm. 13, 2012, p. 60 Disponible en: https://www.raco.cat/index.php/IDP/article/view/251842/337491 (consulta: 22 de noviembre de 2020).

[265] TJCE 2014\85; ECLI:EU:C:2014:317.

[266] En un primer momento, la AEPD, desestimó la reclamación hecha a «La Vanguardia», ya que la publicación realizada por el periódico tenía sustento en lo establecido en el art. 646.1 y 2 de la LEC: «*1. A toda subasta se dará publicidad por medio de edictos, que se fijarán en el sitio destacado, público y visible en la sede del tribunal y lugares públicos de costumbre. Además, a instancia del ejecutante o del ejecutado y si el tribunal lo juzga conveniente, mediante providencia se dará a la subasta la publicidad que resulte razonable, utilizando los medios públicos y privados que sean más adecuados a la naturaleza y valor de los bienes que se pretende realizar. 2. Cada parte estará obligada al pago de los*

pedía al periódico «*La Vanguardia*» que eliminara o modificara la publicación para que no apareciesen sus datos personales y, a *Google* que eliminara u ocultara sus datos personales para que dejaran de incluirse en los resultados de búsqueda y de estar ligados a «*La Vanguardia*», pues ese asunto ya estaba solucionado desde ya hacía varios años y, por lo tanto, la información carecía de relevancia.

El asunto se estimó por parte de la AEPD parcialmente en contra de *Google Spain* S.L., y *Google Inc*., en resolución de fecha de 30 de julio de 2010, al considerar que quienes gestionan los motores de búsqueda están sometidos a la normativa en materia de protección de datos ya que llevaban a cabo un tratamiento de datos del que eran responsables y actuaban como intermediarios de la sociedad de la información. De igual forma la Agencia estima que el requerimiento planteado por el Sr. X, puede dirigirse a motores de búsqueda como es *Google*, sin suprimir los datos o la información de la página donde inicialmente está alojada e, incluso, cuando el mantenimiento de esta información en dicha página esté justificado por una norma legal, por lo que insta a *Google Spain* a que adopte medidas necesarias para la retirada de los datos de su índice de resultados y que imposibilitase el acceso futuro a los mismos[267] ya que *Google Spain, S.L*., debido a que es «representante» en territorio español del motor de búsqueda norteamericano, y realiza tratamiento de datos por medio de *cookies* así como direcciones IP, para proveer de publicidad a las páginas con dominio español[268]. Esta determinación por parte de la AEPD estableció

gastos derivados de las medidas que, para la publicidad de la subasta, hubieran solicitado, sin perjuicio de incluir en la liquidación de costas los gastos que, por este concepto, soporte el ejecutante», y en lo establecido en el art. 117.1 del Real Decreto 1415/2004, de 11 de junio, por el que se aprueba el Reglamento General de Recaudación de la Seguridad Social: «*1. La subasta se publicará en el tablón de anuncios de la Dirección Provincial, de sus dependencias y de los ayuntamientos, en cuyas demarcaciones se hallen los bienes. Cuando el valor de los bienes supere la cuantía que se fije por resolución del Director General de la Tesorería General de la Seguridad Social, el anuncia de la subasta deberá insertarse, además, en el boletín oficial de la provincia o boletín oficial de la comunidad autónoma correspondiente. Cuando, a juicio del Director Provincial de la Tesorería General de la Seguridad Social, sea conveniente para el fin perseguido y resulte proporcionado con el valor de los bienes, podrá publicarse también el anuncio de la subasta en medios de comunicación de gran difusión o en publicaciones especializadas»,* debido a que esta publicación había sido legalmente sustentada y justificada, ya que tuvo lugar por orden del Ministerio de Trabajo y Asuntos Sociales y tenía por objeto dar la máxima publicidad a la subasta para conseguir una mayor concurrencia.

[267] Resolución de la AEPD de 30 de julio de 2010, procedimiento TD/00650/2010 Disponible en: https://www.aepd.es/es/documento/td-00650-2010.pdf (consulta: 19 de junio de 2017).

[268] Se realiza el estudio debido a las alegaciones vertidas en ese procedimiento por *Google Spain*, de que no debe ser considerado como responsable, ya que el solo representa a *Google Inc*. en la venta de

que puede dirigirse directamente ante motores de búsqueda por reclamaciones de esta naturaleza, sin que esta previamente haya sido eliminada de la página *Web* donde inicialmente se albergaba la información que se pretendía eliminar, ordenándose solo la eliminación de la página de resultados indexada por el buscador.

Posteriormente el asunto llega a instancias de la Audiencia Nacional (AN) ya que el representante de *Google* interpuso recurso contencioso-administrativo en contra la resolución de la AEPD, la cual fue admitida y formalizada el 30 de diciembre de 2010. Previos trámites procedimentales, por auto de 27 de febrero de 2011 se acordó plantear una cuestión prejudicial de interpretación, dividida en tres preguntas: la primera cuestión prejudicial versa sobre la aplicación territorial de la Directiva 95/46/CE (art. 4) y, en consecuencia, si debe ser aplicada la normativa española en materia de protección de datos. Esta cuestión prejudicial trata de aclarar cuatro aspectos concretos, el primero ellos pretende conocer si debe considerarse como establecimiento a una empresa filial si: 1) está destinada a la

espacios publicitarios, y que por lo tanto al no ser la responsable del tratamiento de los datos personales, la reclamación deberá efectuarse únicamente contra *Google Inc.,* sin embargo, la resolución establece que *Google Spain* debe ser considerado como encargado del tratamiento de los datos ubicado en territorio español (Art. 3 del RD 1720/2008) y no así como representante, pues a pesar de que *Google Inc*. tiene su domicilio fuera de la UE, los datos tratados no se utilizan con fines de tránsito (en concordancia con lo establecido en el Reglamento art. 3.1.c) y el art. 4.1.c) y numero 18 y 20 de la exposición de motivos de la Directiva 95/45/CE) esto encuentra respaldo también en lo establecido en el Documento 148 de 4 de abril de 2008 del Grupo de Trabajo «WP 29» relativo a buscadores, en donde se establece que se debe considerar responsable del tratamiento, pues *«Un proveedor de motor de búsqueda que trata datos de los usuarios que incluyen direcciones IP y/o cookies permanentes que contienen un identificador único responde a la definición de responsable del tratamiento puesto que determina efectivamente los fines y medios del tratamiento», siempre que se cuente con un establecimiento en un Estado miembro y «la operación de tratamiento debe por otro lado efectuarse "en el marco de las actividades" del establecimiento. Eso significa que el establecimiento debe también desempeñar un papel significativo en el tratamiento en cuestión. Es el caso claramente si: un proveedor de motor de búsqueda establece una oficina en un Estado miembro (EEE) que participa en la venta de publicidad orientada a los habitantes de este Estado»*. Por otra parte, queda evidenciado que la versión española de *Google Search: google.es,* indexa documentos almacenados en la *Web*, a partir de arañas *Web* que *«Analizan de forma metódica páginas web HTML disponibles públicamente, recopilando los hiperenlaces que figuran en éstas (referencias a otras direcciones URL), para extender así su labor de rastreo, de forma encadenada, a todas las páginas y documentos referenciados. El rastreo consiste en extraer, de los documentos visitados (no sólo de las páginas con formato HTML, sino también de los documentos que presentan otros formatos), las palabras clave que serán indexadas» (*Numeral número V de la Resolución R/01680/2010 de 30 de julio de 2010, elaborada por la AEPD), y que la empresa se dedica a ofrecer publicidad con base en los resultados de las búsquedas anteriores de los usuarios (sistema *AdWords*) y en páginas *Web* para que aparezcan anuncios de Google relacionados con el contenido de la propia página, específicamente en el territorio español, lo cual requiere la utilización de *cookies* y la dirección, lo cual implica el tratamiento de datos.

venta y promoción de espacios publicitarios en un Estado miembro por un proveedor del motor de búsqueda, 2) es responsable de ficheros que contengan datos de los clientes, y 3) en caso de que la empresa traslade información a la matriz radicada fuera de la UE (art. 4.1.a) [269]. El segundo de los aspectos a clarificar dentro de esta cuestión prejudicial es conocer si es aplicable la normativa en la materia en el caso de que un motor de búsqueda recurra a medios situados en el territorio español y utilice arañas o robots para indexar la información en páginas web ubicadas en servidores de este Estado, o, en el caso de que el buscador utilice un dominio propio del Estado miembro y dirija las búsquedas y resultados en el mismo idioma que en el de ese Estado. En esta cuestión prejudicial también se pretende conocer si debe considerarse como un recurso a los medios de almacenamiento temporal de la información indexada [270] y, si debe aplicarse la Directiva 95/46/CE a la luz del art. 8 de la CDFUE, en el país miembro donde se localice el conflicto para garantizar la eficacia de los derechos de los ciudadanos de la UE.

La segunda cuestión prejudicial pretende conocer si la actividad de los buscadores debe ser considerada como «tratamiento de datos» de acuerdo con la Directiva 95/46/CE (art. 2.1.b) [271]. En caso de que la respuesta fuese positiva, determinar si los buscadores deben ser considerados como responsables del tratamiento (art. 2.1.d) [272] de la Directiva 95/46/CE, en el caso de que sea

[269] Art. 4.1. a) de la Directiva 95/46/CE: *«Derecho nacional aplicable 1. Los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando: a) el tratamiento sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro. Cuando el mismo responsable del tratamiento esté establecido en el territorio de varios Estados miembros deberá adoptar las medidas necesarias para garantizar que cada uno de dichos establecimientos cumple las obligaciones previstas por el Derecho nacional aplicable».*

[270] Art. 4.1. c) de la Directiva 95/46/CE: *«c) el responsable del tratamiento no esté establecido en el territorio de la Comunidad y recurra, para el tratamiento de datos personales, a medios, automatizados o no, situados en el territorio de dicho Estado miembro, salvo en caso de que dichos medios se utilicen solamente con fines de tránsito por el territorio de la Comunidad Europea».*

[271] Art.2.1 .b) de la Directiva 95/46/CE: *«"Tratamiento de datos personales,, (tratamiento)": cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción».*

[272] Art. 2.1. d) de la Directiva 95/46/CE: *«Responsable del tratamiento»: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que sólo o conjuntamente con otros determine los fines y los medios del tratamiento de datos, personales; en caso de que los fines y los medios del*

considerado como responsable del tratamiento. Por último, se plantea si la autoridad española (AEPD) encargada de tutelar los derechos contenidos en el art. 12.b) [273] y 14.a) [274] en la Directiva antes referida, puede requerir directamente a *Google Search* para exigirle la retirada en sus listas de búsquedas la información publicada por terceros sin dirigirse previa o simultáneamente al responsable de la página web. En caso de que la respuesta fuese afirmativa, si debe ser excluida la obligación a los buscadores cuando la información publicada en la página *Web* sea lícita y se mantenga en la misma.

Por último, la tercera cuestión prejudicial plantea si los derechos de cancelación y oposición pueden ser ejercidos por las personas afectadas hacia los buscadores cuando la información que aparece en la lista de resultados les afecte o deseen que sea olvidada, sin perjuicio de que dicha publicación se haya hecho de manera lícita por un tercero.

El TJUE en su Sentencia de 13 de mayo de 2014, responde a las cuestiones planteadas de la siguiente manera, en cuanto a la segunda cuestión prejudicial, sobre si la actividad de los buscadores debe ser considerada como tratamiento de datos consistente en «*hallar información pública 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"*»[275], *el* TJUE responde diciendo que previamente había tenido oportunidad en la Sentencia *Lindqvist*[276], de considerar

tratamiento estén determinados por disposiciones legislativas o reglamentarias nacionales o comunitarias, el responsable del tratamiento o los criterios específicos para su nombramiento podrán ser fijados por el Derecho nacional o comunitario».

[273] Art. 12. b) de la Directiva 95/46/CE: *«Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: […] b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos»*

[274] Art. 14. a) de la Directiva 95/46/CE: *«Los Estados miembros reconocerán al interesado el derecho a: a) oponerse, al menos en los casos contemplados en las letras e) y f) del artículo 7, en cualquier momento y por razones legítimas propias de su situación particular, a que los datos que le conciernan sean objeto de tratamiento, salvo cuando la legislación nacional disponga otra cosa. En caso de oposición justificada, el tratamiento que efectúe el responsable no podrá referirse ya a esos datos».*

[275] Numeral 21 de la STJUE de 13 de mayo de 2014 (TJCE 2014\85; ECLI:EU:C:2014:317).

[276] STJUE de 6 de noviembre de 2003 (asunto C-101/01; ECLI:EU:C:2003:596), en este caso el Tribunal de Apelación Sueco (*Göta hovrätt*) planteó la cuestión perjudicial de interpretación, relativa a la protección de las personas físicas respecto al tratamiento de datos personales por aplicación de

como «tratamiento de datos» el que se incluyan datos personales en una página *Web.* A su vez, considera que derivado de la actividad que realiza el motor de búsqueda, este puede mostrar datos que identifiquen o hagan identificables a las personas en la listas de resultados previa indexación de los datos encontrados en sitios *Web* y, por tanto, tener la categoría de «datos personales», y en consecuencia declara que: *«al explorar Internet de manera automatizada, constante y sistemática en busca de la información que allí se publica, el gestor de un motor de búsqueda "recoge" tales datos que "extrae", "registra" y "organiza" posteriormente en el marco de sus programas de indexación, "conserva" en sus servidores y, en su caso, "comunica" y "facilita el acceso" a sus usuarios en forma de listas de resultados de sus búsquedas. Ya que estas operaciones están recogidas de forma explícita e incondicional en el artículo 2, letra b), de la Directiva 95/46, deben calificarse de "tratamiento" en el sentido de dicha disposición, sin que sea relevante que el gestor del motor de búsqueda también realice las mismas operaciones con otros tipos de información y no distinga entre éstos y los datos personales»*[277].

En relación con la valoración que hace el Tribunal sobre si debe considerar a los motores de búsqueda como responsables, este establece que, debido a que son estos quienes determinan los fines y medios de su actividad, actividad que está relacionada con el contenido en páginas web y con el contenido de las listas de resultados que ofrecen a los usuarios por búsquedas realizadas por el nombre de una persona, además considerando que los resultados pueden ser lesivos para las

la Directiva 95/46/CE, específicamente de los artículos: 3.1 (aplicación de la Directiva por el tratamiento automatizado de datos personales), art. 8 (tratamiento de categorías especiales de datos, específicamente a que se debe dar el consentimiento explícito cuando se traten datos relativos en este caso a la situación laboral), art. 9 (tratamiento de datos personales y libertad de expresión-fines periodísticos-). La primera cuestión se planteó de la siguiente manera: *«¿Constituye una conducta comprendida en el ámbito de aplicación de la Directiva [95/46] la designación de una persona —con su nombre o con su nombre y número de teléfono— en una página web de Internet? ¿Constituye un "tratamiento total o parcialmente automatizado de datos personales" el hecho de que en una página web de Internet realizada personalmente se relacione a una serie de personas junto con datos y afirmaciones relativas a su situación laboral y a sus aficiones?»,* a lo que el Tribunal determinó con base en lo establecido en los artículos 2.1.a) (lo que se debe considerar como datos personales), art. 2.1.b) (lo que se entiende por datos personales) y el 3.1 (aplicación de la Directiva por el tratamiento automatizado de datos personales) de la Directiva 95/46/CE, *«que la conducta que consiste en hacer referencia, en una página web, a diversas personas y en identificarlas por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un "tratamiento total o parcialmente automatizado de datos personales" en el sentido del artículo 3, apartado 1, de la Directiva 95/46»* (numeral 27 de dicha Sentencia).

[277] Numeral 28 de la STJUE de 13 de mayo de 2014 (TJCE 2014\85; ECLI:EU:C:2014:317).

personas ya que pueden hacerlas plenamente identificables y por tanto, dañar su esfera privada, los motores de búsqueda deben ser considerados como responsable del tratamiento de datos personales [278].

En cuanto a la primera cuestión prejudicial planteada relacionada con la aplicación territorial de la Directiva 95/46/CE y por consiguiente la normativa de transposición del Estado español en materia de protección de datos, el Tribunal con ayuda de lo establecido en el considerando 19 de la Directiva [279], la cual determina que el establecimiento en un Estado miembro debe implicar el ejercicio efectivo y real de una actividad sin importar la forma jurídica del mismo, interpretando el contenido del art. 4.1.a) que señala que *«el tratamiento de datos personales realizado en orden al funcionamiento de un motor de búsqueda como Google Search, gestionado por una empresa que tiene su domicilio social en un Estado tercero pero que dispone de un establecimiento en un Estado miembro, se efectúa "en el marco de las actividades" de dicho establecimiento si éste está destinado a la promoción y venta en dicho Estado miembro de los espacios publicitarios del motor de búsqueda, que sirven para rentabilizar el servicio propuesto por el motor. En efecto, en tales circunstancias, las actividades del gestor del motor de búsqueda y las de su establecimiento situado en el Estado miembro de que se trate están indisociablemente ligadas, dado que las actividades relativas a los espacios publicitarios constituyen el medio para que el motor de búsqueda en cuestión sea económicamente rentable y dado que este motor es, al mismo tiempo, el medio que permite realizar las mencionadas actividades»* [280]. Cabe mencionar que otra de las grandes actividades que realiza *Google Search* es la de insertar publicidad en relación con las búsquedas realizadas por el usuario. Esta utiliza a *Google Spain*, una empresa filial para desarrollar la parte de publicidad en España y a la que se le designó como responsable de dos ficheros de tratamiento de

[278] *Ib.*, numerales 33-41.
[279] Considerando 19 de la Directiva 95/46/CE: *«Considerando que el establecimiento en el territorio de un Estado miembro implica el ejercicio efectivo y real de una actividad mediante una instalación estable; que la forma jurídica de dicho establecimiento, sea una simple sucursal o una empresa filial con personalidad jurídica, no es un factor determinante al respecto; que cuando un mismo responsable esté establecido en el territorio de varios Estados miembros, en particular por medio de una empresa filial, debe garantizar, en particular para evitar que se eluda la normativa aplicable, que cada uno de los establecimientos cumpla las obligaciones impuestas por el Derecho nacional aplicable a estas actividades».*
[280] Numerales 55 y 56 de la STJUE de 13 de mayo de 2014 (TJCE 2014\85; ECLI:EU:C:2014:317).

datos en su momento ante la AEPD. En relación con lo anterior, la sentencia concluye que se ha de considerar a *Google Spain*, como un establecimiento del Grupo *Google*. Ahora bien, debido a que realiza parte del tratamiento de datos de carácter personal en el marco de las actividades de *Google Search*, de acuerdo con lo establecido en el art. 4, apartado1, letra a) de la Directiva, se considera que se lleva a cabo un tratamiento de datos personales en España y por ende, tiene que aplicarse la Directiva 95/46/CE[281]. Es decir, *Google Inc.* lleva a cabo un tratamiento de datos personales en el marco de un establecimiento responsable (*Google Spain*) y en consecuencia debe ser de aplicación la normativa española en materia de protección de datos personales, pues es la que transpone la Directiva 95/46/CE.

En un tercer momento, el Tribunal vuelve a la segunda cuestión prejudicial, para determinar si *«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»*[282] para precisar si se debe excluir a los buscadores de la obligación de la tutela de los derechos de cancelación y oposición, cuando la información haya sido publicada de manera lícita por el titular de la página *web* y esta se mantenga en la misma. Una vez determinada la responsabilidad en el tratamiento de los datos por parte del gestor del motor de búsqueda (*Google Inc.*) y por tanto, el deber de respetar la normativa en esta materia, es decir la Directiva, específicamente lo contenido en el art. 13 (el límite del alcance de las obligaciones y

[281] Lo anterior con base en los apartados 21 al 28 de la STJUE de 13 de mayo de 2014 (TJCE 2014\85; ECLI:EU:C:2014:317).
[282] Numeral 62 de la STJUE, de 13 de mayo de 2014 (TJCE 2014\85; ECLI:EU:C:2014:317).

los derechos)[283], art. 6 (principios relativos a la calidad de los datos)[284], art. 7.f) (principios relativos a la legitimación del tratamiento de datos)[285], art. 28.3 y 4 (autoridad de control tiene poder efectivo de investigación, intervención, capacidad procesal y atención de solicitudes por parte de los afectados)[286], aunado con lo establecido en los arts. 7[287] y 8[288] de la CDFUE, se determina que el interés del motor

[283] Art. 13 de la Directiva 95/46/CE: *«1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) tina función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras personas. 2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas».*

[284] Art. 6 de la Directiva 95/46/CE: *«1. Los Estados miembros dispondrán que los datos personales sean: a) tratados de manera leal y lícita; b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre Y cuando los Estados miembros establezcan las garantías oportunas».*

[285] Art. 7. f) de la Directiva 95/46/CE: *«Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva».*

[286] Art. 28.3 y 4 de la Directiva 95/46/CE: *«3. La autoridad de control dispondrá, en particular, de: - poderes de investigación, como el derecho de acceder a los datos que sean objeto de un tratamiento y el de recabar toda la información necesaria para el cumplimiento de su misión de control; - poderes efectivos de intervención, como, por ejemplo, el de formular dictámenes antes de realizar los tratamientos, con arreglo al artículo 20, y garantizar una publicación adecuada de dichos dictámenes, o el de ordenar el bloqueo, la supresión o la destrucción de datos, o incluso prohibir provisional o definitivamente un tratamiento, o el de dirigir una advertencia o amonestación al responsable del tratamiento o el de someter la cuestión a los parlamentos u otras instituciones políticas nacionales; - capacidad procesal en caso de infracciones a las disposiciones nacionales adoptadas en aplicación de la presente Directiva o de poner dichas infracciones en conocimiento de la autoridad judicial. Las decisiones de la autoridad de control lesivas de derechos podrán ser objeto de recurso jurisdiccional. 4. Toda autoridad de control entenderá de las solicitudes que cualquier persona, o cualquier asociación que la represente, le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales. Esa persona será informada del curso dado a su solicitud. Toda autoridad de control entenderá, en particular, de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales tomadas en virtud del artículo 13 de la presente Directiva. Dicha persona será informada en todos los casos de que ha tenido lugar una verificación».*

[287] Relativo al respeto a la vida privada y familiar: *«Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones».*

[288] Relativo al derecho a la protección de datos de carácter personal.

de búsqueda legitima el tratamiento de datos personales sin embargo, no prevalece sobre los derecho de los interesados, es decir que hay que buscar equilibro entre derechos y legitimidad en el tratamiento de los mismos *«con arreglo a los artículos 7 y 8 de la Carta. Aunque, ciertamente, los derechos de esa persona protegidos por dichos artículos prevalecen igualmente, con carácter general, sobre el mencionado interés de los internautas, no obstante este equilibrio puede depender, en supuestos específicos, de la naturaleza de la información de que se trate y del carácter sensible para la vida privada de la persona afectada y del interés del público en disponer de esta información, que puede variar, en particular, en función del papel que esta persona desempeñe en la vida pública»*[289].

El TJUE determina que la actividad del gestor de motor de búsqueda puede «*afectar significativamente a los derechos fundamentales del respeto a la vida privada y de protección de datos personales cuando la búsqueda realizada sirviéndose de ese motor de búsqueda se lleva a cabo a partir del nombre de una persona física, toda vez que dicho tratamiento permite a cualquier internauta obtener mediante la lista de resultados una visión estructurada de la información relativa a esta persona que puede hallarse en Internet, que afecta potencialmente a una multitud de aspectos de su vida privada»*[290], por lo que establece la total independencia del ejercicio de los derechos de cancelación y oposición frente a los motores de búsqueda respecto al titular del sitio web donde se almacena esa información, y por tanto, la autoridad de control y/o el órgano jurisdiccional competente *«pueden ordenar a dicho gestor 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*»[291] ya que su actividad como deja claro puede lesionar derechos fundamentales y que de lo contrario «*no podría llevarse a cabo una protección eficaz y completa de los interesados si éstos debieran obtener con carácter previo o en paralelo la eliminación de la información que les afecta de los editores de sitios de Internet*»[292].

[289] Numeral 81 de la STJUE, de 13 de mayo de 2014 (TJCE 2014\85; ECLI:EU:C:2014:317).
[290] *Ib.,* numeral 80.
[291] *Ib.,* numeral 82.
[292] *Ib.,* numeral 84.

Por último, el TJUE, resuelve la tercera cuestión prejudicial, determinando que las personas pueden ejercer su derecho de cancelación u oposición cuando la información relativa a su persona se obtenga de una lista de resultados basándose en una búsqueda por su nombre siempre que los resultados sean inadecuados, no pertinentes o excesivos en relación con los fines del tratamiento, o esta lista esté desactualizada o se conserven datos personales por tiempo mayor al necesario[293]. Sin embargo, como se establece en la sentencia, debe realizarse una ponderación entre el derecho público de la persona a tener esa información y el de los derechos contemplados en los art. 7 y 8 de la CDFUE, es por ello, que siempre que la información no tenga relevancia en la vida pública y pueda tener un impacto a la hora de crear una opinión de la vida democrática, prevalecerá el derecho a la protección de datos sobre la información[294].

Es así como a partir de esta sentencia se configura este nuevo derecho, el cual otorga a las personas el poder de decidir qué datos circulan en la *web* sobre sí mismas, por búsquedas realizadas a partir de su nombre, sobre todo si la información les causase algún tipo de perjuicio o simplemente porque se ha cumplido con la finalidad para la cual fueron recogidos sus datos o por su inexactitud, pudiéndose ejercer de manera separada e independiente frente al responsable del tratamiento de datos de la página web; para ejercer sus derechos de oposición y de cancelación. Este último consiste en el derecho que tiene el afectado a suprimir ya sea del contenido de alguna página de *Internet* o de la lista de resultados obtenida de una búsqueda a partir de su nombre en un buscador. Por su

[293] *Ib.*, numeral 92.

[294] Numeral 99 de la STJUE, de 13 de mayo de 2014: « *De las consideraciones anteriores se desprende que procede responder a la tercera cuestión prejudicial que los artículos 12, letra b), y 14, párrafo primero, letra a), de la Directiva 95/46 deben interpretarse en el sentido de que, al analizar los requisitos de aplicación de estas disposiciones, se tendrá que examinar, en particular, si el interesado tiene derecho a que la información en cuestión relativa a su persona ya no esté, en la situación actual, vinculada a su nombre por una lista de resultados, obtenida tras una búsqueda efectuada a partir de su nombre, sin que la apreciación de la existencia de tal derecho presuponga que la inclusión de la información en cuestión en la lista de resultados cause un perjuicio al interesado. Puesto que éste puede, habida cuenta de los derechos que le reconocen los artículos 7 y 8 de la Carta, solicitar que la información de que se trate ya no se ponga a disposición del público en general mediante su inclusión en tal lista de resultados, estos derechos prevalecen, en principio, no sólo sobre el interés económico del gestor del motor de búsqueda, sino también sobre el interés de dicho público en acceder a la mencionada información en una búsqueda que verse sobre el nombre de esa persona. Sin embargo, tal no sería el caso si resultara, por razones concretas, como el papel desempeñado por el interesado en la vida pública, que la injerencia en sus derechos fundamentales está justificada por el interés preponderante de dicho público en tener, a raíz de esta inclusión, acceso a la información de que se trate*».

parte, el derecho de oposición consistiría en oponerse al tratamiento de nuestros datos o a solicitar el cese del tratamiento frente a algún responsable siempre que se afecte el libre desarrollo de la persona solicitante.

El derecho al olvido se crea a partir del haber jurisprudencial reconociéndoles a los interesados el derecho a cancelar sus datos y oponerse al tratamiento de sus datos personales si estos se encuentran en una lista de resultados obtenida por medio de una búsqueda realizada por su nombre haciendo uso de los servicios proporcionados por un el motor de búsqueda y que le causen perjuicio al mismo y hecha la ponderación de los intereses entre los del buscador y los derechos y libertades fundamentales reconocidos a nivel comunitario a favor de los interesados, lo anterior, siempre y cuando no se trate de un personaje de relevancia pública debido al contenido del derecho a la información, como resultado podrán las personas afectadas solicitar que los datos que le afecten ya no se pongan a disposición del público mediante su inclusión en la lista de resultados.

Este derecho atiende a necesidades reales de nuestro tiempo ya que como establece MARTÍNEZ CABALLERO: «*Grabar, guardar, almacenar información es muy barato y, por el contrario, borrar información exige dedicación, tiempo y dinero*»[295] por lo que «*las personas no deben soportar que sus datos permanezcan de manera atemporal en los motores de búsqueda*»[296], ya que estos últimos pueden «*generar una multiplicación sin límites de la información, la dotan de un carácter "cuasi eterno" que puede alterar la línea del tiempo*»[297], de manera que si la información que indexan puede dañar los derechos de los individuos, también podrá serlo la información albergada en otro tipo de fuente digital, como las redes sociales o los medios periodísticos digitales[298].

---

[295] MARTÍNEZ CABALLERO, J., «Cómo conjugar el derecho al olvido», *Revista Jurídica de Castilla-La Mancha*, núm. 57, 2015, p. 145.

[296] SUÁREZ VILLEGAS, J.C., «El derecho al olvido, base de tutela de la intimidad. Gestión de los datos personales en la Red», *Telos: Cuadernos de comunicación e innovación*, núm. 97 (en línea) 2014, p. 39. Disponible en: https://telos.fundaciontelefonica.com/url-direct/pdf-generator?tipoContenido=articuloTelos&idContenido=2014042310020002&idioma=es (consulta: 19 de junio de 2017).

[297] RALLO LOMBARTE, A., «El Derecho al olvido y su protección a partir de la protección de datos», *Telos: Cuadernos de comunicación,* núm. 85, 2010, p. 105.

[298] MATE SATUÉ, L.C., «¿Qué es realmente el Derecho al Olvido?», *Revista de Derecho Civil*, núm. 2, vol. 3, (abril-junio), 2016, p. 192.

4.2 Configuración normativa del derecho al olvido.

El nuevo RGPD ha introducido en su art. 17 el denominado derecho de supresión y se ha colocado entre paréntesis «el derecho al olvido». Sin embargo, durante la elaboración del RGPD se plantearon otras propuestas que van a ser analizadas. El derecho al olvido inicialmente se preveía en la propuesta presentada por la Comisión en los considerandos 53 y 54. En el considerando 53 se habla del ejercicio de este derecho en cuatro supuestos: 1) cuando ya no fuesen necesarios para los fines para los que fueron recogidos, 2) cuando los interesados retirasen su consentimiento, 3) cuando los interesados se opusieran al tratamiento de sus datos personales, y 4) cuando no se ajustase a lo dispuesto por el RGPD; dentro de este considerando también se prevé «la posterior conservación» autorizada debido a los fines perseguidos como la investigación histórica, estadística y científica, «*por razones de interés público en el ámbito de la salud pública, para el ejercicio del derecho de libertad de expresión, cuando la legislación así lo exija, o en caso de que existan motivos para restringir el tratamiento de los datos en vez de proceder a su supresión*». Continua en el considerando siguiente diciendo que «*a fin de reforzar el "derecho al olvido" en el entorno en línea, el derecho de supresión también debe ampliarse de tal forma que los responsables del tratamiento que hayan hecho públicos los datos personales deben estar obligados a informar a los terceros que estén tratando los datos de que un interesado les solicita que supriman todo enlace a tales datos personales, o las copias o réplicas de los mismos. Para garantizar esta información, el responsable del tratamiento debe tomar todas las medidas técnicas razonables, incluidas las de carácter técnico, en relación con los datos cuya publicación sea de su competencia. En relación con la publicación de datos personales por un tercero, el responsable del tratamiento debe ser considerado responsable de la publicación, en caso de que haya autorizado la publicación por parte de dicho tercero*». Sin embargo, en la versión final del RGPD, este derecho se prevé en los considerandos 65 y 66, manteniendo estos cuatro supuestos para su ejercicio, y se añade a los supuestos de retención mencionados el de «*ejercicio o la defensa de reclamaciones*». Prácticamente el considerando 66 del RGPD queda igual, con la salvedad de que en vez de hablar de terceros se hace referencia a los responsables cuando el responsable inicial haya hecho públicos los datos de los interesados, lo anterior atiende a razones de

coherencia ya que, el RGPD prevé como responsable a «*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*»[299], siguiendo con esta idea, al final en el texto definitivo señala como responsables a esos terceros que tratan datos como consecuencia de esa publicación, ya que estos determinan también los fines y los medios de ese tratamiento posterior.

Desde la propuesta del texto del art. 17 hasta su publicación definitiva sufrió varios cambios tanto en la redacción como en el fondo. El apartado 1 hacía mención expresa a la obligación del responsable de abstenerse de la difusión de datos personales que hayan sido proporcionados por los interesados siendo niños, sin embargo, en la versión final se elimina. En este mismo apartado se señalan las circunstancias que deben concurrir para que se supriman los datos personales del interesado (en ambas versiones se establece de esta manera); se modifica el inciso b) que trata acerca de la retirada de datos, cuando el interesado retire su consentimiento, en este caso se elimina en la versión definitiva la frase que se contenía en la propuesta: «o ha expirado el plazo de conservación», ya que la «expiración» en sí misma no supone la retirada del consentimiento del interesado. Para que la retirada del consentimiento sea válida debe ser la base de licitud del tratamiento conforme a los establecido en el art. 6.1.a) del RGPD o si el interesado lo ha otorgado para el tratamiento de datos de categorías especiales, de acuerdo con el art. 9.2.a) del reglamento. El inciso c) del art. 17 preveía como motivo para la supresión la oposición del interesado. Se añade en la versión final que se suprimirá esta información siempre que no prevalezcan «otros motivos legítimos para el tratamiento» del responsable. En este apartado se incluyen otros tres supuestos para la supresión de la información en los incisos d), e) y f): «*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*

[299] Art. 4.7 del RGPD.

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 art. 8.1». En relación con estos tres supuestos es necesario señalar lo siguiente, la propuesta de reglamento elimina de su epígrafe d) lo relativo a la supresión de los datos personales si el tratamiento no fuese conforme al Reglamento, ahora en este inciso solo se hace referencia a la licitud del tratamiento. El último inciso integra lo que se incluía en el apartado 1 ya que el art. 8.1 hace referencia a las condiciones del consentimiento otorgado por los menores de edad.

En el apartado 2 del art. 17 se establecía de manera inicial que el responsable en caso de haber hecho públicos los datos personales del interesado debía adoptar las medidas con la finalidad de informar a terceros sobre la supresión. En la versión definitiva la adopción de esas medidas se hará «*teniendo en cuenta la tecnología disponible y el coste de su aplicación*».

El apartado 3 del mismo artículo tanto inicialmente como en la versión definitiva, excluye la aplicación de lo establecido en los apartados anteriores, es decir, la supresión siempre y cuando se realicen determinados supuestos. El inciso a) de este artículo no sufre modificaciones sustanciales y queda redactado de este modo: «*para ejercer el derecho a la libertad de expresión*». En los incisos b) y c) de la propuesta se preveían motivos de interés público como la salud, la investigación histórica, estadística y científica, circunstancias genéricas que limitan el ejercicio de este y de los demás derechos de acuerdo con el actual art. 89 (garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos). En la versión definitiva se traslada a los incisos c) y d) añadiéndose como motivo de interés público la finalidad archivística. En cuanto al inciso b) de la versión definitiva se añade como motivo de exclusión el cumplimiento de una obligación legal o en cumplimiento de un interés público o en ejercicio de los poderes conferidos al responsable, determinado por el derecho de la Unión o por el del Estado miembro. Estos supuestos se relacionan con las bases de licitud establecidas en el art. 6.1. c) y e), los cuales normalmente son las bases de licitud que utilizan las autoridades públicas y que legitiman dicho tratamiento de datos. Finalmente, el inciso e) de la propuesta que preveía la

limitación del tratamiento como motivo para su supresión se sustituye por «*la formulación, el ejercicio o la defensa de reclamaciones*», relacionado con el derecho legítimo de los interesados de hacer valer sus derechos y a defenderse. El apartado 4 en la redacción de la propuesta preveía la limitación del tratamiento, sin embargo, en la redacción definitiva del RGPD este supuesto se traslada al art. 18, el cual prevé a esa limitación como otro derecho que tienen los interesados.

Es necesario señalar que previamente a la publicación del RGPD, el GT29 elaboró unas Directrices para la ejecución de la STJUE de 13 de mayo de 2014. En su apartado 9 había establecido como norma general que los motores de búsqueda no debían realizar ninguna información a los *webmaster* de las páginas web donde se albergaba la información afectada por la supresión al no haber un fundamento legal en el marco de la legislación en la materia [300]. Sin embargo, en el nuevo RGPD, específicamente, el apartado segundo de este nuevo art. 17, sí prevé como obligación de los responsables que han hecho públicos los datos, informar a otros responsables que estén tratando los datos personales sobre la solicitud del ejercicio del derecho de supresión en relación con algún enlace o contenido, debiendo de tomar en cuenta «*la tecnología disponible y el coste de su aplicación*». Si atendemos a la literalidad de esta parte del precepto, serán los motores de búsqueda y los editores de las páginas dónde se alberga la información que se ha hecho pública, quienes tengan que informar, teniendo en cuenta sus medios tecnológicos, a otros responsables. En relación a esta cuestión muy acertadamente la Profesora ÁLVAREZ CARO señala que: «*se deduce que, para cumplir con la obligación de tomar medidas razonables, teniendo en cuenta la tecnología y medidas técnicas, con el fin de informar a otros responsables que estén tratando datos, cabría entender que la utilización de protocolos de exclusión*

[300] El numeral 9 literalmente establece que: «*9. Communication to website editors on the de-listing of specific links Search engines should not as a general practice inform the webmasters of the pages affected by de-listing of the fact that some web pages cannot be acceded from the search engine in response to a specific name-based query. There is no legal basis for such routine communication under EU data protection law. In some cases, search engines may want to contact the original editor in relation to particular request prior to any de-listing decision, in order to obtain additional information for the assessment of the circumstances surrounding that request. Taking into account the important role that search engines play in the dissemination and accessibility of information posted on the Internet and the legitimate expectations that webmasters may have with regard to the indexing and presentation of information in response to users' queries, the Article 29 Working Party (hereinafter: the Working Party) strongly encourages the search engines to provide the de-listing criteria they use, and to make more detailed statistics available*» *vid.* Directrices de ejecución de la STJUE de 13 de mayo de 2014 Disponibles en: https://www.pdpjournals.com/docs/88377.pdf (consulta: 18 de octubre de 2019).

(robot.txt) es un mecanismo válido para dar cumplimiento a dicha obligación»[301], ya que como lo establecía el Abogado general Sr. NIILO JÄÄSKINEN en el punto 41 de sus conclusiones de fecha 25 de junio de 2013 en el caso de Mario Costeja, AEPD v. Google, que «*las páginas web fuente se almacenan en servidores de alojamiento conectados a Internet. El editor de páginas web fuente puede utilizar "códigos de exclusión" para el funcionamiento de los motores de búsqueda de Internet. Los códigos de exclusión recomiendan a los motores de búsqueda que no indexen o almacenen una página web fuente, o que no la muestren en los resultados de la búsqueda. Su uso indica que el editor no desea que determinada información de la página web fuente pueda ser recuperada para su difusión a través de motores de búsqueda*», sin embargo, también estos códigos de exclusión se utilizan por los motores de búsqueda en su actividad exactamente «*el proveedor de servicios de motor de búsqueda en Internet controla su índice, en el sentido de que decide si los códigos de exclusión de la página web fuente han de cumplirse o no*»[302], así que siguiendo esta posición podríamos concluir en este caso específico que no bastaría con la aplicación de estos códigos de exclusión por parte del *webmaster*, sino que el propio motor de búsqueda los hiciera efectivos también.

En relación con lo previsto en el art. 17 del RGPD y con el análisis previo a la sentencia del TJUE de 13 de mayo de 2014, es importante señalar que el denominado derecho al olvido como lo concibió el TJUE no se ha plasmado como tal en el contenido de este artículo, más bien se hace un desarrollo más exhaustivo del derecho de supresión tomando como base el hasta entonces denominado derecho de cancelación antes previsto en el art. 12.b) de la Directiva 95/46/CE y en parte el derecho de oposición previsto en el art. 14 de la misma Directiva, pero desarrollando las causas para el ejercicio de este derecho y las excepciones para su aplicación. Este derecho de supresión es más extenso en cuanto al contenido que se desea suprimir, no solo se pueden eliminar enlaces de la lista de resultados del motor de búsqueda

[301] ÁLVAREZ CARO, M., «El derecho a la supresión o al olvido», PIÑAR MAÑAS, J. L. (Dir.). *Reglamento General de Protección de Datos Personales. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, p. 250.

[302] Apartado 91 de las Conclusiones del Abogado general de 25 de junio de 2013, disponibles en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=617784#Footref69 (consulta: 23 de octubre de 2019), ECLI:EU:C:2013:424.

hechas a partir del nombre, se entiende de la literalidad de este artículo que se podrán borrar todos aquellos datos entendidos como «*toda información sobre una persona física identificada o identificable (…); se considerará persona física identificable toda persona 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*»[303]. No solo será ejercitable frente a los motores de búsqueda como señalaba la sentencia, podrá ser ejercitable frente a «*la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento*». Tal y como lo apunta ÁLVAREZ CARO «*vemos como el texto normativo es mucho mayor, pues se traduce en una obligación de supresión para todo responsable del tratamiento, en determinadas circunstancias, no quedando sólo circunscrito ni mucho menos a motores de búsqueda en Internet como en el caso de la sentencia en el caso Mario Costeja AEPD v. Google*»[304], podrá ser ejercido en un entorno en línea frente a cualquier responsable de los servicios de la sociedad de la información, entendido como tal a «*todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios. A efectos de la presente definición se entenderá por: i) "a distancia", un servicio prestado son que las partes estén presentes simultáneamente, ii) "por vía electrónica", un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transcribe, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético, iii) "a petición individual de un destinatario de servicios", un servicio prestado mediante transmisión de datos a petición individual*»[305], sin exclusión de los que se

[303] Art. 4.1 del RGPD.
[304] ÁLVAREZ CARO, M., *op. cit.,* pp. 242-243.
[305] Art. 1.1.b) de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (versión codificada).

prestan sin remuneración alguna como contraprestación como las redes sociales, los blogs, los medios electrónicos abiertos, etc.

Ahora bien, como ya se ha señalado el derecho de supresión se incorpora en la nueva LOPDGDD en su art. 15, en los términos establecidos en el art. 17 del RGPD de la siguiente forma: «*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*». Sin embargo, en esta nueva LO también se prevé en su art. 93 «el derecho al olvido en búsquedas de internet», cuyo contenido es más próximo al de la STJUE de 13 de mayo de 2014, y que al tenor literal establece: «*1. Toda persona tiene derecho a que los motores de búsqueda en Internet eliminen de las listas de resultados que se obtuvieran tras una búsqueda efectuada a partir de su nombre los enlaces publicados que contuvieran información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información. Del mismo modo deberá procederse cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los enlaces por el servicio de búsqueda en Internet. Este derecho subsistirá aun cuando fuera lícita la conservación de la información publicada en el sitio web al que se dirigiera el enlace y no se procediese por la misma a su borrado previo o simultáneo. 2. El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho*»[306].

Es menester señalar que el legislador español ha querido matizar el contenido del art. 17 del RGPD, que si bien es un derecho genérico y universal ejercitable frente a los responsables que han publicado la información que

[306] PUENTE, A., *op. cit.,* p 204.

identifique o haga identificable al interesado, no traslada de manera íntegra lo que el TJUE ha determinado como «derecho al olvido», esta matización se realiza en el art. 93 de la LOPDGDD, en dónde se establece un derecho al olvido en búsquedas de internet a modo de la STJUE de 13 de mayo de 2014, pues es ejercitable frente a los motores de búsqueda cuyo parámetro de búsqueda sea el nombre del interesado y que se pretenda la eliminación por contener «información relativa a esa persona cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información» [307]. También se señala que este derecho «subsistirá» aunque la información haya sido inicialmente publicada de forma lícita y no se proceda a su eliminación, como, por ejemplo, cuando la información sea publicada en los portales de internet o en las sedes electrónicas de las Administraciones públicas como parte de un trámite de publicidad dentro de un procedimiento administrativo específico, tal y como en el caso de *Google* vs. Mario Costeja. Otro ejemplo se daría cuando la información esté amparada por el Derecho a la información del art. 20 CE. Finalmente, el apartado 2 de este artículo establece que «*El ejercicio del derecho al que se refiere este artículo no impedirá el acceso a la información publicada en el sitio web a través de la utilización de otros criterios de búsqueda distintos del nombre de quien ejerciera el derecho*», es decir, que se podrán utilizar otros criterios de búsqueda que no sea el nombre para legitimar la prevalencia de la información en el sitio web y que tiene que ver con el contenido de la STC 58/2018, de 4 de junio de 2018, que será analizada más tarde [308]. De todo ello, se deduce que el legislador integra el contenido de la jurisprudencia comunitaria y nacional para proyectarlo en el contenido de este artículo.

No solo el art. 93 completa el derecho de supresión del art. 17, creando en el ámbito nacional un derecho para los interesados. El art. 94 también crea un nuevo derecho al olvido, específicamente ejercitable frente a los prestadores de servicios de «redes sociales y servicios equivalentes», con especial referencia a los datos

[307] Cfr. Art. 93.1 de la LOPDGDD.
[308] Cfr. en la página 151.

personales sobre menores y se exceptúa como lo hace el RGPD, a aquellas situaciones en el ámbito doméstico[309].

4.3 Interpretación doctrinal y jurisprudencial.

Es innegable que el «derecho al olvido» o mejor dicho «derecho de supresión» es parte del derecho a la protección de datos personales, por tanto, también es un instrumento para la protección de otros derechos fundamentales contenidos en la CDFUE y en la CE, principalmente el derecho a la vida privada y familiar de las personas contemplado en el art. 7 de la CDFUE, y el derecho de libertad de expresión e información establecido en el art. 11 de la Carta, correlativamente contemplados en los artículos 18.1 y 20.1 de la CE.

SIMÓN CASTELLANO, en España, encuentra su fundamento en el derecho a la protección de datos de carácter personal, previsto en el art. 18.4 CE[310] y en el valor de la dignidad de las personas contemplada en el art. 10.1 CE[311]. Esta categorización se lleva a cabo tomando en cuenta el contenido de la propia sentencia del TJUE, y el contenido de los derechos en nuestro sistema jurídico español, en donde se prevé la protección de datos personales y la dignidad como punto de partida, debido a la relevancia de su carga axiológica constitucional. El reconocimiento de esta manifestación del derecho a la protección de datos *«nace como un derecho a la autodeterminación informativa, esto es, un derecho a tener el control sobre tus datos personales – habeas data- a decidir cuáles pueden ser tratados y consultados por ojos extraños. Y la autodeterminación informativa, consciente y responsable es una*

---

[309] Literalmente este artículo establece que: «*1. Toda persona tiene derecho a que sean suprimidos, a su simple solicitud, los datos personales que hubiese facilitado para su publicación por servicios de redes sociales y servicios de la sociedad de la información equivalentes. 2. Toda persona tiene derecho a que sean suprimidos los datos personales que le conciernan y que hubiesen sido facilitados por terceros para su publicación por los servicios de redes sociales y servicios de la sociedad de la información equivalentes cuando fuesen inadecuados, inexactos, no pertinentes, no actualizados o excesivos o hubieren devenido como tales por el transcurso del tiempo, teniendo en cuenta los fines para los que se recogieron o trataron, el tiempo transcurrido y la naturaleza e interés público de la información. Del mismo modo deberá procederse a la supresión de dichos datos cuando las circunstancias personales que en su caso invocase el afectado evidenciasen la prevalencia de sus derechos sobre el mantenimiento de los datos por el servicio. Se exceptúan de lo dispuesto en este apartado los datos que hubiesen sido facilitados por personas físicas en el ejercicio de actividades personales o domésticas. 3. En caso de que el derecho se ejercitase por un afectado respecto de datos que hubiesen sido facilitados al servicio, por él o por terceros, durante su minoría de edad, el prestador deberá proceder sin dilación a su supresión por su simple solicitud, sin necesidad de que concurran las circunstancias mencionadas en el apartado 2*».

[310] SIMÓN CASTELLANO, P., *op. cit.*, pp. 137-153.

[311] *Ib.*, pp. 117-124.

manifestación directa de la integridad moral del ser humano, que frente a la ingente memoria digital exime el control de los datos personales en aras de permitir el libre desarrollo de la vida conforma a las convicciones, creencias y principios que cada uno escoja»[312]. El derecho al olvido tiene que ser acorde y respetuoso con otros derechos como los de expresión e información, por lo que se deberá llevar a cabo una ponderación de derechos al caso concreto si estos colisionan. PERE SIMÓN en relación con lo establecido en la STJUE de 12 de mayo de 2014, determina que: *«En caso de conflicto entre bienes jurídicos que la normativa europea protege y reconoce -principio de transparencia y derecho a la protección de datos-, el TJUE entiende que debe aplicarse el principio de Proporcionalidad, que exige en todo caso, que los medios empleados permitan alcanzar "el objetivo que éste persigue y no vayan más allá de lo que es necesario para alcanzarlo"»*[313]*.*

Desde mi perspectiva el derecho al olvido no cuenta con una esfera jurídica y protección propia, este constituye una manifestación del derecho a la protección de datos personales, coincidiendo con MATÉ SAUTÉ[314] y MARTÍNEZ CABALLERO[315]. Por otra parte, ÁLVAREZ CARO determina que el Derecho al olvido tiene su origen en el derecho a la intimidad y en el de protección de datos personales: *«El derecho al olvido encuentra sus raíces en el derecho a la intimidad (the rigth to privacy en su denominación en inglés) y en el derecho a la protección de datos personales, pudiendo considerarse que el derecho al olvido deriva de ellos»*[316]*.* Hay quienes afirman de manera tajante que el TJUE «*no se refiere al "derecho al olvido" como un nuevo derecho, sino que engarza el derecho del individuo a que no sean accesibles determinados contenidos obtenidos en búsquedas realizadas a través de motores a*

[312] *Ib.*, pp. 119- 120.
[313] *Ib.*, pp. 154.
[314] «*El fundamento del derecho al olvido tiene su base en el derecho a la protección de datos reconocido constitucionalmente de forma generalista en el apartado 4 del artículo 18 de la Constitución Española»* Cfr. MATE SATUÉ, L.C., *op. cit.,* p. 189.
[315] «*A la hora de conjugar el derecho al olvido, en lugar de optar por configurarlo como derecho autónomo, existen dos alternativas: bien construirlo corno proyección de los derechos a la intimidad y al honor; bien como proyección del derecho a la protección de datos de carácter personal. La primera alternativa ha sido la admitida por la doctrina y la jurisprudencia española en relación con los medios tradicionales de comunicación, pero que también puede extenderse a las formas de divulgación on line de la información. La segunda es la adoptada por la Comisión Europea a la luz de la propuesta del Reglamento general de protección de datos»*, Cfr. MARTÍNEZ CABALLERO, J., *op. cit.,* p. 156.
[316] ÁLVAREZ CARO, M., *Derecho al Olvido en Internet: El nuevo paradigma de la privacidad en la era Digital,* Madrid, Reus, 2015, p.27.

partir de su nombre y apellidos con el derecho fundamental a la protección de datos de carácter personal y el, en la terminología del Tribunal Constitucional español, haz de facultades que el mismo implica»[317] tal y como lo establece el TC por Sentencia 292/2000, de 30 de noviembre, este «*haz de facultades*» puede traducirse «*en su mayor parte en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos*»[318]. En este mismo sentido ÁLVAREZ CARO determina que «*no se trata de un nuevo derecho, si no de una manifestación de un derecho ya existente, en un entorno muy concreto. En este sentido, se trataría de la manifestación del derecho a la cancelación de datos en el entorno de Internet*»[319]. La AEPD considera que *«El derecho de supresión ('derecho al olvido') hace referencia al derecho a impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información)»* [320].

Además, en cuanto a su denominación, y a la posición del Parlamento Europeo en la primera lectura de la entonces propuesta del RGPD eliminaba del considerando 53 y 54 el término «olvido» sustituyéndolo por «supresión»[321], incluso no se utiliza el término de derecho al olvido en un documento posterior a la sentencia titulado «Directrices sobre la aplicación del Tribunal de Justicia de la Unión Europea "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) y Mario Costeja González C-131/12"» en su versión en inglés se utiliza el

[317] PUENTE, A., *op. cit.,* p. 192.
[318] F.J. 5 de la STC (Pleno) 292/2000, de 30 de noviembre (ECLI:ES:TC:2000:292).
[319] ÁLVAREZ CARO, M., «El derecho (…)», *op. cit.,* p. 242.
[320] Definición sacada de la página de internet de la AEPD Disponible en: http://www.agpd.es/portalwebAGPD/CanalDelCiudadano/derecho_olvido/index-ides-idphp.php (consulta: 19 de junio de 2017).
[321] Cfr. Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM (2012)0011 – C7-0025/2012 – 2012/0011(COD)), Procedimiento legislativo ordinario: primera lectura. Disponible en: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//ES (consulta 17 de octubre de 2019).

término «*deslisting*», «*que podría traducirse como supresión o borrado o retirada de la información de la lista de resultados del motor de búsqueda, más acorde con la naturaleza del derecho consagrada por el tribunal*»[322]. Ocurre lo mismo incluso cuando el idioma de trabajo es el francés, de hecho, es el propio TJUE que utiliza términos como «desreferenciación»[323] o «borrado»[324] en la reciente sentencia del TJUE de 24 de septiembre de 2019 en su numeral 46[325].

Respecto a la interpretación jurisprudencial en España sobre el Derecho al olvido, fue la propia AN por Sentencia de 29 de diciembre de 2014, el primer Tribunal español en emitir una resolución relacionada con el Derecho al olvido. En esta sentencia, la AN define al Derecho al olvido, como *«el poder de disposición del particular sobre las informaciones que se publican en la red sobre su persona»*[326]y realiza una ponderación entre los derechos de la personalidad y protección de datos en relación con el derecho de expresión y el de información y comunicación aplicada al caso concreto concluyendo que los *«anuncios en dos páginas web del periódico "La Vanguardia"(…) relativos a una subasta inmobiliaria vinculada a un embargo por deudas a la Seguridad Social del reclamante, sin que tenga ninguna relevancia el interesado en la vida pública que justificara que prevaleciera el interés del público general dicho dato personal sobre los derechos reconocidos en los artículos 7 y 8 de la Carta Europea de Derechos Fundamentales»*[327], por tanto, se estimó el recurso presentado por la persona afectada basándose en que esta *«tiene derecho a que la información sobre a una subasta de inmuebles relacionada con un embargo derivado de deudas a la Seguridad Social ya no esté vinculada a su nombre por una lista de resultados obtenida tras una búsqueda efectuada a partir de sus datos personales»*[328].

---

[322] PUENTE, A., *op. cit.,* pp. 213-214.
[323] La sentencia habla de un desreferenciamiento en los siguientes términos: «*droit au déréférencement de la personne*», *vid.* http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=7103394 (consulta: 23 de octubre de 2019).
[324] Literalmente hace referencia a el «derecho al borrado», trad. del francés: *le « droit à l'effacement*», Cfr. STJUE de 24 de septiembre de 2019. Disponible en: http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=7103394 (fecha de consulta: 23 de octubre de 2019).
[325] STJUE de 24 de septiembre de 2019 (TJCE 2019\203; ECLI:EU:C:2019:772).
[326] F.D. 12º, de la SAN, de 29 de diciembre de 2014 (RJCA 2014\1065; ECLI: ES:AN:2014:5129).
[327] F.D. 14º, de la SAN, de 29 de diciembre de 2014 (RJCA 2014\1065; ECLI: ES:AN:2014:5129).
[328] *Íd.*

De acuerdo con una búsqueda realizada por medio de palabras clave entrecomilladas "derecho al olvido" en el "buscador de jurisprudencia" del Centro de documentación judicial (CENDOJ) perteneciente al Consejo General de Poder Judicial arroja que se dictaron un buen número de sentencias por la Sala de lo contencioso de la Audiencia Nacional. En el año 2014: 34, 2015: 46, 2016: 1, 2017: 9, 2018: 13 y para el 2019: 24.

En relación con los recursos resueltos en el año 2014, se estiman a favor de *Google Spain, S.L* los siguientes asuntos: 657/2009[329], 661/2009[330], 470/2010[331], 588/2010[332], 220/2011[333], 242/2011[334], 490/2012[335], 25/2013[336] y 355/2013[337]. La información que se pretendía eliminar del buscador y por la cual se derivaba el ejercicio del derecho de supresión era insuficiente para realizar una ponderación de derechos. En la resolución de todos estos asuntos se siguió esta línea argumental: «*dichos datos suministrados por la interesada resultan insuficientes para determinar la naturaleza de la información y su carácter sensible para la vida privada de la afectada, bien por no resultar necesarios los mismos en relación con los fines para los que se recogieron, bien por otras razones, siendo imposible con el contenido de la información que consta en las actuaciones realizar la ponderación de intereses en conflicto*» [338]. De manera parcial se estima por sentencia 70/2015 el recurso 587/2010 presentado por *Google Spain* S.L. a su favor, pues determina la sala que la resolución recurrida «*no es afortunada, pues insta a Google Spain, S.L. para que "adopte las medidas necesarias para retirar los datos de su índice e imposibilite el acceso futuro a los mismos". Tan confusa redacción genera serias dudas sobre el alcance de lo así acordado y las concretas obligaciones impuestas a Google (…) Por ello, la obligación impuesta por la resolución recurrida a Google Spain, S.L. debe interpretarse en el sentido de que debe adoptar las medidas necesarias para retirar o*

[329] SAN de 29 diciembre de 2014 (JUR 2015\27215; ECLI:ES:AN:2014:5210).
[330] SAN de 29 diciembre de 2014 (JUR 2015\26747; ECLI:ES:AN:2014:5198).
[331] SAN de 29 diciembre de 2014 (JUR 2015\59185; ECLI: ES:AN:2014:5251).
[332] SAN de 29 diciembre de 2014 (JUR 2015\58789: ECLI:ES:AN:2014:5249).
[333] SAN de 29 diciembre de 2014 (JUR 2015\26253; ECLI:ES:AN:2014:5211).
[334] SAN de 30 de diciembre de 2014 (JUR 2015\59844; ECLI:ES:AN:2014:5248).
[335] SAN de 30 de diciembre de 2014 (JUR 2015\58115; ECLI:ES:AN:2014:5243).
[336] SAN de 29 de diciembre de 2014 (RJCA 2015\183; ECLI:ES:AN:2014:5202).
[337] SAN de 30 de diciembre de 2014 (JUR 2015\57618; ECLI:ES:AN:2014:5241).
[338] F.D. 9 de la Sentencia de fecha 29 de diciembre de 2014, recaída al recurso 220/2011 (JUR 2015\26253; ECLI: ECLI:ES:AN:2014:5211).

eliminar de la lista de resultados, obtenida tras una búsqueda efectuada a partir del nombre del reclamante, los vínculos a las páginas web objeto de reclamación»[339]. En vista del análisis de las sentencias referidas anteriormente, se puede inferir que la mayoría de los recursos contencioso-administrativos se presentan por *Google Spain S.L.*, y que los recursos estimados por sentencia obtienen este resultado por errores formales en el recurso, pues por la falta de información no se puede realizar la ponderación de derechos a la luz de la entonces Directiva 95/46/CE y de lo determinado por la STJUE de 13 de mayo de 2014.

En el año 2015 se estiman en sentencia ocho de los cuarenta y seis recursos presentados: SSAN 60/2015[340], 61/2015[341], 88/2015[342], 98/2015[343], 104/2015[344], 240/2015[345], 341/2015[346], 425/2015[347], parcialmente se estiman dos: SSAN 82/2015[348] y 107/2015[349], de todos estos recursos son tres los que se presentan por particulares como parte demandante. En este año casi de manera idéntica al anterior, se estiman los recursos contencioso-administrativos que no aportan información suficiente para determinar la afectación del derecho a la protección de datos y realizar una ponderación de derechos[350], o aquellos en los cuales la información señalada para el ejercicio del derecho de cancelación es demasiado amplia y ambigua de tal manera que no se puede determinar «*su relevancia a la hora de efectuar la ponderación de los intereses en juego*»[351]; solo en dos de los casos estimados (SSAN 341/2015 y 425/2015) se realiza una ponderación de derechos entre el de protección de datos personales, específicamente de los derechos de

[339] F.D. 13º de la SAN 70/2015, de 29 de diciembre de 2014 (JUR 2015\68260; ECLI: ECLI:ES:AN:2014:5252).
[340] SAN de 3 de febrero de 2015 (JUR 2015\58568; ECLI:ES:AN:2015:344).
[341] SAN de 3 de febrero de 2015 (JUR 2015\58992;ECLI:ES:AN:2015:342).
[342] SAN de 12 de febrero de 2015 (JUR 2015\88275; ECLI:ES:AN:2015:643).
[343] SAN de 19 de febrero de 2015 (JUR 2015\88582; ECLI:ES:AN:2015:622).
[344] SAN de 19 de febrero de 2015 (JUR 2015\89367; ECLI:ES:AN:2015:649).
[345] SAN de 9 de junio de 2015 (RJCA 2015\842: ECLI:ES:AN:2015:2149).
[346] SAN de 2 de octubre de 2015 (RJCA 2015\869; ECLI:ES:AN:2015:3501).
[347] SAN de 6 de octubre de 2015 (JUR 2016\14341; ECLI: ES:AN:2015:4456).
[348] SAN de 24 de febrero de 2015 (JUR 2015\82308; ECLI:ES:AN:2015:568).
[349] SAN de 17 de febrero de 2015 (JUR 2015\89705; ECLI:ES:AN:2015:661).
[350] Por ejemplo, en el F.D. 9º de la SAN 61/2015 (JUR 2015\58992; ECLI:ES:AN:2015:342), se determina por la Sala que: «*no se hace ninguna referencia a cuál era el contenido de la información a la que dirigían, ni cuál era la información que facilitaban; tampoco se conoce cuáles eran las circunstancias personales del denunciante por lo que tampoco era posible conocer su posible relevancia a la hora de efectuar la ponderación de los intereses en juego*».
[351] F.D. 7º de la SAN 60/2015, de 3 de febrero de 2015 (JUR 2015\58568; ECLI:ES:AN:2015:344).

cancelación y oposición en relación con el derecho a la libertad de información. Respecto a las sentencias parcialmente estimatorias, se concede la petición de retirada de datos del índice de indexación en búsquedas realizadas a partir del nombre del interesado.

En el año 2016 se resuelve un recurso contencioso-administrativo por sentencia 562/2016 [352], la relevancia de esta resolución radica en hacer una diferenciación de la responsabilidad de *Google Spain S.L* y *Google Inc*., siguiendo la doctrina de la Sala Tercera del Tribunal Supremo relacionada con el tema desde el 11 de marzo de ese año, la cual toma en cuenta lo establecido así en el RGPD, y considera que no hay una corresponsabilidad por parte de *Google Spain S.L*, ya que para ello sería necesario que su actividad estuviese directamente relacionada con la indexación y almacenamiento de datos [353] y debido a que *Google Spain S.L*. no determina los fines ni los medios del tratamiento de datos, sin embargo, sí que considera como responsable a *Google Inc*. en consonancia con lo establecido en la STJUE de 13 de mayo de 2014. A partir de este momento ante la AN se persona como responsable Google Inc., ya no más *Google Spain S.L*. que es la entidad que gestiona los espacios publicitarios.

En el año 2017 de las nueve sentencias recaídas a los recursos contencioso-administrativos se estiman dos: rec. núm. 1797/2015 [354] y 30/2016 [355], en la resolución de estos se realiza una ponderación de derechos en donde prevalece el derecho a la libertad de expresión, en el F.D. 5º de la SAN de 6 de junio de 2017 se toma en cuenta para la resolución del caso concreto lo establecido en la *Guidelines on the implementatión of the Courrt of Justice of the European Unión Judgmente on "Google Spain and inc v, AEPD and Mario Costeja C-131/12*, específicamente lo relativo a la diferenciación entre lo que debe entenderse como vida privada de una persona y su vida pública o profesional: «*Hay una diferencia básica entre la vida privada de la persona y su vida pública o profesional. La disponibilidad de la información en los resultados de búsqueda deviene más aceptables cuanta menos*

[352] SAN 562/2016, de 18 de noviembre de 2016 (RJCA 2017\466; ECLI:ES:AN:2016:4713).
[353] F.D. 7º de la SAN 562/2016, de 18 de noviembre de 2016 (RJCA 2017\466; ECLI:ES:AN:2016:4713).
[354] SAN de 6 de junio de 2017 (JUR 2017\206541; ECLI:ES:AN:2017:3111).
[355] SAN de 11 de mayo de 2017 (RJCA 2017\487; ECLI:ES:AN:2017:2433).

información revele sobre la vida privada de una persona (...) es más probable que la información tenga relevancia si está relacionada con la vida profesional del interesado, pero dependerá de la naturaleza del trabajo del interesado y del interés legítimo del público en tener acceso a esa información a través de una búsqueda por su nombre"»[356], debido a que la información que se pretende obtener tiene que ver con el aspecto profesional de la misma, realizada la ponderación se determina que la información está amparada bajo el derecho a la libertad de expresión contenida en un blog publicado en el ámbito digital sobre opiniones referidas al interesado, por la «*significativa notoriedad pública en el ámbito digital, dada su condición de responsable de redes sociales e Internet de un grupo de comunicación, como es Intereconomía y que desarrollaba actividad docente en ese ámbito del marketing digital, al menos hasta el tiempo de los hechos. Por ello, existe un interés legítimo de los internautas en tener acceso a dicha publicación en cuanto pone de manifiesto críticas a su desempeño y a las prácticas digitales en dicho grupo, no es obsoleta y despierta interés en círculos del ámbito digital*»[357]. En este año se desestiman seis recursos: núm. 1568/2015[358], 4/2016[359], 114/2016[360], 119/2016[361], 190/2016[362] y 467/2016[363], y parcialmente se estima uno: rec. núm. 1842/2015[364], ordenándose eliminar un enlace a *Google Inc*., que con el tiempo ya no cumple con los principios de calidad (adecuación, pertinencia, proporcionalidad y exactitud) y por tanto carece de relevancia pública, no así otro enlace que se pretendía eliminar que hace referencia a contenido albergado en *Badoo.com*, del cual *Google Inc.* no es *webmaster*.

Antes de continuar con el haber jurisprudencial de la Sala de lo Contencioso-administrativo de la AN, es menester señalar que *Google Inc.* ya contaba desde el año 2003 con su filial europea *Google Ireland Limited*, «*y desde finales de 2018 es la*

[356] F.D. 5º de la SAN de 6 de junio de 2017 (JUR 2017\206541; ECLI:ES:AN:2017:3111).
[357] F.D. 5º de la SAN de 6 de junio de 2017 (JUR 2017\206541; ECLI:ES:AN:2017:3111).
[358] SAN de 18 de julio de 2017 (JUR 2017\206454; ECLI:ES:AN:2017:3029).
[359] SAN de 13 de julio de 2017 (JUR 2017\208178; ECLI:ES:AN:2017:3257).
[360] SAN de 25 de julio de 2017 (JUR 2017\207817; ECLI:ES:AN:2017:3260).
[361] SAN de 31 de octubre de 2017(JUR 2017\306556; ECLI:ES:AN:2017:4412).
[362] SAN de 31 de octubre de 2017 (JUR 2018\6478; ECLI:ES:AN:2017:4674).
[363] SAN de 4 de diciembre de 2017 (JUR 2018\12571; ECLI:ES:AN:2017:5091).
[364] SAN de 19 de junio de 2017 (RJCA 2017\559; ECLI:ES:AN:2017:2562).

encargada de gestionar los datos de los usuarios en Europa»[365] e incluso así lo manifiesta en su política de privacidad vigente a partir del 15 de octubre de 2019 en el apartado de «Requisitos europeos», en donde literalmente se establece que: «*Si la normativa de protección de datos de la Unión Europea es de aplicación al tratamiento de tu información, te proporcionaremos los controles que se describen en esta política para que puedas ejercitar tu derecho a solicitar el acceso a tus datos, actualizarlos, retirarlos y restringir su tratamiento. También tienes derecho a oponerte al tratamiento de tu información o a exportarla a otro servicio. El responsable del tratamiento de los datos de los usuarios con residencia habitual en el Espacio Económico Europeo o Suiza es Google Ireland Limited, a menos que se indique lo contrario en un aviso de privacidad específico de un servicio. En otras palabras, Google Ireland Limited es la entidad asociada de Google responsable del tratamiento de tus datos y del cumplimiento de las leyes sobre privacidad aplicables*»[366]. Por lo tanto y a partir de este momento la ejecución de las sentencias en el sentido de retirar enlaces de la lista de indexación del buscador de *Google* cuyos criterios sean los nombres de los interesados, se ejecutará en Europa por *Google Ireland Limited.*

Continuando con el recuento de las sentencias, para el año 2018 de las trece sentencias de la Sala de lo Contencioso de la AN, recaídas a este tipo de procedimientos se estiman once: rec. núm. 46/2016[367], 415/2016[368], 498/2016[369], 50/2017[370], 360/2017[371], 361/2017[372], 476/2017[373], 485/2017[374], 520/17[375],

[365] *Vid.* El País, Google traslada la gestión de sus pagos online de Londres a Dublín para sortear el brexit:https://cincodias.elpais.com/cincodias/2019/04/03/companias/1554294595_506135.html (consulta: 30 de octubre de 2019) y *The Irish Times, Google Ireland takes the reins for European services.* Disponible en: https://www.irishtimes.com/business/technology/google-ireland-takes-the-reins-for-european-services-1.3730721 (consulta: 30 de octubre de 2019).

[366] Políticas de privacidad de Google para Europa vigente a partir de 22 de enero según el «pdf» que se pone a disposición en la URL: https://policies.google.com/privacy, aunque en la página web se establezca que la fecha de vigencia es a partir del día 15 de octubre de 2019. Disponible en: https://www.gstatic.com/policies/privacy/pdf/20190122/f3294e95/google_privacy_policy_es_eu.pdf (consulta y descarga: 30 de noviembre de 2019).

[367] SAN de 2 de enero de 2018 (JUR 2018\64230; ECLI:ES:AN:2018:509).

[368] SAN de 27 de abril de 2018 (RJCA 2018\607; ECLI:ES:AN:2018:1929).

[369] SAN de 10 de mayo de 2018 (JUR 2018\144348; ECLI:ES:AN:2018:1932).

[370] SAN de 2 de noviembre de 2018 (JUR 2018\331762; ECLI:ES:AN:2018:4476).

[371] SAN de 11 de diciembre de 2018 (RJCA 2018\1869; ECLI:ES:AN:2018:5427).

[372] SAN de 19 de diciembre de 2018 (JUR 2019\80800; ECLI:ES:AN:2018:5432).

[373] SAN de 12 de diciembre de 2018 (RJCA 2018\1657; ECLI:ES:AN:2018:5065).

[374] SAN de 14 de diciembre de 2018 (JUR 2019\48088; ECLI:ES:AN:2018:5038).

[375] SAN de 14 de diciembre de 2018 (JUR 2019\48440; ECLI:ES:AN:2018:5045).

545/2017 [376] y, 577/2017 [377], y se desestiman dos: rec. núm. 191/2016 [378] y 406/2017 [379], las cuales fueron promovidas por particulares. Finalmente, para el año 2019 [380] de los veinticuatro recursos contencioso-administrativos, se estiman dieciséis: 88/2017 [381], 411/2017 [382], 469/2017 [383], 479/2017 [384], 491/2017 [385], 509/2017 [386], 510/2017 [387], 518/2017 [388], 519/2017 [389], 609/2017 [390], 617/2017 [391], 20/2018 [392] ,106/2018 [393], 125/2018 [394], 215/2018 [395] y 217/2018 [396]; desestimándose ocho de los recursos presentados: rec. núm. 343/2017 [397], 416/2017 [398], 468/2017 [399], 482/2017 [400], 528/2017 [401], 67/2018 [402], 477/2018 [403] y 1105/2018 [404] (FIGURA 2).

Por su parte el TS, ha tenido ocasión de pronunciarse sobre el denominado Derecho al olvido, en diversas sentencias emitidas por la Sala de lo Civil y por la Sala de lo Contencioso-Administrativo. La primera sentencia emitida por la Sala de lo civil del Tribunal Supremo es la 545/2015 de 15 octubre [405], la cual deriva de un procedimiento ordinario de defensa del derecho al honor y a la intimidad. En ella se

[376] SAN de 21 de diciembre de 2018 (JUR 2019\48876; ECLI:ES:AN:2018:5066).
[377] SAN de 27 de noviembre de 2018 (JUR 2019\26446; ECLI:ES:AN:2018:4712).
[378] SAN de 26 de enero de 2018 (JUR 2018\101897; ECLI:ES:AN:2018:1033).
[379] SAN de 26 de diciembre de 2018 (ECLI:ES:AN:2018:5064; JUR 2019\48444).
[380] Hasta el día 31 de octubre de 2018.
[381] SAN de 24 de abril de 2019 (RJCA 2019\571; ECLI:ES:AN:2019:1801).
[382] SAN 22 de enero de 2019 (JUR 2019\81313; ECLI:ES:AN:2019:507).
[383] SAN de 26 de marzo de 2019 (JUR 2019\128004; ECLI:ES:AN:2019:1120).
[384] SAN de 26 de marzo de 2019 (JUR 2019\159830; ECLI:ES:AN:2019:1549).
[385] SAN de 9 de mayo de 2019 (RJCA 2019\781; ECLI:ES:AN:2019:2766).
[386] SAN de 26 de marzo de 2019 (JUR 2019\137227; ECLI:ES:AN:2019:1329).
[387] SAN de 9 de mayo de 2019 (JUR 2019\227525; ECLI:ES:AN:2019:2764).
[388] SAN de 2 de abril de 2019 (RJCA 2019\565; ECLI:ES:AN:2019:1804).
[389] SAN de 2 de abril de 2019 (RJCA 2019\170; ECLI:ES:AN:2019:1805).
[390] SAN de 16 de mayo de 2019 (JUR 2019\189339; ECLI:ES:AN:2019:2063).
[391] SAN de 8 de enero de 2019 (JUR 2019\137033; ECLI:ES:AN:2019:1243).
[392] SAN de 13 de septiembre de 2019 (JUR 2019\278879; ECLI:ES:AN:2019:3447).
[393] SAN de 21 de junio de 2019 (JUR 2019\232080; ECLI:ES:AN:2019:2897).
[394] SAN de 15 de marzo de 2019 (JUR 2019\111973; ECLI:ES:AN:2019:782).
[395] SAN de 21 de junio de 2019 (JUR 2019\213368; ECLI:ES:AN:2019:2593).
[396] SAN de 21 de junio de 2019 (JUR 2019\231991; ECLI:ES:AN:2019:2899).
[397] SAN de 22 de abril de 2019 (RJCA 2019\317; ECLI:ES:AN:2019:1996).
[398] SAN de 14 de febrero de 2019 (JUR 2019\80463; ECLI:ES:AN:2019:514).
[399] SAN de 26 de marzo de 2019 (JUR 2019\127544; ECLI:ES:AN:2019:1117).
[400] SAN de 12 de febrero de 2019 (JUR 2019\77084; ECLI:ES:AN:2019:403).
[401] SAN de 2 de abril de 2019 (RJCA 2019\564; ECLI:ES:AN:2019:1806).
[402] SAN de 26 de febrero de 2019 (JUR 2019\123159; ECLI:ES:AN:2019:998).
[403] SAN de 24 de julio de 2019 (JUR 2019\269932; ECLI:ES:AN:2019:3348).
[404] SAN de 20 de septiembre de 2019 (JUR 2019\281494; ECLI:ES:AN:2019:3483).
[405] STS (Sala de lo Civil) 545/2015, de 15 de octubre de 2015 (RJ 2015\4417; ECLI:ES:TS:2015:4132).

realiza una ponderación entre el derecho a la libertad de expresión e información y los derechos de protección de datos y los de la personalidad, específicamente, el derecho a la intimidad y al honor. En este caso la parte demandada no es Google, si no «Ediciones El País, S.L.» por una noticia contenida en su página web, la cual corresponde a hechos publicados en el diario en el año 1985 e instalados en su hemeroteca digital desde el año 2007 de manera general y gratuita. Parte de la condena en primera instancia establece que «Ediciones El País, S.L.» debe cesar de «*inmediato a la difusión de dicha noticia, debiendo implantar las medidas tecnológicas adecuadas para impedir dicha difusión que se establecen en el suplico de la demanda y se dan por reproducidas, en aras a evitar que dicha noticia aparezca cuando se insertan los nombres y apellidos de ... en Google. (…) En concreto y como medida más importante además de las establecidas en el suplico, a introducir el comando NO INDEX, de tal manera que con tal solo esta medida, poniendo los nombres y apellidos de (...) en Google o en otro buscador no saldrá la noticia publicada en "El País" en el año 1.985*»[406]. Como era de esperar «Ediciones El País, S.L.», recurre la sentencia. En segunda instancia la sección 14ª de la Audiencia Provincial de Barcelona por sentencia núm. 486/2013, estima que «Ediciones El País, S.L.» debe cesar «*en el uso de los datos personales de ... en el código fuente de la página web que contiene la noticia de ... y en la propia página web, sin que pueda constar ni sus nombres ni apellidos ni sus iniciales. Y, que se condene a la demandada a no publicar en ninguna noticia que se refiriese al procedimiento los datos identificativos de ... ni sus nombres ni apellidos ni sus iniciales*» [407] . Ediciones El País, S.L. recurre en casación manteniendo los siguientes motivos: «*Primero. - Caducidad de la acción ejercitada: infracción del art. 9.5 de la Ley Orgánica 1/82, de 5 de mayo, de protección civil del derecho al honor, a la intimidad personal y familiar y a la propia imagen, en relación con la vulneración del art. 20.1.d) de la Constitución Española. Segundo. - Infracción del art. 7 de la Ley Orgánica 1/82, de 5 de mayo, en relación con el art. 2.1 del mismo Cuerpo normativo y en conexión con la vulneración del art. 20.1.d de la Constitución Española*»[408].

[406] Antecedente de hecho 7º de la STS 545/2015, de 15 octubre (RJ 2015\4417; ECLI:ES:TS:2015:4132).
[407] Antecedente de hecho 9º, *íd.*
[408] Antecedente de hecho 10º de la STS 545/2015, *íd.*

La Sala determina finalmente que la acción no había caducado debido a que en la fecha de la presentación de la demanda ante el Juez de primera instancia persistía la inclusión en la hemeroteca virtual del diario la indexación de la noticia y, a su vez, se obtenían resultados en los resultados de la lista de indexación por los buscadores de internet como *Google* y *Yahoo*. También concluye que «Ediciones El País S.L.» es el responsable del tratamiento de datos de una hemeroteca virtual, que la información contenida en la misma es veraz y cumple con los principios de la protección de datos establecidos en ese entonces en el art. 4 de la LOPD, y que la finalidad por la que fueron recogidos era la de informar, derecho con un amplio espectro de protección tanto a nivel nacional como internacional, es por ello que *«Los elementos para realizar esta ponderación son el potencial ofensivo que para los derechos de la personalidad tenga la información publicada y el interés público que pueda suponer que esa información aparezca vinculada a los datos personales del afectado»*[409], es decir, que las hemerotecas digitales tienen una protección al amparo del art. 10 del CEDH, y que las noticias pasadas no pueden ser objeto de cancelación o alteración *«Por tanto, la integridad de los archivos digitales es un bien jurídico protegido por la libertad de expresión»,* lo cual supone que *«el derecho al olvido digital[…] no ampara que cada uno construya un pasado a su medida».* Sin embargo, en este caso al no tratarse de ningún personaje público ni con interés histórico, el resultado de la ponderación de derechos y para evitar que los derechos de la personalidad contenidos en el art. 18.1 CE continuasen afectándose, se permite la adopción de códigos que no permitan la indexación por motores de búsqueda, pero que la noticia sea conservada en la hemeroteca virtual.

La Sala Primera del Tribunal Supremo desde que dicta esta sentencia ha resuelto otros casos similares que se han iniciado por una acción de protección de los derechos de la personalidad, a la fecha son seis sentencias de casación en la que ponderan los derechos contenidos en el art. 18.1 de la CE, tomando en cuenta que «derecho al olvido», realiza una protección instrumental a los derechos de la personalidad en un entorno digital cuando colisionan con los contenidos en el art. 20.1 de la CE. Las sentencias emitidas por esta sala son las siguientes: SSTS

[409] F.D. Sexto de la STS núm. 545/2015 de 15 octubre.

210/2016, de 5 de abril[410]; 426/2017, de 6 de julio[411]; 446/2017, del 13 de julio[412]; 585/2017, de 2 de noviembre[413] y 273/2019, de 21 de mayo[414].

Por su parte la Sala de lo Contencioso-administrativo del Tribunal Supremo ha resuelto numerosos pronunciamientos en esta materia. La primera sentencia de casación en dictarse por esta sala fue la de fecha 11 de marzo de 2016[415], recurso que fue interpuesto por «*Google Spain S.L.*», como consecuencia de la SAN de 12 de febrero de 2015, en esta última sentencia se condenaba a «*Google Spain S.L.*» a adoptar «*las medidas necesarias que evitasen la indexación de los datos y que no aparezcan respecto de los enlaces web objeto de resolución*»[416] en consonancia con la resolución de la AEPD recaída al caso. Se formulan cuatro motivos de casación, el primero de ellos por la incongruencia *extra petitum* de la sentencia de la AN, la cual confirma la resolución de la AEPD y en la cual a su vez se le considera como corresponsable del tratamiento de datos personales, excediéndose «*los límites fijados por las partes para que pudieran formular alegaciones, generándoles de ese modo la correspondiente indefensión. El demandado no planteó que debía considerarse "corresponsable" del tratamiento a Google Spain S.L. sobre la base de "unidad de negocio" o "unidad material" o sobre la base de "presuntos actos propios"*»[417]. El segundo motivo que se esgrime en el recurso de casación alega la vulneración de la Directiva 95/46/CE y a la LOPD, específicamente por considerarle como responsable del tratamiento sin que «*Google Spain S.L.*» determine los fines y los medios del tratamiento de datos personales. El tercer motivo de casación tiene que ver con la «*vulneración de la jurisprudencia relativa a la doctrina de los actos propios, argumentando que la Sentencia de instancia hace una errónea interpretación de la misma, al fundamentar también en ella, la corresponsabilidad de Google Spain S.L.*»[418]. El último motivo de casación planteado por «*Google Spain S.L.*» es la vulneración del art. 24 CE y la «*jurisprudencia sobre valoración de los hechos y ello*

[410] STS 210/2016, de 5 de abril (RJ 2016\1006; ECLI:ES:TS:2016:1280).
[411] STS 426/2017, de 6 de julio (RJ 2017\3194; ECLI:ES:TS:2017:2675).
[412] STS 446/2017, del 13 de julio (RJ 2017\3960; ECLI:ES:TS:2017:2843).
[413] STS 585/2017, de 2 de noviembre (RJ 2017\6147; ECLI:ES:TS:2017:3797).
[414] STS 273/2019, de 21 de mayo (RJ 2019\1971; ECLI:ES:TS:2019:1592).
[415] STS de 11 de marzo de 2016 (RJ 2016\1519; ECLI:ES:TS:2016:1055).
[416] *Ib.,* F.D. 1º.
[417] *Ib.,* F.D. 2º.
[418] *Íd.*

por cuanto los hechos que se atribuyen a la recurrente, para justificar la aplicación de la doctrina de los actos propios son inexactos e incluso en algunos casos inveraces, habiendo realizado una valoración arbitraria de unos hechos que ni fueron objeto de prueba en el procedimiento, ni esgrimidos por la parte demandada, sin que Google Spain S.L. haya reconocido nunca, ni de forma explícita o implícita que hubiera efectuado actuaciones como "responsable de tratamiento"»[419].

Esta sentencia se resuelve tomando en cuenta por una parte el contenido de la Directiva 95/46/CE, la LOPD y el reglamento de esta última, el contenido del RGPD relacionado con la figura de responsable de tratamiento, así como lo establecido en el Dictamen 1/2010, sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», adoptado el 16 de febrero de 2010 por el GT29, y a la luz de la STJUE de 13 de mayo de 2014, resolviéndose que la cuestión perjudicial primera planteada por «*Google Spain S.L.*», que la responsabilidad del tratamiento de datos personales era una cuestión que era objeto del debate procesal, introducido incluso *por la propia recurrente*[420], con lo cual se desestima. Respecto a los otros tres motivos de la casación, se estudian en conjunto por tener una estrecha relación, determinándose por una parte que *Google Spain S.L*. se dedica únicamente a ofertar y vender espacios publicitarios de *Google* en territorio español y sin que en ningún caso realice la labor de motor de búsqueda ni de tratamiento de datos, pues el motor de búsqueda es gestionado por *Google Search,* perteneciente a su vez a *Google Inc.*, que es quien fija las finalidades y los medios en el tratamiento de datos personales[421]. Se señala además que tampoco puede considerársele corresponsable pues ello implicaría la necesaria *participación concreta e identificada en la determinación de los fines y medios del tratamiento de que se trate*[422], en este caso concreto relacionada con la actividad realizada por el motor de búsqueda. Tampoco puede considerarse a *Google Spain S.L.* tal naturaleza de actos propios a la luz de la Jurisprudencia del TC y del TS, solo por el hecho de haber participado en los procedimientos administrativos y judiciales «*cuando: en primer lugar, la propia Sala de instancia no habla de actuaciones indubitadas o concluyentes por parte de Google*

[419] *Íd.*
[420] *Ib.,* F.D. 3º.
[421] *Ib.,* F.D. 7º.
[422] *Íd.*

Spain, S.L., en el sentido de asumir la condición de responsable del tratamiento, sino que, por el contrario, dice que estamos ante un indicio; segundo, no se advierte ni valora por la Sala de instancia la distinta condición en que puede intervenir en tales procedimientos una persona física o jurídica, mero interesado o titular de derechos u obligaciones; tercero, que solo la comparecencia como responsable del tratamiento de datos, es decir, de la determinación de los fines y medios del tratamiento de datos, puede dar lugar a manifestaciones o actos válidos de reconocimiento de tal condición; cuarto, que la condición de responsable del tratamiento de datos viene definida legalmente, como se ha indicado antes de forma prolija, y su régimen jurídico no puede modificarse por las actuaciones de quien carece de facultades de disposición al respecto; y quinto, que la legitimación ha de examinarse en cada procedimiento y, por lo tanto, ha de estarse a la actitud del compareciente en el mismo, que este caso ha sido, desde la vía administrativa, negar tal legitimación» [423]. Derivado de la estimación de este motivo de casación debe estimarse el cuarto planteado por «*Google Spain S.L.*», obteniendo como consecuencia la anulación de la SAN en cuanto a las obligaciones derivadas de la misma impuestas a «*Google Spain S.L.*», sin embargo, se hace mención en esta sentencia específicamente en su F.D. 11, que sin perjuicio de lo anterior, debe considerarse como responsable del tratamiento a Google Inc. y, por tanto, «*ha de dirigirse frente al responsable del tratamiento controvertido, que en este caso es Google Inc*»[424].

El criterio anterior es el que ha seguido la Sala de lo Contencioso Administrativo para resolver los sesenta y dos recursos presentados por «*Google Spain S.L.*»[425] a lo largo del 2016, determinándose la falta de responsabilidad de «*Google Spain S.L.*» para hacer frente a la obligación impuesta por la AN de eliminar de la lista de resultados las búsquedas realizadas a partir del nombre. En el año 2019

[423] *Ib.,* F.D. 10º.
[424] *Ib.,* F.D. 11º.
[425] En la mayoría de los recursos presentados se planteaban cuatro motivos de casación, casi idénticos al del primer recuso presentado: el primero tenía que ver con la alegación de una incongruencia *extra petita* por infracción de los arts. 33.3 y 65.2 de la LJCA y 24 constitucional, el segundo tiene que ver con la atribución de corresponsable en el tratamiento de datos personales, el tercero estaba relacionado con la infracción de la doctrina de los actos propios y el cuarto por infracción del art. 24 debido a la valoración de los hechos tomados en cuenta habiendo contrariado la sentencia, las reglas de la sana critica en la apreciación de la prueba en relación con la responsabilidad que se le atribuía a «*Google Spain S.L.*». Debido a la extensión de las referencias relativas a los sesenta y dos recursos las mismas se han incluido en el Anexo III de este trabajo.

solamente se ha dictado una sentencia de esta sala resolviendo un recurso en relación con el derecho al olvido presentado por *Google LLC*. Esta sentencia reitera que el Derecho al olvido es una manifestación del haz de facultades «*conferidas a su titular para oponerse a un uso ilegítimo de sus datos personales*»[426]. También se reconoce el potencial daño que pueden efectuar los motores de búsqueda a los diversos derechos fundamentales contemplados en la CE: «*puede afectar significativamente a los derechos fundamentales de respeto a la vida privada y la protección de los datos personales cuando la búsqueda se lleva a cabo a partir del nombre de una persona física, toda vez que dicho tratamiento permite a cualquier interesado conocer mediante la lista de resultados la visión estructurada de la información relativa a esa persona en internet, que afecta potencialmente a una multitud de aspectos de su vida privada*»[427]. Reconoce la responsabilidad de Google LLC en el tratamiento de datos personales, debemos de recordar que ahora la multinacional tiene una sede en Irlanda para la gestión de sus negocios y servicios prestados en Europa, entre los que se encuentra su motor de búsqueda. Debe «*interpretarse en el sentido de que debe garantizarse la protección del derecho al olvido digital (de conformidad con lo dispuesto en el artículo 18 de la Norma Fundamental) en aquellos supuestos en que la información que es objeto de difusión, y cuya localización se obtiene a través de motores de búsqueda en internet que contenga datos inexactos que afectan en lo sustancial a la esencia de la noticia*»[428].

En este mismo periodo el Tribunal Constitucional se pronuncia por primera vez acerca del derecho al olvido en Sentencia 58/2018, de 4 de junio, de la Primera Sala. Esta sentencia se ha dictado diez días después de la entrada en vigor del nuevo RGPD, por lo que aplica de manera directa su contenido y resuelve también lo relativo a las hemerotecas virtuales. En la sentencia se deja claro que el derecho al olvido es «*una vertiente del derecho a la protección de datos personales frente al uso de la informática*»[429].

[426] F.D. 3 de la STS 12/2019, de 11 de enero (RJ 2019\8; ECLI:ES:TS:2019:19).
[427] *Ib.,* F.D. 2.
[428] *Ib.,* F.D. 3.
[429] F.J. 5 de la STC 58/2018, de 4 de junio de 2018 (RTC 2018\58; ECLI:ES:TC:2018:58).

Las hemerotecas virtuales de los principales medios de comunicación contenidas en sus páginas web cuentan con un motor de búsqueda propio del contenido albergado en su sitio web. En relación con lo anterior esta sentencia resulta de gran importancia pues determina que la medida tecnológica idónea y respetuosa de los derechos a la protección de datos personales y del derecho de la información es que se permita el acceso a la noticia por medio de este buscador interno, es decir, que siga indexándose la información en aras de proteger el contenido de las hemerotecas en relación con el art. 20.1.d) de la CE, sin embargo, no es proporcionada con otros derechos que estas búsquedas sigan siendo realizadas a partir del nombre y apellidos de las personas afectadas que carezcan de relevancia pública[430]. Determina que es excesiva la medida de eliminar del código fuente el nombre y los apellidos de las personas involucradas en los hechos y publicados en la nota periodística originaria publicada en la hemeroteca virtual, sustituyéndolos 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. Y, descartada la necesidad de la medida, huelga toda consideración en torno a la proporcionalidad en sentido estricto de la misma*»[431].

Recientemente el TJUE por sentencia de 24 de septiembre de 2019 ha resuelto una cuestión prejudicial planteada por el Consejo de Estado Francés contra Google LLC, relativa a la retirada de varios enlaces obtenidos tras una búsqueda realizada a partir del nombre. Esta cuestión prejudicial tiene su origen en una resolución de la autoridad francesa de control denominada CNIL. Esta autoridad estima una solicitud de un particular en la que solicita que sean eliminados de la lista

[430] *Ib.*, F.J. 8.
[431] *Íd.*

de resultados del motor de búsqueda algunos enlaces obtenidos tras una búsqueda realizada a partir del nombre del afectado. Sin embargo, la peculiaridad de esta resolución radica en que se ordena la eliminación de este enlace en «todas las extensiones de dominio» del buscador. Google cumple de manera parcial lo dispuesto en la resolución, solo son eliminados los enlaces de las extensiones de dominio pertenecientes a los países de la Unión Europea. Esto provoca que el CNIL multe a Google por una cantidad de cien mil euros. Como respuesta a esta situación, Google recurre esta determinación ante el Consejo de Estado Francés (Conseil d´État) solicitando su anulación. Durante la tramitación de esta cuestión prejudicial *Google* decide cambiar su configuración de tal manera que en el caso que los usuarios introdujeran manualmente el nombre de dominio no se determinase los resultados en su búsqueda, pues estos están condicionados a la localización geográfica del usuario. A lo cual el TJUE falla en el sentido que «*cuando el gestor de un motor de búsqueda estime una solicitud de retirada de enlaces en virtud de estas disposiciones, estará obligado a proceder a dicha retirada no en todas las versiones de su motor, sino en las versiones de este que correspondan al conjunto de los Estados miembros, combinándola, en caso necesario, con medidas que, con pleno respeto de las exigencias legales, impidan de manera efectiva o, al menos, dificulten seriamente a los internautas que efectúen una búsqueda a partir del nombre del interesado desde uno de los Estados miembros el acceso, a través de la lista de resultados que se obtenga tras esa búsqueda, a los enlaces objeto de la solicitud de retirada*» [432]. Con esta sentencia se reitera lo que resultaba casi evidente, el derecho a la supresión no es efectivo fuera de las fronteras europeas. Sin embargo, los motores de búsqueda están sujetos a lo establecido por el RGPD, en el marco de la prestación de servicios en el territorio de la Unión y para los usuarios de esos territorios.

[432] Apartado 73 de la STJUE de 24 de septiembre de 2019 (TJCE 2019\203; ECLI:EU:C:2019:772).

CAPÍTULO III

LA PROTECCIÓN DE DATOS EN EL SECTOR PÚBLICO.

1. LAS AUTORIDADES DE CONTROL COMO GARANTES DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL RGPD.

El RGPD tiene aplicabilidad directa en todos los Estados miembros de la UE y, por tanto, las disposiciones que regulan a las autoridades de control en materia de protección de datos deben ser observadas por todas estas con independencia del Estado en el que se encuentren. En consecuencia, las funciones y poderes son las mismas para todas con el fin de proteger los derechos y libertades fundamentales de las personas físicas y facilitar la libre circulación de los datos dentro del territorio de la Unión[433]. Las autoridades de control deben cooperar entre ellas cuando se realicen tratamientos transfronterizos o cuando un responsable tenga más de un establecimiento en la UE, sin perjuicio del deber de colaboración que tienen con la Comisión y con el CEPD.

El nuevo panorama normativo en la materia ha introducido cambios sustanciales relacionados con las autoridades de control, entre las que destacan los mecanismos de cooperación y coherencia. El CEPD tiene un papel angular en los mismos, pues una de sus funciones principales es velar por la aplicación coherente del RGPD. Este organismo tiene personalidad jurídica propia, pero está «*vinculado administrativamente al Supervisor Europeo*»[434], sin que afecte a su independencia en el desempeño de sus funciones[435]. Este organismo ha sustituido al GT29 el cual fue creado por la Directiva 95/46/CE. El Comité tiene asignadas distintas funciones de:

[433] Cfr. Art. 51.1 del RGPD.
[434] Cfr. CERVERA NAVAS, L., «Las instituciones y organismos europeos de protección de datos: El Supervisor Europeo y el Comité Europeo de Protección de Datos», *El Cronista del Estado Social y Democrático de Derecho,* mayo-junio 2020, núm. 88-89, p. 109.
[435] Conforme al apdo. 3 del art. 8 de la CDFUE y al contenido del art. 69 del RGPD.

supervisión, asesoramiento e información [436]. Entre las competencias que tiene atribuidas y de relevancia en este caso son aquellas relacionadas con el mecanismo de coherencia, las cuales se encuentran recogidas en los incisos a) y t) del art. 70.1 del RGPD. El Comité será el encargado de emitir un dictamen, el cual tendrá carácter de potestativo en algunos casos y de vinculante en otros, lo cual se explicará de manera detallada más adelante.

1.1 La configuración de las autoridades de control.

A las autoridades de control se les se les atribuyen distintas cualidades, entre las que destaca la independencia. El RGPD también determina cuestiones relacionadas con sus funciones y poderes, centrándose en pormenorizar las competencias de cada una de las autoridades de control cuando se realicen tratamientos transfronterizos dentro de la UE. De acuerdo con la definición establecida en el art. 4.21 del RGPD se entiende como autoridad de control a aquella «*autoridad pública independiente establecida por un Estado miembro*». Los Estados podrán establecer dentro de su territorio más de una autoridad de control en la materia y cada una contará en principio con las mismas competencias, funciones y poderes. Los Estados miembros deberán además determinar cuál de las autoridades de control existentes en su territorio representará a todas las demás ante el CEPD [437]. Aquella que represente a su Estado en el CEPD deberá establecer un instrumento que garantice el cumplimiento del mecanismo de coherencia en la aplicación del RGPD por las demás autoridades de control dentro de ese territorio, tal y como lo ordena el apartado 3 del art. 51 del RGPD.

Como se señaló anteriormente, la independencia es una de las características definitorias de las autoridades de control especialmente en el desempeño de sus

[436] Tal y como lo determina CERVERA NAVAS, L., *op. cit.,* p. 111. La totalidad de sus funciones se contienen en el art. 70 del RGPD. Para un estudio en mayor profundidad *vid.* CERVERA NAVAS, L., «XXVIII. El Comité Europeo de Protección de Datos», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2016, pp. 527-538; CAMISÓN YAGÜE, J.A., Artículo 60. Coordinación en caso de emisión de dictamen por el Comité Europeo de Protección de Datos, pp. 279-282; ORTEGA GIMÉNEZ, A., «Artículo 61. Intervención en caso de tratamientos transfronterizos», p. 283; CAMISÓN YAGÜE, J.A., «Artículo 62. Coordinación en caso de resolución de conflictos por el Comité Europeo de Protección de Datos», pp. 284-286, estos últimos en ARENAS RAMIRO, M. y ORTEGA GIMÉNEZ, A. (Dirs.), *Protección de datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*, Sepín, Madrid, 2019.

[437] Además, el Presidente de esta autoridad de control formará parte del CEDP, de acuerdo con lo establecido en el art. 68.3 del RGPD.

funciones[438]. Esta independencia busca la objetividad sobre todo a la hora de tomar decisiones, ya que las autoridades de control no están sometidas a ninguna otra autoridad de manera directa o indirecta, lo que supone una garantía de imparcialidad en el ejercicio de sus funciones[439]. Esta independencia exige que cada autoridad de control disponga, dentro de su territorio, «*en todo momento de recursos humanos, técnicos y financieros*»; lo cual no significa que estas no estén sometidas a controles sobre el manejo de sus presupuestos[440]. En relación con lo anterior, el TJUE ha tenido oportunidad de pronunciarse al respecto, determinando que «*La garantía de independencia no se ha establecido para conceder un estatuto particular a esas autoridades mismas o a sus agentes, sino para reforzar la protección de las personas y de los organismos afectados por sus decisiones. De lo anterior resulta que, en el ejercicio de sus funciones, las autoridades de control deben actuar con objetividad e imparcialidad, y, para ello, han de estar a resguardo de toda influencia externa, incluida la ejercida directa o indirectamente por el Estado*»[441].

Otras garantías previstas para asegurar la independencia de las autoridades de control son aquellas de carácter formal, específicamente las relativas a su personal y presupuesto. Las autoridades de los Estados miembros son quienes deben elegir y disponer de su personal. El nombramiento de estos deberá realizarse de manera transparente conforme con lo establecido en el art. 53. También se

[438] Cfr. Art. 52 del RGPD.

[439] Esta cualidad ya se reflejaba en el contenido del art. 28.1 de la antigua Directiva 95/46/CE, cuando se determinaba que la autoridad de control debía ejercer sus funciones con total independencia. En este sentido el apartado 51 de la STJUE de 8 de abril de 2014 interpretando el contenido de este artículo establece que estas: «*para vigilar el tratamiento de datos personales han de disfrutar de la independencia que les permita ejercer sus funciones sin influencia externa. Esta independencia en particular excluye toda orden o influencia externa con independencia de la forma que revista, directa o indirecta, que pudiera orientar sus decisiones y, en consecuencia, poner en peligro el cumplimiento de la tarea que corresponde a dichas autoridades de establecer un justo equilibrio entre la protección del derecho a la intimidad y la libre circulación de datos personales*», Cfr. Apdo. 51 (TJCE\2014\139; ECLI:EU:C:2014:237).

[440] Considerando 118 del RGPD.

[441] Cfr. Apdo. 25 de la STJUE de 9 de marzo de 2010 (TJCE\2010\68; ECLI:EU:C: 2010:125). Esta sentencia tuvo cabida un asunto donde la parte demandante era la Comisión Europea junto con el Supervisor Europeo de Protección de Datos en contra de la República Federal de Alemania. Los demandantes consideraban que no se había transpuesto de manera correcta el contenido del art. 28.1 de la Directiva 95/46/CE al sistema jurídico alemán. En esta se clarifica la cualidad de independencia de la que están dotadas todas las autoridades de control, incluso cuando la normativa nacional de los Estado miembros contemplen una diferenciación entre tratamiento llevados a cabo por el sector público y el sector privado, y existan autoridades de control distintas para estos. Con base en esta sentencia se han emitido otras en el mismo sentido, por ejemplo, la STJUE de 16 de octubre de 2012 (TJCE\2012\287; ECLI:EU:C:2012:631), *vid.* Apdos. 41 y ss.

establecen determinados criterios objetivos que deben tomarse en cuenta para el nombramiento de su personal, de acuerdo con el apartado 2 del referido artículo, las personas que formen parte de la autoridad de control deberán poseer «*una titulación, la experiencia y las aptitudes, en particular en el ámbito de la protección de datos personales*» necesarias para cumplir con sus funciones y ejercer los poderes que les son asignados. Estas cualificaciones, al igual que las condiciones de idoneidad, las normas y el procedimiento que tendrá que seguirse para el nombramiento de sus miembros, deberán estar reguladas por ley[442]. Así como otras cuestiones como la duración del cargo (el cual no podrá ser inferior a cuatro años), la renovación de este, el número de veces de renovación, las obligaciones de sus miembros y de su personal, las incompatibilidades durante y después del mandato, y la forma de su cese [443].

Las funciones de los miembros de las autoridades de control podrán concluirse de manera normal cuando se termine el mandato, por dimisión o jubilación. Solo podrán ser destituidas del cargo las personas que cometan conductas irregulares graves o si estas dejasen de cumplir con «*las condiciones exigidas en el desempeño de sus funciones*» [444]. Esto constituye otro elemento esencial relacionado con la independencia de estas autoridades, puesto que anteriormente la inamovilidad no estaba regulada en la Directiva 95/46/CE, mientras que la normativa de transposición española si lo contemplaba en su art. 36.3 [445]. En este sentido, el Profesor TRONCOSO REIGADA determina que es: «*el elemento más importante del estatuto jurídico de los miembros de las autoridades de control*» [446].

El personal de este tipo de autoridades durante el ejercicio de su cargo deberá abstenerse de la realización de acciones incompatibles con sus funciones,

[442] Incisos b) y c) del art. 54.1 del RGPD.
[443] Incisos d), e) y f) del art. 54.1 del RGPD.
[444] Art. 53.4 del RGPD.
[445] Que hablaba sobre el cese del cargo de la figura de Director, en cuyo caso solo podría ser separado del cargo: «*previa instrucción de expediente, en el que necesariamente serán oídos los restantes miembros del Consejo Consultivo, por incumplimiento grave de sus obligaciones, incapacidad sobrevenida para el ejercicio de su función, incompatibilidad o condena por delito doloso*».
[446] TRONCOSO REIGADA, A., «XXVI. Autoridades de control independientes», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2016, pp. 478-479. En este mismo sentido también se pronuncia NEIRA BARRAL, D., *op. cit.,* p. 685.

sean remuneradas o no[447]. Así pues, durante y después de su mandato el personal de cada autoridad de control estará sometido al deber de secreto en relación con la información confidencial a la que hayan tenido acceso; especialmente si el personal ha tenido conocimiento de infracciones cometidas por personas físicas[448]. Asimismo, el Profesor RUBÍ NAVARRETE establece que esta previsión «*parece ir dirigida a poder garantizar el anonimato de quienes ponen en conocimiento de la autoridad de control posibles infracciones del Reglamento*»[449].

La independencia financiera también es una garantía formal que tienen este tipo de autoridades. En este caso, los Estados miembros deberán asegurarse de que cada una de las autoridades establecidas en su territorio cuenten con recursos financieros de manera anual, incluso se señala que estos podrán formar parte de los presupuestos generales o de otra índole, como es el caso de las autoridades de control autonómicas, en cuyo caso dependen de los presupuestos de la Comunidad Autónoma dónde se sitúen y realicen su función. De acuerdo con el Profesor TRONCOSO REIGADA esta garantía constituye «*Un elemento necesario tanto para la independencia de las autoridades de control como para el correcto cumplimiento de sus funciones y autonomía de personal, presupuestaria y financiera*»[450]. Las autoridades de control no están exentas de controles financieros, sin embargo, los Estados deben garantizar que este tipo de controles no afecten la independencia de las autoridades de control[451]. No obstante, la rendición de cuentas de su gestión como bien apunta RUBÍ NAVARRETE «*deberá de estar a disposición de la opinión pública y del control parlamentario*»[452].

[447] Art. 52.3 del RGPD.
[448] ART.54.2 del RGPD.
[449] RUBÍ NAVARRETE, J., «La Agencia Española de Protección de Datos», RALLO LOMBARTE, A. (Dir.), *Tratado de protección de datos. actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, Tirant lo Blanch, Valencia, 2019, pp. 491-520.
[450] TRONCOSO REIGADA, A., «XXVI. Autoridades (…)», *op. cit.,* p. 481.
[451] Apartados 4 y 6 del RGPD.
[452] RUBÍ NAVARRETE, J., «La Agencia…» *op. cit.,* p. 97.

1.2 Competencias, funciones y poderes de las autoridades de control.

Las autoridades de control de manera general serán competentes en el territorio de su Estado miembro para ejercer sus funciones y poderes. De igual manera serán competentes cuando el tratamiento de datos personales sea efectuado por autoridades públicas u otros organismos privados cuya base de licitud sea el cumplimiento de una obligación legal, el cumplimiento del interés general o el ejercicio de sus competencias atribuidas [453]. Se comprende dentro de sus competencias el conocimiento de reclamaciones realizadas por los interesados, cuyo objeto sea investigar si el tratamiento de datos efectuado por los responsables se adecúa al contenido del RGDP o si por el contrario, se han realizado conductas calificadas como infracciones en la normativa de la materia; siempre que estas se refieran solo al establecimiento de un responsable situado en el Estado miembro de su competencia o, si afectase sustancialmente a los interesados del territorio antes referido [454]. En ambos casos, esta autoridad deberá dar parte a la autoridad de control principal para que esta última determine si recurre o no al mecanismo de cooperación establecido en el art. 60 del RGPD [455], el cual se explicará de manera detallada posteriormente.

El art. 57.1 del RGPD nos ofrece un listado de carácter enunciativo más no limitativo de las funciones que deberán ser desempeñadas por todas las autoridades de control. La primera y quizás la principal sea la de controlar la aplicación del RGPD y hacerlo aplicar a los sujetos intervinientes en el tratamiento de datos personales [456]. También serán las encargadas de promover la sensibilización de público en general sobre los riesgos, normas, garantías y derechos relacionados con el tratamiento de datos personales, con especial atención a las actividades dirigidas

[453] Cfr. Apdos. 1 y 2 del art. 55 en relación con los incisos c) y e) del art. 6.1 del RGPD. En este caso específico no se le aplicará lo relativo a la autoridad de control principal establecido en el art. 56, por tanto, siempre será competente en este caso. En relación con lo anterior, se excluye de su competencia los tratamientos de datos efectuados por los tribunales.
[454] Art. 56.2 RGPD.
[455] Esta decisión deberá tomarse en el plazo de tres semanas contadas a partir de dicha comunicación. En relación con los apdos. 2 y 3 del art. 56 del RGPD. Cfr. TRONCOSO REIGADA, A., «XXVI. Autoridades (…)», *op. cit.,* p. 493-494
[456] Art. 57.1 a) del RGPD

a niños; esta sensibilización también estará dirigida a los responsables y encargados del tratamiento de datos personales respecto a sus obligaciones[457]. Las autoridades de control asesorarán al poder legislativo de su Estado, al Gobierno, y a otras instituciones y organismos acerca de las medidas legislativas y administrativas que se deben adoptar en relación con la protección de datos de carácter personal, y demás derechos y libertades de las personas físicas[458]. Igualmente contribuirán con las actividades realizadas por el CEPD[459].

En relación con los interesados las autoridades de control deberán proporcionarles información relacionada con el ejercicio de sus derechos y en caso de que sea presentada una reclamación investigar el motivo de la misma e informarle del curso y el resultado de esta. Las autoridades de control deberán facilitar la presentación de reclamaciones por medio de un formulario al efecto, que pueda ser cumplimentado por medios electrónicos, sin excluir otros medios de comunicación[460]. Estas autoridades también tendrán que hacer seguimiento a las nuevas tecnologías aplicadas al tratamiento de datos personales, así como a las prácticas comerciales que les sean de interés y que puedan afectar a los usuarios[461], cuestión que está estrechamente vinculada con su labor de vigilancia. También elaborarán y autorizarán cláusulas tipo que deberán utilizarse para la elaboración de contratos entre el responsable del tratamiento y el encargado, y en contratos celebrados entre encargados del tratamiento. En relación con la transmisión de datos a un tercer país u organización internacional, las autoridades de control serán las que se encarguen de autorizar este tipo de transmisiones y, de vigilar que se ofrezcan garantías adecuadas como cláusulas entre los agentes intervinientes en la transferencia[462] de tal manera que, los derechos de los interesados no sean infringidos.

Respecto a la evaluación de impacto, las autoridades de control deberán elaborar, publicar y mantener actualizada la lista de tratamientos que requieran una

[457] Incisos b) y d) del art. 57.1 del RGPD.
[458] Inciso c) del art.57.1 del RGPD.
[459] Inciso t) del art. 57.1 del RGPD.
[460] Incisos e) y f) del art. 57.1 y art. 57.2 del RGPD.
[461] Inciso i) del art. 5701 del RGPD.
[462] Incisos j) y r) del art. 57.1 del RGPD., en relación con el contenido del art. 46 del mismo instrumento jurídico.

evaluación de impacto antes de iniciar el tratamiento[463]. En el caso de que los responsables consulten a la autoridad y el tratamiento entrañe un alto riesgo para los derechos y libertades de los interesados, la autoridad de control debe ofrecer asesoramiento por escrito al responsable y al encargado[464]. Estas autoridades también serán las encargadas de promover, dictaminar y aprobar los códigos de conducta de las asociaciones y otros organismos representativos de categorías de responsables o encargados, para que proporcionen garantías suficientes destinadas a la correcta aplicación del RGPD[465]. En cuanto a los mecanismos de certificación de datos, sellos y marcas en la materia, las autoridades de control fomentarán su creación, y serán las encargadas de aprobar los criterios de certificación, igualmente si procede llevarán a cabo una revisión periódica de las certificaciones expedidas a los responsables o encargados del tratamiento[466]. También elaborarán y publicarán los requisitos para la acreditación de organismos de supervisión, en este sentido, serán las competentes para efectuar la misma, tanto de organismos de supervisión, de códigos de conducta y de organismos de certificación[467]. Por lo que concierne a las normas corporativas vinculantes relacionadas con el mecanismo de coherencia del art. 63, será competencia de cada autoridad de control aprobarlas en su territorio siempre que sean conformes con el contenido del art. 47 del RGPD[468]. En relación con sus poderes correctivos llevarán a cabo un registro de las infracciones y sanciones, así como de las medidas que deban adoptar los responsables o encargados del tratamiento para adaptar su actuación a lo establecido en el

[463] En este sentido la AEPD ha publicado dos listados: el primero se refiere a los tratamientos de datos que requieren de una evaluación de impacto previa al tratamiento y otra, que exime a determinados sujetos o tratamientos de dicha evaluación de impacto previa. Cfr. AEPD, «*Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art. 35.4)*». Disponible en: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf (consulta: 18 de noviembre de 2020) y, AEPD, «*Lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos según el art. 35.5 RGPD*». Disponible en: https://www.aepd.es/sites/default/files/2019-12/ListasDPIA-35.5l.pdf (consulta: 18 de noviembre de 2020).

[464] Incisos k) y l) del art. 57.1, en relación con el art. 36.2 y 35.1 del RGPD.

[465] Inciso m) del art. 57.1, en relación con lo establecido en los apartados 1 y 5 del art. 40 del RGPD.

[466] Incisos n) y o) del art. 57.1 en relación con el art. 42 apartados 1, 5 y 7 del RGPD.

[467] Incisos p) y q) del art. 57.1 del RGPD.

[468] Si se adecuan al contenido del art. 47 del RGPD, de acuerdo con el inciso s) del art. 57.1 del RGPD.

RGPD[469]. Finalmente, de forma residual, las autoridades de control desempeñarán «*cualquier otra función relacionada con la protección de los datos personales*»[470].

Las funciones que desempeñen las autoridades de control y estén dirigidas a los interesados o a los delegados de protección de datos tendrán que ser gratuitas, salvo, cuando las solicitudes de los interesados sean manifiestamente infundadas o excesivas, por ser repetitivas, en cuyo caso se podrá establecer una tasa para cubrir los costes administrativos o en su caso negarse a actuar respecto a la solicitud. Sin embargo, será la autoridad de control la que deberá de probar este tipo de situaciones[471].

Los poderes que son conferidos a las autoridades de control conforme a lo establecido en el art. 58 del RGPD, pueden clasificarse según la función que desempeñan: a) poderes de investigación, b) poderes correctivos y, c) poderes de autorización y consultivos. Estos poderes están sujetos a «*garantías adecuadas, incluida la tutela judicial efectiva y respeto a las garantías procesales, establecidas en el Derecho de la Unión y de los Estados miembros de conformidad con la Carta*»[472]. En relación con los poderes antes descritos se determina en el RGPD que los Estados miembros deberán disponer por ley: a) que su autoridad de control este facultada para poner en conocimiento al órgano jurisdiccional competente sobre infracciones cometidas y, b) otros poderes siempre y cuando no interfieran con la cooperación entre autoridades de control cuando el tratamiento de datos personales se realice de manera transfronteriza[473].

La finalidad principal de los poderes de investigación que les son conferidos es hacerse con toda la información necesaria para desempeñar sus funciones, para lo cual podrán: a) ordenar al responsable, encargado o en su caso al representante de estos para que le facilite información, incluso obtener del responsable y del encargado acceso a todos los datos y a toda la información que estimen necesaria para el ejercicio de sus funciones; b) llevar a cabo auditorías y revisión de certificaciones; c) notificar al responsable o encargado de la comisión de presuntas

[469] Inciso u) del art. 57.1 del RGPD.
[470] Inciso v) del art. 57.1 del RGPD.
[471] Apartados 3 y 4 del art. 57 del RGPD.
[472] Art. 58.4 del RGPD.
[473] Apartados 5 y 6 del art. 58 del RGPD.

infracciones; d) «*obtener acceso a los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos*»[474], siempre que sea conforme con el derecho procesal de la UE y de ese Estado. En el caso de España se debe contar con una autorización judicial previa, de modo que no se trasgreda la inviolabilidad del domicilio, la cual está estrechamente relacionada con el derecho a la intimidad de las personas[475].

Los poderes correctivos de las autoridades de control para sancionar a todo responsable o encargado del tratamiento de datos personales podrán ejercerse incluso con sanciones de previa advertencia o con apercibimiento para disuadir las conductas que infrinjan el contenido del RGPD[476]. En su caso también podrán ordenar al responsable o al encargado según sea el caso para que: a) atiendan las solicitudes de ejercicio de derechos de los interesados, b) que el tratamiento se ajuste al RGPD y c) que el responsable comunique a los interesados las violaciones de seguridad. La autoridad de control igualmente podrá limitar el tratamiento de manera temporal o definitiva, e incluso prohibirlo; ordenar la rectificación o supresión de los datos e incluso limitar el tratamiento de los datos personales por parte de los responsables, y que estos comuniquen a su vez a los interesados de la adopción de alguna de estas medidas[477]. Las autoridades de control podrán además retirar certificaciones u ordenar al organismo que las expida a no expedir más si no se cumplen o dejan de cumplirse los requisitos para la obtención de estas; imponer multas administrativas con arreglo a las condiciones generales para la imposición

[474] Vid art.58.1 y considerando 129 del RGPD.

[475] De acuerdo con lo establecido en el art. 18.2 de la CE, en este sentido el F.J. 6 la STC 10/2002, de 17 de enero (RTC 2002\10; ECLI:ES:TC:2002:10) determina que la CE no ofrece una definición de domicilio con lo cual debe entenderse que se trata de aquel espacio «*en el cual el individuo vive sin estar sujeto necesariamente a los usos y convenciones sociales y ejerce su libertad más íntima*». Sin embargo, esta definición no es aplicable a el domicilio de las personas jurídicas pues en ellas no se desarrolla tal desenvolvimiento de la vida íntima de las personas físicas. Sin embargo, fue por el F.J. 3 de la STC (Sala Segunda)137/1985, de 17 de octubre (RTC 1985\137; ECLI:ES:TC:1985:137) que se determinó que la inviolabilidad del domicilio también es extensiva a las personas jurídicas. Posteriormente se ha ido perfilando su contenido en relación con estas últimas, así pues la STC (Sala Segunda) 69/1999, de 26 de abril (RTC\1999\69; ECLI:ES:TC:1999:69)estableció en su F.J. 2 que: «*la protección constitucional del domicilio de las personas jurídicas y, en lo que aquí importa, de las sociedades mercantiles, sólo se extiende a los espacios físicos que son indispensables para que puedan desarrollar su actividad sin intromisiones ajenas, por constituir el centro de dirección de la sociedad o de un establecimiento dependiente de la misma o servir a la custodia de los documentos u otros soportes de la vida diaria de la sociedad o de su establecimiento que quedan reservados al conocimiento de terceros*».

[476] Incisos a) y b) del art. 58.2 del RGPD.

[477] Conforme a lo establecido en los arts. 16, 17, 18 y 19 del RGPD;

de multas establecidas en el art. 83 del RGPD y, ordenar que se detengan los flujos de datos a terceros países u organizaciones internacionales[478].

Todas las autoridades de control tienen como obligación elaborar un informe de actividades que incluya las decisiones adoptadas con motivo de sus poderes correctivos, deberán transmitirlo a su parlamento nacional, a su gobierno, y a «*las demás autoridades designadas en virtud del Derecho de los Estados miembros*». Este informe también deberá ponerse a disposición del público en general, a la Comisión y al CEPD[479].

En relación con sus poderes de autorización y consultivos estas autoridades podrán emitir dictámenes en la materia, aprobar cláusulas contractuales, aprobar códigos de conducta, asesorar al responsable cuando el tratamiento de datos requiera una evaluación de impacto, autorizar tratamientos con motivo del cumplimiento de un interés público como la protección social o la salud pública, acreditar a los organismos de certificación, así como expedir certificaciones y aprobar criterios de certificación, la adopción de cláusulas tipo para contratos celebrados entre responsable y encargado del tratamiento y, aprobar normas corporativas vinculantes[480].

1.3 Los mecanismos de cooperación y coherencia: significado y alcance.

Como novedad el RGPD estructura un marco competencial de las autoridades de control, de tal manera que cada una de las autoridades involucradas sepa cómo actuar en el ejercicio de sus competencias, en especial, cuando una autoridad actuase como autoridad de control principal y el responsable o el encargado llevaran a cabo tratamientos transfronterizos de datos o tuvieran más de un establecimiento

[478]Art. 58.2 del RGPD. Los sistemas jurídicos de Dinamarca y de Estonia no prevén que se puedan imponer multas por autoridades de naturaleza administrativa, en estos dos casos tal y como describe el considerando 151 del RGPD «*las normas sobre multas administrativas pueden ser aplicadas en Dinamarca de tal manera que la multa sea impuesta por los tribunales nacionales competentes en cuanto sanción penal, y en Estonia de tal manera que la multa sea impuesta por autoridades de control en el marco de un juicio de faltas, siempre que tal aplicación de las normas en dichos Estados miembros tenga un efecto equivalente a las multas administrativas impuestas por las autoridades de control*».
[479] Art. 59 del RGPD.
[480] Art. 58.3 del RGPD.

en varios territorios de la UE[481]. Con lo anterior «*se intenta responder de este modo a las insuficiencias del sistema precedente*»[482] en el que solo se contemplaba la cooperación entre ellas con la finalidad de cumplir con las funciones de cada una de ellas manera separada, especialmente en el intercambio de información que estimasen útil de acuerdo con el art. 28.6 de la hoy derogada Directiva 95/46/CE. En palabras de BLANCO ANTÓN este nuevo marco de cooperación previsto por el RGPD pretende alcanzar la coherencia en su aplicación a través de criterios comunes. Es decir, las autoridades de control «*deben y tienen que cooperar entre ellas y con la Comisión, sin necesidad de otros acuerdos entre Estados miembros sobre la prestación de asistencia mutua ni sobre dicha cooperación*»[483].

Las autoridades que tienen condición de autoridad de control principal son aquellas que se ajustan a alguno de estos tres supuestos: a) la autoridad que está situada donde se encuentre el establecimiento principal del responsable, es decir, donde se sitúe el establecimiento encargado de determinar los fines y los medios del tratamiento con el poder de aplicarlos en los demás establecimientos situados en otros Estados miembros de la UE[484]; b) la autoridad que se sitúe en el mismo territorio del único establecimiento del responsable y, c) la autoridad situada en el mismo territorio que el establecimiento principal del encargado de tratamiento, en

[481] Es importante señalar la crítica que hace el Profesor LÓPEZ CALVO a este nuevo marco de cooperación entre las autoridades de control. De acuerdo con este autor el legislador europeo «*Renuncia así a un mecanismo centralizado que probablemente hubiera resultado más operativo en el caso de los tratamientos transfronterizos*», Cfr. LÓPEZ CALVO, J., «Cooperación y coherencia (Arts. 60-76. Arts. 60-62 LOPDGDD)», LÓPEZ CALVO, J., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Wolters Kluwer Bosch, España, 2019, p. 638.

[482] IRURZUN MONTORO, F., «XXVII. Cooperación y coherencia entre autoridades de control», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2016, p. 513.

[483] Cfr. BLANCO ANTÓN, M.J., «Autoridades de control independientes (Arts. 51-59 RGPD). Autoridades de Protección de Datos (Arts. 44-59 y Disposición adicional cuarta LOPDGDD)», LÓPEZ CALVO, J., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Wolters Kluwer Bosch, España, 2019, p. 604.

[484] El RGPD no determina que autoridad de control será la principal cuando exista corresponsabilidad en el tratamiento de datos personales. En este caso el GT29 ha esclarecido esta situación determinando que: «*con el fin de beneficiarse del principio de ventanilla única, los corresponsables del tratamiento deben designar (entre los establecimientos en los que se toman las decisiones) qué establecimiento tendrá la potestad para ejecutar las decisiones relativas al tratamiento con respecto a todos los corresponsables. Dicho establecimiento se considerará el establecimiento principal para el tratamiento realizado en caso de corresponsables*», Cfr. GT29, Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento. Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp244rev01-es.pdf (consulta: 10 de noviembre de 2020).

este caso será aquella donde se realice la administración central en la UE o a falta de esta, en donde se realicen las actividades principales de tratamiento «*en el contexto de las actividades de un establecimiento encargado en la medida en que el encargado esté sujeto a obligaciones específicas*» [485]. Esta autoridad de control será la interlocutora del responsable o encargado en relación con el tratamiento de datos transfronterizo [486].

Por otro lado, el RGPD nos ofrece una definición de autoridad de control interesada en su art. 4.22 como aquella «*autoridad de control a la que afecta el tratamiento de datos personales debido»* cuando: «*a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o c) se ha presentado una reclamación ante esa autoridad de control*», cuyo caso podrán participar en los mecanismos de control y coherencia.

En el sistema de cooperación participan las autoridades de control interesadas junto con la autoridad de control principal. El mecanismo de cooperación es obligatorio en determinados casos y si este no prosperase adecuadamente estas autoridades de control deberán acudir al mecanismo de coherencia ante el CEPD, organismo encargado de dirimir la controversia entre autoridades de control. Para comenzar a explicar este mecanismo es importante recordar que las autoridades de control deberán informar a la autoridad de control principal sobre la existencia de reclamaciones o investigaciones abiertas de hechos previstos como infracciones en el RGPD, si estas se refieren únicamente al establecimiento del responsable o encargado situado en territorio de su competencia o, afecte a los interesados en el territorio de su Estado miembro. De manera que la autoridad de control principal valore si debe o no llevar a cabo el mecanismo de cooperación del art. 60 del RGPD en un plazo de tres semanas. Este mecanismo de cooperación funciona como bien lo señala el Profesor TRONCOSO REIGADA como «*un sistema de ventanilla única en los tratamientos transfronterizos*

[485] Cfr. Art. 4.16 del RGPD.
[486] Arts. 56.1 y 56.6 RGPD.

que atribuye como regla general la competencia de la autoridad de control principal»[487]. Lo anterior inhibe la tramitación paralela de procedimientos en las distintas autoridades de control en la UE.

Cuando la autoridad de control principal decida llevar la tramitación de dicho caso con arreglo al mecanismo de cooperación del art. 60, la autoridad de control informante podrá presentarle a esta un proyecto de decisión. Este proyecto deberá ser tomado en cuenta por la autoridad de control principal al preparar su proyecto de decisión. Por el contrario, si la autoridad de control principal decide no tratar el caso conforme al art. 60, la autoridad de control informante tratará el asunto conforme a lo establecido por los arts. 61 y 62, relativos a la asistencia mutua entre autoridades de control y a las operaciones llevadas a cabo conjuntamente por estas[488].

Ya que se ha planteado el esquema de los mecanismos de cooperación y asistencia mutua resulta importante explicarlos de manera separada. El mecanismo de cooperación del art. 60 es un procedimiento instruido por la autoridad de control principal a fin de llegar a un consenso. Primeramente, se tiene que puntualizar que estas comunicaciones deberán llevarse a cabo de manera electrónica y por medio de formularios normalizados[489]. Este sistema presenta varias ventajas sobre todo para los ciudadanos, ya que evita que los interesados que estimen vulnerado su derecho de protección de datos por un responsable o un encargado que trata datos de manera transfronteriza tengan que acudir a la autoridad de control donde se encuentre el establecimiento principal. Otro problema que se evita es lidiar con la barrera idiomática que existiría entre el personal de la autoridad de control y el interesado[490].

Continuando con el procedimiento del sistema de cooperación, cuando la autoridad de control principal decida optar por este procedimiento y presente su proyecto de decisión a la autoridad de control interesada, esta última tendrá la posibilidad de objetar este en un plazo de cuatro semanas. Si no se realizasen

[487] TRONCOSO REIGADA, A., «XXVI. Autoridades (…)», *op. cit.,* p. 497. En este mismo sentido
[488] Arts. 56.5 y 60.2 del RGPD.
[489] Art. 60.12 del RGPD.
[490] En este mismo sentido Cfr. LÓPEZ CALVO, J. *op. cit.,* p. 639.

objeciones se considerará que las autoridades de control están de acuerdo y quedarán vinculadas por este[491]. Por el contrario, si la autoridad de control interesada objetara el proyecto de decisión de la autoridad de control principal, esta última podrá: a) no seguir con lo indicado en la objeción o estimar que no es pertinente o no está motivada, en este caso someterá el asunto al mecanismo de coherencia en cuyo caso el CEPD deberá emitir un dictamen al respecto, de acuerdo con el art. 63 del RGPD[492]; b) seguir con lo que le fue indicado en la objeción de la autoridad de control interesada, en este caso presentará un proyecto de decisión revisado ante las demás autoridades de control interesadas para ser sometido a consulta en un plazo de dos semanas. Si ninguna de las autoridades de control interesadas presentase objeciones a este nuevo proyecto de decisión, se entenderá que todas las autoridades están de acuerdo con dicho proyecto y quedarán vinculadas por este[493].

Adoptada la decisión por la autoridad de control principal, se deberá notificar la resolución según sea el caso: a) al establecimiento principal, b) al establecimiento único del responsable o, c) al encargado del tratamiento; a la que deberá acompañar un resumen sobre los hechos y la motivación. También se informará de la decisión a las autoridades de control interesadas y al CEPD. En todo caso, será la autoridad de control ante la que se presentó la reclamación la que debe notificar al reclamante[494]. Recibida la resolución por el responsable o encargado, según sea el caso, este adoptará las medidas necesarias para garantizar el cumplimiento de la decisión en todos sus establecimientos en la UE en relación con las actividades de tratamiento que realice. Una vez adoptadas estas medidas serán notificadas a la autoridad de control principal, la cual se encargará de informar a las demás autoridades de control interesadas.

Las decisiones que rechacen o desestimen una reclamación, han de ser adoptadas y notificadas por la autoridad de control ante la cual se presentó dicha

[491] Art. 60.6 del RGPD.
[492] *Vid.* arts. 60.4, 63, 64 y 70.1 t) del RGPD. Tal y como lo establece el Profesor IRURZUN MONTORO el rechazo de las objeciones por la autoridad principal activa el mecanismo de coherencia del art. 63, Cfr. IRURZUN MONTORO, F., *op. cit.,* p. 516.
[493] Art. 60.6 del RGPD.
[494] Art. 60. 7 del RGPD.

reclamación, dando a conocer igualmente al responsable el sentido de la decisión[495]. Lo anterior cobra sentido si pensamos en el sistema de ventanilla única, de tal manera que los interesados podrán recurrir dicha decisión dentro del territorio de su Estado miembro[496].

Cuando una reclamación sea parcialmente favorable esta deberá ser resuelta por distintas autoridades de control de forma separada. La autoridad de control principal resolverá y notificará al establecimiento principal la parte favorable referente a acciones relacionadas con el responsable del tratamiento, y también notificará de ello al reclamante. En cuanto a la parte desfavorable, bien por haberse desestimado o rechazado, la autoridad de control ante la que se haya presentado la reclamación será la encargada de resolver y notificar la decisión al reclamante, e informará sobre este asunto al responsable o al encargado según sea el caso[497]. Este procedimiento puede resultar un tanto confuso, sin embargo, recientemente el CEPD ha publicado una figura que puede hacer más fácil la comprensión del contenido del art. 60 del RGPD bajo el nombre de «procedimiento de ventanilla única», en el que también se puede apreciar la intervención del CEPD y el mecanismo del art. 65 del RGPD (Figura 4).

Otras formas de cooperación entre autoridades de control son los instrumentos de asistencia mutua, regulados en los art. 61 y 62 del RGPD. El primero de estos dos artículos establece que las autoridades de control se facilitarán informaciones y prestarán asistencia específicamente en lo relativo a las solicitudes de información y medidas de control, que suelen traducirse en llevar a cabo autorizaciones, consultas previas, inspecciones e investigaciones por la autoridad de control requerida en su territorio. Las solicitudes de asistencia deberán contener toda aquella información necesaria que se relacione con la finalidad y motivos de la solicitud.

---

[495] Art. 60.8 del RGPD.

[496] En este sentido el Profesor LÓPEZ CALVO indica que: «*La razón presumible para ello, como se ha expuesto, es la de habilitar el recurso ante los tribunales de su EM al perjudicado. Bien sea el sancionado que recurrirá ante los tribunales de la ACP. Bien el denunciante al que se ha desestimado su pretensión, que recurrirá ante los tribunales de la autoridad de residencia*», Cfr. LÓPEZ CALVO, *op. cit.,* p. 647.

[497] Art. 60.9 RGPD.

El intercambio de información que lleven a cabo las autoridades de control con motivo de asistencia mutua solo podrá ser usada para los motivos expresados en la solicitud, y será facilitada por medios electrónicos, utilizando un formato normalizado. En relación la transmisión de la información de acuerdo con el Profesor LÓPEZ CALVO: «*Debe deducirse, aunque no se incluye previsión alguna al respecto, que la información deberá enviarse cifrada teniendo en cuenta que incluirá en particular, la información pertinente sobre el desarrollo de una investigación*»[498].

En los apartados posteriores se realiza una descripción procedimental sobre la tramitación de este tipo de solicitudes. Recibida la solicitud por la autoridad de control, esta podrá: a) adoptar todas aquellas medidas necesarias para responder a dicha solicitud en el plazo máximo de un mes y notificarle a la autoridad de control requirente los resultados obtenidos, b) negarse a responder en el caso de que no sea competente para atender al objeto de la solicitud o ejecutar lo que se le solicita o, c) negarse a responder si la respuesta a la solicitud implicaría una infracción al RGPD, al Derecho de la Unión o al Derecho de la autoridad de control requerida. Cuando la autoridad de control requerida no facilite información en el plazo de un mes contado a partir de la fecha de su recepción, la autoridad de control requirente podrá adoptar medidas provisionales cuando exista una urgente necesidad como la protección de derechos y libertades de los interesados, con un periodo de validez no mayor a tres meses y, remitirá el asunto al CEPD para que adopte un dictamen o una decisión urgente vinculante. Las medidas provisionales adoptadas por la autoridad del Estado requirente deberán ser notificadas a las otras autoridades de control interesadas, al CEPD y a la Comisión.

Las autoridades de control que asistan a otras autoridades de control no cobrarán tasas por las medidas acordadas, excepcionalmente, las autoridades de control podrán convenir normas de indemnización por gastos específicos. En relación con lo anterior, el Profesor IRURZUN MONTORO determina que este «*aspecto no dejara de tener su relevancia en el caso de aquellas autoridades que tengan más frecuentemente la condición de interesadas o requeridas y menos la de la autoridad de control principal, pues estas son las que, simplificando, obtendrían unos mayores*

[498] López Calvo, J., *op. cit.,* p. 674.

ingresos vía tasas o sanciones económicas, para las que habrán contado con asistencia obligatoria del resto de las autoridades»[499].

Las autoridades de control conforme al art. 62 del RGPD también pueden realizar operaciones conjuntas, como investigaciones o medidas de ejecución en el que participen miembros o personal de autoridades de control de otros Estados miembros. Lo que habilita o da derecho a las autoridades de control para poder participar en este tipo de operaciones es el tratamiento de datos personales trasfronterizo, específicamente, cuando el responsable del tratamiento o el encargado tenga establecimientos en varios Estados miembros o afecte significativamente a interesados de más de un Estado miembro.

Sin embargo, la redacción de este instrumento de asistencia mutua es bastante farragosa, por una parte, se establece que será la autoridad de control principal la encargada de invitar a las demás autoridades de control a participar en las operaciones conjuntas y, en su caso, de aceptar las solicitudes de las autoridades de control a participar en dichas operaciones conjuntas. El plazo para invitar y responder a las solicitudes será de un mes, en el caso de que la autoridad de control de origen o principal no contestase una solicitud de otra autoridad de control con derecho a participar en operaciones conjuntas, se podrán adoptar medidas provisionales urgentes por la autoridad de control requirente, de acuerdo con lo establecido en los apartados 1 y 2 del art. 66, en cuyo caso el CEPD tendrá que adoptar una decisión de carácter vinculante en forma de Dictamen o decisión vinculante urgente[500].

Ahora bien, se establece la posibilidad de que una autoridad de control pueda conferir poderes, incluidos poderes de investigación para participar en operaciones conjuntas a miembros o al personal de control de origen con arreglo a la legislación de su Estado y con la autorización de la autoridad de control de origen. Cabe señalar que en ninguna otra parte del RGPD incluidos los considerandos se hace referencia a lo que debe entenderse como «la autoridad de control de origen», sin embargo, se deduce que es la que inicia el procedimiento de las operaciones conjuntas, que será

[499] IRURZUN MONTORO, F., *op. cit.,* p. 516.
[500] Los dictámenes y decisiones vinculantes hasta le fecha se pueden consultar en el siguiente enlace: https://edpb.europa.eu/our-work-tools/consistency-findings_es (consulta:3 de febrero de 2020).

siempre la autoridad de control principal. También las autoridades de control cuentan con la posibilidad de aceptar que miembros o personal de la autoridad de control de origen ejerzan poderes de investigación en el Estado miembro de la autoridad de control de acogida, en la medida que lo permita el Derecho del Estado de esta última, estos miembros o personal de la autoridad de control de origen ceñirán su actuación al Derecho de ese Estado y quedarán sujetos al mismo. Se deduce que el legislador comunitario cuando se refiere a la «autoridad de control de acogida» hace referencia a la autoridad de control competente territorialmente para llevar a cabo la investigación en el territorio de su Estado. El ejercicio de los poderes de investigación conferidos a miembros o personal de la autoridad de control de origen o principal, solo podrán llevarse a cabo bajo la orientación y presencia de miembros o personal de la autoridad de control de acogida.

El artículo 62 realiza un marco de responsabilidad de las autoridades de control en el ejercicio de los poderes de investigación en el Estado de la autoridad de control de acogida. Aunque la redacción continúa siendo farragosa pues literalmente se establece en el apartado cuatro que cuando participe «*personal de la autoridad de control de origen en operaciones en otro Estado miembro, el Estado miembro de la autoridad de control de acogida asumirá la responsabilidad de acuerdo con el Derecho del Estado miembro en cuyo territorio se desarrollen las operaciones, por los daños y perjuicios que haya causado dicho personal en el transcurso de las mismas*». Resulta bastante confuso el hecho de que aun determinando que la autoridad de control de acogida sea quién asuma la responsabilidad del personal de la autoridad de control de origen cuando causen daños y perjuicios en el transcurso de las actuaciones, el RGPD haga referencia al Derecho del Estado miembro dónde se desarrollen las operaciones, pues como bien sabemos no se puede asumir esa responsabilidad conforme al derecho de otro Estado miembro, ya que como marca la lógica se tiene que acudir a las leyes del Estado donde se originó el daño. Puede que la redacción sea confusa porque parecería que se está hablando de un tercer Estado donde se desarrollan las operaciones y no del Estado donde territorialmente tiene competencia la autoridad de acogida, y que la autoridad de este último Estado, la de acogida, tuviese que asumir la responsabilidad conforme a las leyes del Estado dónde se desarrollan las operaciones, cuando en realidad es la misma.

En relación con la reparación de los daños causados en diligencias realizadas por dos autoridades de control, se establece en el apartado cinco del art. 62 que el «*Estado miembro en cuyo territorio se causaron los daños y perjuicios asumirá su reparación en las condiciones aplicables a los daños y perjuicios causados por su propio personal. El Estado miembro de la autoridad de control de origen cuyo personal haya causado daños y perjuicios a cualquier persona en el territorio de otro Estado miembro le restituirá íntegramente los importes que este último haya abonado a los derechohabientes*». Este epígrafe debe estudiarse en dos partes, la primera se refiere a la reparación del daño causado por personal de la autoridad de control de origen, en relación con esto no hay mucho que comentar pues es como normalmente se asume la reparación de los daños y perjuicios en cada Estado miembro (con sus matices). La segunda parte habla de la restitución de importes, la cual deberá ser llevada a cabo por el Estado de la autoridad de control de origen cuando esta última los haya abonado con motivo de los daños o perjuicios causados a sus derechohabientes. Esto nos hace pensar que inicialmente quien asume la restitución total por los daños o perjuicios causados a terceros es el Estado de la autoridad de control de acogida, pudiéndole solicitar al Estado de la autoridad de control de origen el importe que resulte de los daños causados por los miembros o personal de su autoridad de control.

En el epígrafe seis del artículo del RGPD antes referido se determina que los Estados miembros deberán renunciar a solicitar el reembolso de los daños o perjuicios causados con motivo de las operaciones conjuntas, realizados por miembros o personal de la autoridad de control de origen, sin perjuicio de los daños causados a personas o derechohabientes según sea el caso. Lo que puede traducirse en que, al asumir la responsabilidad de miembros o personal de la autoridad de control de origen, si estos le causaran un daño al Estado donde se desarrollan esas labores de investigación, este último bajo este supuesto renunciará al reembolso por dichos daños o perjuicios, pues a la letra de este artículo asume la responsabilidad[501].

[501] Cfr. apartado 4 del art. 62 en relación con el apartado 5 del mismo artículo del RGPD.

Además de los medios de cooperación otro mecanismo que contribuye a una correcta aplicación del contenido del RGPD es el mecanismo de coherencia. Este será tramitado y resuelto por el CEPD. Se puede acceder a este por dos motivos, bien dirimir una controversia entre autoridades de control o que se emita un dictamen sobre determinados asuntos por el Comité. En este último caso este dictamen podrá tener carácter preceptivo o potestativo.

Tendrá carácter preceptivo cuando una autoridad competente manifieste su intención de adoptar alguna medida que suponga: la realización de una evaluación de impacto a determinados tratamientos de datos, la adopción de cláusulas tipo, la autorización de cláusulas contractuales, de normas corporativas vinculantes o la aprobación de un código de conducta o certificación; o bien determinar si alguno de estos instrumentos es conforme al contenido del RGPD.

El dictamen del Comité tendrá carácter potestativo cuando tenga como finalidad obtener un pronunciamiento sobre la aplicación coherente de determinados aspectos previstos en el reglamento, en palabras de LÓPEZ CALVO sería un medio de unificación de criterios[502]. Este dictamen podrá tener efectos en más de un Estado miembro si se ha solicitado así por alguna autoridad de control, por la Comisión o por considerarlo así el presidente del Comité, especialmente si tiene que ver con el cumplimiento de obligaciones de asistencia mutua entre autoridades de control.

En caso de no prosperar la cooperación entre autoridades de control se podrá acudir al CEPD a fin de que determine una solución coherente y vinculante, de acuerdo con los arts. 63 y 65. En palabras de IRURZUN MONTORO se trata de un «*modo de facilitar la aplicación lo más homogénea posible entre diversas autoridades*»[503]. En este caso el CEPD deberá emitir un dictamen motivado y dirigido a la autoridad de control principal y a las demás interesadas, en el plazo de un mes, adoptado por la mayoría de dos tercios de sus miembros. Con base en este dictamen posteriormente

[502] El cual deberá ser instado por una autoridad de control o por la Comisión, *vid.* LÓPEZ CALVO, J., *op. cit.,* pp. 650-651.
[503] IRURZUN MONTORO, F., *op. cit.,* p. 521.

se deberá adoptar una decisión definitiva por la autoridad de control competente en términos de lo establecido en los apartados 7,8 y 9 del art. 60.

Finalmente, el CEPD puede intervenir de manera urgente cuando sea necesario «proteger los derechos y libertades del interesado» instado por una autoridad de control interesada. En cuyo caso por obvias razones se reduce el plazo a dos semanas para emitir un dictamen o una decisión vinculante urgente, de conformidad con lo establecido en el art. 66 del RGPD. De manera que se adopten medidas encaminadas para proteger los derechos de los interesados siempre que se justifiquen dichas razones, ya que, de manera contraria la autoridad de control competente deberá instar su intervención por los cauces ordinarios.

1.4 Régimen de infracciones y sanciones en el RGPD

El RGPD establece un régimen de infracciones y sanciones relacionado con el derecho a la protección de datos. Se establece de forma generalizada la multa como medio de sanción por la comisión de infracciones establecidas en el RGPD. Las infracciones están contempladas en los epígrafes cuatro, cinco y seis del art. 83.

El apartado cuatro del referido artículo establece conductas que son consideradas como infracciones, los sujetos responsables de su comisión pueden ser: el responsable, el encargado y los organismos de certificación. De manera general se establece que la vulneración de determinados artículos constituye una infracción, la responsabilidad de las infracciones depende del incumplimiento de obligaciones de determinados sujetos que intervienen en el tratamiento de los datos personales, por ejemplo, si el RGPD determina una obligación a cargo del responsable y este la incumple, pero además se contempla como una infracción, será responsable de la misma y la autoridad de control podrá sancionarle. El apartado a) del artículo arriba referido establece una serie de infracciones a cargo de los responsables y encargados del tratamiento. A efectos de tener un panorama claro de responsabilidad por la comisión de una infracción las clasificaremos según a quien la cometa. Son infracciones cometidas por el responsable o por los corresponsables [504]: 1) el incumplimiento de las condiciones de consentimiento de

[504] Si son más de dos personas quienes fijan los objetivos y los medios del tratamiento, de acuerdo con el art. 26 del RGPD.

los menores establecido en el art. 8 y que a su vez tiene relación con la base del tratamiento del art. 6.1.a) del RGPD; 2) la conservación, obtención y tratamiento de información adicional si la finalidad del tratamiento no requiere la identificación de los interesados o ya no la requiere; 3) si no toman medidas técnicas y organizativas adecuadas para llevar a cabo el tratamiento de datos conforme al art. 25; 4) la falta de designación de un representante en la Unión si fuese el caso, de acuerdo con el contenido del art. 27; 5) no llevar un registro de tratamiento de acuerdo con el art. 30 (si el responsable no se encuentra dentro del territorio de la UE, su representante será el obligado a llevar un registro); 6) no cooperar con la autoridad de control; 7) no aplicar medidas técnicas y organizativas para salvaguardar la seguridad de los datos personales (art. 32) ;8) la falta de notificación a la autoridad de control y a los interesados sobre las violaciones de seguridad (arts. 33 y 34); 9) la ausencia de la evaluación de impacto, así como las obligaciones derivadas de la misma establecidas en el art. 35; 10) no haber consultado de manera previa a la autoridad de control si la evaluación de impacto refleja alto riesgo en los derechos y las libertades de los interesados según el contenido del art. 36; 11) no haber designado a un delegado de protección de datos (art. 37); 12) no respetar la independencia y posición del delegado de protección de datos de tal manera que no pueda desempeñar correctamente sus funciones (arts. 38 y 39) y no cumplir lo referente al sistema de certificación contemplado en los arts. 42 y 43.

Se considerarán infracciones la vulneración de una obligación a cargo del encargado relacionadas con: 1) la falta de observancia de las medidas relacionadas con el consentimiento de menores, si el encargado ha sido el que ha recabado el consentimiento (art. 8); 2) el incumplimiento de las obligaciones como encargado del tratamiento del art. 28; 3) la falta de designación de un representante si el encargado no estuviese establecido en la Unión, conforme con el art. 27; 4) no llevar a cabo el tratamiento de datos bajo las órdenes del responsable (art.29); 5) no cooperar con la autoridad de control; 6) no aplicar medidas técnicas y organizativas para salvaguardar la seguridad de los datos personales(art. 32); 7) la falta de notificación a la autoridad de control y a los interesados sobre las violaciones de seguridad (arts. 33 y 34); 8) no haber designado a un delegado de protección de datos (art. 37); 9) no respetar la independencia y posición del delegado de

protección de datos, de tal manera que no puedan desempeñar correctamente sus funciones (arts. 38 y 39); y 10) la falta de cumplimiento de las obligaciones asumidas por algún mecanismo de certificación (art. 42 y 43).

El inciso b) del art. 83.4 del RGPD establece una serie de infracciones cuyos responsables de la comisión son los organismos de certificación. Estos cometerán una infracción si incumplen las obligaciones de los artículos 42 y 43 del RGPD. El inciso c) de este mismo artículo considera como infracción el incumplimiento de las obligaciones de las autoridades de control relacionadas con el contenido del art. 41.4, aunque este último regula las medidas que deberán adoptar los organismos de certificación en caso de que sean infringidos los códigos de conducta por responsables o encargados, así como su notificación a la autoridad de control. Esta resulta cuanto menos curiosa, sobre todo por el hecho de que una autoridad no puede ser juez y parte en la determinación de su responsabilidad y menos se podrá autoimponer una multa, aunque no sea de carácter económico. Es por ello que este caso se antoja inviable, sobre todo porque las autoridades de control tienen delimitadas sus competencias materiales y territoriales. Una alternativa de solución sería acudir ante el CEPD y hacer de su conocimiento esta situación para que emita una recomendación o especifique los requisitos del art. 43, ya que no tiene competencia para ejercer la potestad sancionadora.

La comisión de alguna de las conductas antes descritas se considerará una infracción y podrá ser sancionada con multas, cuya cuantía máxima podrá ser de diez millones de euros. En caso de que la infracción sea cometida por una empresa podrá ser el equivalente «*al 2% como máximo del volumen de su negocio total anual global del ejercicio financiero anterior*», optándose en su caso por la multa de mayor cuantía.

El apartado cinco del art. 83 del RGPD, establece otras infracciones, sin embargo, no están vinculadas a un agente específico en el tratamiento de datos personales. Se consideran como infracciones las vulneraciones: «*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». El apartado cinco de este artículo contempla infracciones que podrán ser cometidas por todos los agentes intervinientes en el tratamiento de datos al resultar obligaciones genéricas. Dicho esto, la vulneración de las disposiciones descritas en el apartado 5 del art. 83, se sancionarán con multas de hasta veinte millones de euros, y si son cometidas por alguna empresa se le podrá sancionar con «*una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía*».

El apartado seis contempla un solo supuesto de infracción y no señala el sujeto activo de la infracción. Cualquier agente interviniente en el tratamiento de datos personales que incumpla las resoluciones de la autoridad de control competente, podrá ser sancionado con una multa de hasta veinte millones de euros. En caso de que la infracción sea cometida por una empresa podrá ser sancionada con «*una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía*».

Estas multas administrativas pueden imponerse con motivo de los poderes correctivos que le son atribuidos a las autoridades de control. Las multas deberán ser impuestas observando los parámetros establecidos en el art. 83.2 en cada caso concreto, de manera que, resulten efectivas, proporcionadas y disuasorias. Los parámetros a tener en cuenta son: la naturaleza, la gravedad, la duración de la infracción, el número de interesados afectados, los daños y perjuicios sufridos; si las infracciones son cometidas con intencionalidad o negligencia; las medidas tomadas por el responsable o encargado del tratamiento para aminorar los daños y perjuicios de los interesados; el grado de responsabilidad de los agentes intervinientes con base en las medidas técnicas y organizativas por diseño y por defecto o de seguridad adoptadas por cada uno de ellos; el grado de cooperación con las autoridades de control, las categorías de datos relacionadas con la comisión de la infracción; si se dio parte de la infracción a la autoridad por el responsable o el encargado del

tratamiento; si el responsable o el encargado se habían adherido a códigos de conducta o a mecanismos de certificación. Para la imposición de multas en relación con los poderes correctivos de las autoridades de control, si estas fueron ordenadas de manera previa al responsable o al encargado del tratamiento, y si estas fueron cumplidas o no; así como «*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*».

Si se determinase que los responsables o encargados del tratamiento han cumplido de forma intencionada o negligente las conductas consistentes en infracciones o las obligaciones derivadas de esa actividad, podrán ser sancionados con una multa administrativa que no deberá superar la cuantía de las infracciones consideradas más graves. Esta cuantía no podrá ser superior a veinte millones de euros o tratándose de empresas al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior.

La imposición de multas administrativas por las autoridades de control estará sujeta y respetará las garantías procesales establecidas en el derecho del Estado miembro donde sea competente y el en derecho de la Unión, como la tutela judicial efectiva.

En el caso de Dinamarca y Estonia donde no se prevé la imposición de multas de carácter administrativo, será la autoridad de control quien las incoe y los tribunales quienes las impongan. Estos Estados deberán garantizar que las multas sean efectivas y equivalentes a las de carácter administrativo impuestas por las autoridades de control, es decir, individuales, efectivas, proporcionadas y disuasorias.

Adicionalmente, el art. 84 prevé la posibilidad de que los Estados miembros puedan establecer normas que prevean otro tipo de sanción a las infracciones que se establecen en el RGPD, así como la adopción de medidas necesarias para garantizar su observancia y, que esas sanciones en todo caso sean efectivas, proporcionadas y disuasorias. También corre a cargo de los Estados informar a la Comisión la adopción de leyes que contengan otro tipo de sanción aplicable a las infracciones contempladas en el RGPD. Se atribuye a los Estados establecer normas

en donde se determine si se puede y en qué medida imponer multas de carácter administrativo a sus organismos y autoridades públicas.

1.5 Autoridades de control en España.

1.5.1 La Agencia Española de Protección de Datos, novedades del RGPD.

La primera ley de protección de datos en España [505], anterior incluso a la normativa europea en la materia, ya preveía la creación de una agencia que garantizara el cumplimiento de la normativa de protección de datos. La aprobación de la Directiva 95/46/CE también preveía la creación de una agencia con esa finalidad y también está previsto así en la CDFUE [506]. Por tanto, se incluía en la norma de transposición española [507]. Por supuesto, la LO 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales en cumplimiento de lo dispuesto en el RGPD incluye la regulación de la Agencia Española de Protección de Datos y de algunas previsiones de carácter ordinario relativas a las agencias a autonómicas. Actualmente, a nivel Autonómico, existen dos agencias independientes en materia de protección de datos personales, la de la Comunidad Autónoma de Cataluña y la del País Vasco. Sin perjuicio, de la existencia del Consejo de Transparencia y protección de datos de Andalucía, el cual es parte de la administración institucional de esa Comunidad Autónoma con competencias atribuidas en esta materia. Como vemos en España tradicionalmente se ha adoptado por la terminología americana para nombrar a la autoridad de control en la materia como «Agencia». Sin embargo, todas las autoridades de control constituidas en España, de este tipo son «*autoridades de garantía*» [508], del derecho fundamental a la protección de datos personales.

Como hemos visto anteriormente, estas autoridades de control tienen un papel crucial en la correcta aplicación de los principios y demás previsiones establecidas en el RGPD como en la ley nacional en la materia, sobre todo en relación con el ejercicio de los derechos establecidos en la normativa por los ciudadanos

[505] LO 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD).
[506] Cfr. Art. 8.3 de la CDFUE.
[507] Cfr. art. 35 y ss. de la LO 15/1999, de 13 de diciembre.
[508] FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales en las Administraciones Públicas,* Thomson Civitas, 2003, p. 396.

frente a responsables o encargados que realicen tratamientos transfronterizos, las actuaciones entre agencias en relación con la asistencia mutua, las actuaciones conjuntas y los mecanismos de cooperación y coherencia. Por lo que resulta necesario conocer cuáles son las autoridades de control existentes en España, sus potestades y obligaciones de acuerdo con el marco jurídico nacional que complementa lo establecido en el RGPD.

La Agencia Estatal de protección de datos se ha configurado desde su primera regulación como una autoridad administrativa independiente (AAI), y así lo ratifica el art. 44 de la LOPDGDD, que la define como una autoridad con plena independencia funcional relacionada con el Gobierno a través del Ministerio de Justicia (art. 44.1 LOPDGDD y 109.1 de la Ley 40/2015)[509].

Este tipo de autoridades se rigen por el contenido en su ley de creación, es decir, que se someterá a lo establecido por el RGPD, la LO 3/2018, sus Estatutos, y de manera supletoria por el contenido de las leyes administrativas españolas, en cuanto a su función o actividad. Ahora bien, no solo porque estas sean calificadas por la norma como una autoridad independiente lo son, para ello como establece el Profesor TRONCOSO REIGADA, dicha independencia «*tiene que traducirse en unas técnicas organizativas concretas. Por tanto, es la presencia de unas garantías formales y sustanciales de independencia lo que permite afirmar que estamos ante una Administración Independiente*»[510].

Primeramente, es pertinente determinar en qué consiste la garantía sustancial de independencia de esta autoridad, que equivaldría a neutralidad, ya que en este caso la AEPD de conformidad con lo que establece la LOPDGDD no admite instrucciones de ningún otro poder público sobre cómo llevar a cabo su labor, la cual es garantizar el cumplimiento del derecho a la protección de datos personales, tal y

[509] Se trata de una autoridad administrativa independiente de ámbito estatal regulada por los arts. 109-110 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), es decir, que forma parte de las denominadas «Autoridades Administrativas Independientes» (AAI). Tal y como lo ordena el RGPD, la LO 3/2018 que complementa a este último, también la contempla como una autoridad con plena independencia funcional y relacionada con el Gobierno a través del Ministerio de Justicia (art. 44.1 LOPDGDD y 109.1 de la ley 40/2015).

[510] TRONCOSO REIGADA, A., «Las agencias de protección de datos como administración independiente», PAUNER CHULVI, C. y TOMÁS MALLÉN, B. (coord.), *Las Administraciones independientes*, Tirant lo Blanch, Valencia, 2009, p.169.

como lo establecen las disposiciones del RGPD y en la LO 3/2018. Esto implica que la AEPD debe permanecer ajena a los intereses políticos del gobierno ya que su función es meramente jurídica. Sin embargo, como bien apunta el Profesor TRONCOSO REIGADA en relación con las AAI: «*la independencia de estos entes no destruye su pertenencia a la Administración Pública, y, por tanto, al poder ejecutivo. Es decir, el hecho de que estos organismos no estén concebidos como subordinados del poder ejecutivo, no los convierte en una prolongación del poder legislativo –como lo son el Defensor del Pueblo o el Tribunal de Cuentas-, ni en una Autoridad Judicial. No son, por tanto, simples órganos independientes, sino auténticas Administraciones Independientes*»[511].

El apartado 2 del art. 48 de la LOPDGDD determina que la Presidencia de la AEPD como titular, y su Adjunto, quien auxiliará esta última deberán actuar con independencia y objetividad en el desempeño de sus funciones. Antes de continuar, es necesario destacar que la LO 3/2018, apuesta por un modelo diferente al anterior, por lo que las funciones y competencias de su titular ahora no están concentradas en una sola persona[512]. La Presidencia puede delegar funciones al Adjunto, salvo las relativas a los procedimientos relacionados con la posible vulneración de la normativa de protección de datos, conforme con el Título VIII de la LO 3/2018, y a lo establecido también en su Estatuto[513]. La LO establece que la AEPD estará representada por la Presidencia de la Agencia[514], esta persona estará asesorada por

[511] *Ib.*, p. 47.
[512] En este sentido RUBÍ NAVARRETE, J., «La Agencia…», 2020, *op. cit.,* p. 97.
[513] La Disposición transitoria primera del al LOPDGDD, determina que el Estatuto de la Agencia Española de Protección de Datos (R.D. 428/1993, de 26 de marzo) continuará estando vigente en lo que no se oponga al título VIII, es decir, en lo relativo a los procedimientos en caso de posible vulneración de la normativa de protección de datos, el cual se regulan las formas de iniciación de procedimientos y su duración, la admisión a trámite de las reclamaciones, la determinación del alcance del personal, las actuaciones previas de investigación, el acuerdo de inicio del procedimiento para el ejercicio de la potestad sancionador y las medidas provisionales y garantía de los derechos, previsto de los arts. 63 al 69 de la ley.
[514] La presidencia estará asistida *ad intra* por distintas unidades de apoyo en materia jurídica, relaciones internacionales, tecnologías de la información y difusión en medios de su actividad, con el fin de proveer, las cuales le permitirán desempeñar sus funciones y poderes de manera correcta, *vid.* AEPD, Información de carácter institucional, organizativa y de planificación. Disponible en: https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/organigrama-AEPD/la-directora (consulta 15 de noviembre de 2020). De acuerdo con RUBÍ NAVARRETE es de reciente creación la Unidad de Evaluación y Estudios Tecnológicos, la cual está «*dirigida a establecer contactos con empresas, universidades y, en general,*

un Consejo Consultivo, cuyos integrantes deberán ser expertos en la materia y nombrados por el Ministerio de Justicia[515]. Sin embargo, la LOPDGDD evidencia su independencia sustancial cuando determina que las decisiones tomadas por este Consejo Consultivo no tendrán carácter de vinculante respecto a las decisiones tomadas por la Presidencia o por el Adjunto de la AEPD[516].

En relación con las garantías formales que aseguran esa independencia, en primer lugar, nos vamos a referir a la relativa al nombramiento de su titular. Este nombramiento corresponde al Gobierno a propuesta del Ministerio de Justicia, «*entre personas de reconocida competencia profesional, y en particular en materia de protección de datos*»[517]. El art. 48.3 de la LOPDGDD, establece el procedimiento que deberá llevarse a cabo cuando se designe al nuevo titular de la agencia, sea bien por expirar su mandato o por que se presente alguna de las causas de cese del mismo. Dos meses antes a la expiración del mandato o en su defecto el Ministerio de Justicia ordenará en el BOE «*la convocatoria pública de candidatos*» en caso de que se haya producido su cese. Previo estudio de la idoneidad para desempeñar el cargo, el Gobierno deberá remitir al Congreso de los Diputados una propuesta acerca de quiénes deberán ocupar el cargo, quien ostentará la presidencia de la AEPD, y del Adjunto, acompañado de un informe por el cual se justifique su idoneidad. Tras la audiencia preceptiva de los candidatos ante la Cámara, la propuesta deberá ser ratificada por la Comisión de Justicia por tres quintos de sus miembros en primera votación o por mayoría absoluta en segunda votación, si en la primera no se

todo tipo de agentes que intervengan en desarrollos tecnológicos para analizar sus implicaciones en la protección de los datos personales. Adicionalmente, la UEET es la Unidad que analiza inicialmente las notificaciones de quiebras de seguridad de forma separada a la Subdirección general de inspección de datos de forma que las notificaciones obligatorias que exige el Reglamento no sean consideradas como responsables o encargados del tratamiento como una autoinculpación que conduzca por sí misma a la apertura de un procedimiento por infracción de la norma», Cfr. RUBÍ NAVARRETE, J., «La Agencia…», 2020, pp. 100-101.

[515] Art. 49.2 de la LOPDGDD y art. 11 RD. 428/1993, de 26 de marzo.

[516] Art. 49.5 de la LOPDGDD. Para RUBÍ NAVARRETE, J. las «*consideraciones sobre las limitadas funciones del Consejo Consultivo no resultan congruentes con la pluralidad de entidades de todo tipo que, durante la tramitación del proyecto de ley, han insistido a los grupos parlamentarios y han conseguido garantizar su incorporación como miembros natos del Consejo Consultivo. De lo que cabe concluir que, o bien que pese a estas consideraciones hay un reconocimiento explícito de la utilizada de integrar el Consejo Consultivo. O, complementariamente con lo anterior, que los agentes que han promovido su incorporación al Consejo Consultivo están particularmente interesados en multiplicar las sugerencias de asesoramiento que la Ley atribuye al Consejo*», Cfr. RUBÍ NAVARRETE, J., «La Agencia…» , 2019, *op. cit.,* p. 502.

[517] Art. 48.3 de la LOPDGDD.

alcanzase dicho porcentaje. En la segunda votación, la propuesta deberá ser ratificada, aceptada y votada por Diputados de grupos Parlamentarios diferentes para finalmente ser nombrados por el Consejo de Ministros mediante Real Decreto.

Por tanto, el procedimiento anterior deja entrever, por una parte, el carácter neutral de la Presidencia y del Adjunto, al estar involucrados en su nombramiento más de dos poderes del Estado y en consenso con otras fuerzas de carácter político en segunda votación. Por otra parte, el carácter específico en la cualificación del candidato robustece esa neutralidad, que en palabras de TRONCOSO REIGADA: «*una persona mejor formada puede tener criterio propio para librarse de las presiones políticas, para evitar la captura de los sectores regulados o para verse absorbida por la burocracia, sino también el buen desempeño de su actividad*»[518].

Otra garantía formal que se contempla en la LOPDGDD tiene que ver con el nombramiento de las personas que ocuparán tanto la Presidencia como el puesto de Adjunto, especialmente en relación con la duración de su mandato. Con esta nueva ley la duración de ambos cargos será de cinco años[519], prorrogables por otro periodo igual, siempre y cuando no se dé ninguna de las causas de cese establecidas en el apartado 5 del art. 48 de la LOPDGDD[520]. En los casos de incumplimiento grave de sus funciones, incapacidad sobrevenida o incompatibilidad para ejercer el cargo, su cese deberá someterse a votación parlamentaria, en primera votación tendrá que ser aprobado por tres quintas partes y en caso de no alcanzarse esta mayoría, en segunda votación deberá aprobarse por mayoría absoluta, en cuyo caso deberá

[518] TRONCOSO REIGADA, A., «Las agencias…» *op. cit.,* p. 176. En palabras de del Profesor RUBÍ NAVARRETE este «*proceso de designación de los miembros de la Agencia pretende estar dirigido a reforzar la competencia profesional de los designados, promoviendo consensos sobre los mismos a través de mayorías reforzadas*», Cfr. RUBÍ NAVARRETE, J., «La Agencia…», 2019, *op. cit.,* p. 493.

[519] Por el Real Decreto 715/2015, de 24 de julio, por el que se nombra Directora de la Agencia Española de Protección de Datos a doña María del Mar España Martí, cuando aún no tenía vigencia ni el RGPD ni la LOPDGDD, de manera que la duración de su cargo era de cuatro años, sin embargo, parece que se ha renovado su nombramiento en 2019, sin que se haya publicado en su sede electrónica dicha circunstancia como parte de sus obligaciones de transparencia activa de acuerdo con lo establecido en los arts. 2.1.c), 5.4 y 6.1 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. De tal manera que, de acuerdo con la normativa vigente esta renovación ha sido por cinco años más.

[520] Lo son: a) el incumplimiento grave de sus obligaciones, b) incapacidad sobrevenida para el ejercicio de su función, c) incompatibilidad y, d) condena firme por delito doloso.

obtenerse un resultado favorable procedente de al menos dos grupos parlamentarios diferentes.

Es necesario hacer hincapié en el periodo de la duración de los cargos de la Presidencia y del Adjunto, ya que tanto el Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos en su art. 14, como la LO 15/1999, de 13 de diciembre en su art. 36, establecían que el mandato era de cuatro años, por lo que el nombramiento del Director (ahora Presidencia) solía coincidir con el inicio del mandato del Gobierno. La ampliación del mandato a un periodo de cinco años, sin duda aumentará su independencia y la neutralidad en el ejercicio de sus funciones y poderes[521].

A la Presidencia y al Adjunto de la AEPD les será aplicable la legislación de altos cargos de la Administración General del Estado[522], a la que habrá que acudir para conocer el régimen de incompatibilidades. La Ley 3/2015, de 30 de marzo, reguladora del ejercicio de alto cargo de la Administración General del Estado, establece en su art. 1.1 d) su aplicación a los titulares de las Agencias Estatales. Su Título II regula el «Régimen de conflictos de intereses y de incompatibilidades», así pues, el art. 13 establece que los altos cargos deberán ejercer sus funciones de manera exclusiva y que «*no podrán compatibilizar su actividad con el desempeño, por sí, o mediante sustitución o apoderamiento, de cualquier otro puesto, cargo, representación, profesión o actividad, sean de carácter público o privado, por cuenta propia o ajena. Tampoco podrán percibir cualquier otra remuneración con cargo a los presupuestos de las Administraciones públicas o entidades vinculadas o dependientes de ellas, ni cualquier otra percepción que, directa o indirectamente, provenga de una actividad privada simultánea*».

De manera posterior al cese o a la expiración del mandato del Presidente de la Agencia y del Adjunto, conforme a lo establecido en el art. 15 de la L 3/2015, de 30 de marzo, no podrán prestar servicios en entidades privadas en las que: a) hayan

[521] Además de acuerdo con RUBÍ NAVARRETE «*esta ampliación está justificada por la conveniencia de facilitar el diseño y cumplimiento del proyecto que se defina desde la Presidencia de la Agencia, para el que el de cuatro años la experiencia ha demostrado ser demasiado ajustado*», Cfr. RUBÍ NAVARRETE, J., «La Agencia…», 2020, *op. cit.,* p. 98.
[522] Cfr. Arts. 45.5 y 48.2 de la LOPDGDD.

resultado afectadas por decisiones en las que este haya participado, por ejemplo, inmersas en un procedimiento sancionador o en empresas beneficiarias de una licitación para la contratación de servicios u obras de la AEPD; b) que hayan estado sujetas bajo su supervisión en el cumplimiento de lo establecido en el RGPD, por ejemplo, en empresas de certificación. En un periodo de dos años posterior a su cese, deberá hacer llegar a la Oficina de conflictos de intereses una declaración con carácter previo a la iniciación de actividades en entidades privadas descritas en este párrafo, la cual deberá pronunciarse al respecto. Conforme al art. 16 de esta Ley, también deberá en un plazo de dos años posterior al cese del desempeño del cargo informar al Registro de Actividades de Altos Cargos el inicio de una nueva actividad económica.

Siguiendo con las garantías que afectan a su independencia, en el plano organizativo será la AEPD en ejercicio de las garantías formales atribuidas por la LO 3/2018 (art. 46.6) la encargada de elaborar y aprobar la relación de puestos de trabajo, respetando el límite de gasto establecido para ello. Su personal podrá ser tanto funcionarial como laboral. En el plano presupuestario, la AEPD será la encargada de elaborar y aprobar su presupuesto y remitirlo al Gobierno, para que sea integrado de manera independiente en el Presupuesto General del Estado. Finalmente, otra cuestión que garantiza su independencia es su capacidad normativa en cuanto a su auto-organización, pues la AEPD elabora la propuesta de su Estatuto y lo envía al Gobierno para que este lo apruebe mediante Real Decreto[523].

Antes de analizar las funciones y poderes de la AEPD, se debe mencionar que las facultades de representación ante el CEPD, le corresponden a la AEPD, y así lo establece el art. 44. 2: «*tendrá la condición de representante común de las autoridades de protección de datos del Reino de España en el Comité Europeo de Protección de Datos*», recayendo en la Presidencia de la AEPD esta representación conforme al art. 48.1 de la LOPDGDD[524]. Esta situación es reiterada también por lo establecido en el

[523] Art. 45.2 de la LOPDGDD.
[524] Contemplado también así por el art. 12 del estatuto de la AEPD.

art. 56.2, en lo relativo a las acciones exteriores de la AEPD, tal y como lo contemplan los arts. 51.3 y 68.4 del RGPD.

En cuanto a las funciones y poderes con las que cuenta la AEPD, son las establecidas por los arts. 57 y 58 del RGPD[525]. Sin duda, la principal función es la de supervisar la aplicación del contenido en el RGPD y de la LOPDGDD[526]. La LO también le reconoce a la AEPD poderes de investigación, correctivos, de autorización y consultivos. En cuanto a la potestad de investigación, la LOPDGDD, complementando lo establecido por el RGPD, establece que esta agencia ajustará su actuación al Título VIII a través de los planes de auditoría preventiva. Ahora bien, el Título VIII desarrolla el procedimiento a seguir en caso de una posible vulneración de la normativa de protección de datos, cuando en la investigación se realizan actuaciones previas al inicio del procedimiento para el ejercicio de la potestad sancionadora[527]. Estas investigaciones serán llevadas a cabo por los funcionarios de la AEPD o por funcionarios ajenos a ella, pero habilitados por la misma, pensemos, por ejemplo, cuando se realicen en territorio español operaciones conjuntas de investigación con otras agencias por un tratamiento trasfronterizo[528]. Otras autoridades tendrán el deber de colaborar con la AEPD por mandato legal cuando esta última ejerza sus potestades de investigación, como otras Administraciones públicas, incluso las tributarias y las de la Seguridad Social. También los particulares deberán colaborar con la AEPD, proporcionando los documentos que esta les solicite como informes, antecedentes y justificantes. En el caso de que estos documentos contengan datos personales, el tratamiento de datos se considerará lícito por cumplir con una obligación legal y en cumplimiento de sus competencias conforme con lo establecido en el art. 6.1 c) y e) del RGPD[529].

[525] Es importante señalar que las guías, los informes y las notas técnicas que emite la AEPD, están amparadas por el art. 57.1.b) como parte de las acciones encaminadas a la sensibilización del público y la «*comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento*». La propia AEPD ha determinado que estos tienen carácter divulgativo, cfr. https://www.aepd.es/es/areas-de-actuacion/innovacion-y-tecnologia (consulta: 10 de enero de 2021).
[526] Art. 47 de la LOPDGDD.
[527] *Vid.* arts. 67 y 68 de la LOPDGDD.
[528] Art. 51 de la LOPDGDD.
[529] Art. 52.1 de la LOPDGDD.

Cuando la AEPD lleve a cabo una investigación previa para el ejercicio de la potestad sancionadora, a efectos de identificación podrá solicitar informaciones a otras autoridades, como las tributarias y las de la seguridad social, para identificar inequívocamente el posible infractor. En caso de que la información obtenida de las autoridades antes descritas no sirviese para cumplir el cometido de identificar inequívocamente al posible infractor, la AEPD, podrá solicitarles a los operadores de servicios de comunicaciones electrónicas y a los prestadores de servicios de la sociedad de la información, los datos que obren en su poder y que sirvan para cumplir con la finalidad perseguida. La Agencia requerirá estos datos a los operadores de comunicaciones electrónicas y a los prestadores de servicios de la sociedad de la información de manera motivada para que le sean transmitidos, con excepción de los datos de tráfico, en cuyo caso se necesitará la autorización judicial para la misma. Esta petición motivada de cesión solamente procederá si las actuaciones de investigación son iniciadas con motivo de una denuncia por el afectado/interesado o siempre que el infractor utilice «*sistemas que permitan la divulgación sin restricciones de datos personales*» [530]. También se requerirá autorización judicial en el caso de que la AEPD pretenda llevar a cabo labores de investigación que requiera el acceso de su personal al domicilio del inspeccionado, o en su defecto, el consentimiento de este último para llevar a cabo esa labor investigadora [531]. La AEPD con motivo de sus poderes de investigación también podrá llevar a cabo auditorías preventivas para vigilar el cumplimiento de la

[530] Art. 52 de la LOPDGDD.

[531] De acuerdo con lo establecido en el art.53.2 de la LOPDGDD. Antes se hizo referencia a la inviolabilidad del domicilio en relación con el poder de investigación que tienen las autoridades de control, específicamente con la obtención del acceso a los locales del responsable conforme al derecho procesal tanto de la Unión como de los Estados miembros (art. 58.1.f) del RGPD). Ahora bien, dentro del territorio español los jueces competentes para conocer de este tipo de autorizaciones serán los Juzgados de lo Contencioso-administrativo de la circunscripción territorial donde se encuentre el inmueble donde realice su actividad el responsable del tratamiento, de acuerdo con los establecido en el art. 8.6 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, que a tenor literal establece que: «*Conocerán también los Juzgados de lo Contencioso-administrativo de las autorizaciones para la entrada en domicilios y restantes lugares cuyo acceso requiera el consentimiento de su titular, siempre que ello proceda para la ejecución forzosa de actos de la administración pública, salvo que se trate de la ejecución de medidas de protección de menores acordadas por la Entidad Pública competente en la materia*». Como sería el caso de una inspección en materia de defensa de la competencia llevada a cabo por la Comisión Nacional de Mercados y la Competencia haya requerido al titular del inmueble el consentimiento para llevar a cabo una inspección en sus instalaciones y este se haya opuesto a la práctica de esta diligencia o exista un riesgo inminente de su oposición, tal y como se regula también por el art. 27.4 de la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y la Competencia.

normativa comunitaria de protección de datos y nacional, dirigidas al tratamiento de datos en sectores concretos[532] .

La AEPD tiene también atribuida la potestad de «regulación», es decir, que esta podrá aprobar criterios de actuación en forma de «Circulares» [533] . Anteriormente, el TC reconoció esta potestad a la AEPD señalando que debía ceñirse «*en lo esencial a dictar las instrucciones precisas para adecuar los tratamientos automatizados a los principios*»[534]. La elaboración de este tipo de documentos estará sujeto al procedimiento establecido en el Estatuto de la Agencia (EAEPD), que como mencionamos con anterioridad, de acuerdo con la Disposición transitoria primera continuará vigente en lo que no se oponga a lo dispuesto en la LO 3/2018, en relación con el procedimiento de reclamaciones o sancionador. En el art. 5 incisos c) y d) del EAEPD, no indica un procedimiento, sino más bien una competencia para la elaboración de instrucciones y recomendaciones para la adecuación del tratamiento automatizado de datos a los principios y, para la aplicación a las disposiciones legales en materia de seguridad de datos. Por lo que la agencia deberá autorregular este aspecto e incluir el procedimiento de elaboración de circulares en su Estatuto.

Los procedimientos llevados a cabo ante a la AEPD por tratamientos que vulneren la normativa de protección de datos serán de dos tipos: como consecuencia del ejercicio de derechos de los ciudadanos contemplados en la normativa en la materia, o bien para que la AEPD determine la existencia de una infracción En el primero de los casos, los interesados podrán interponer una reclamación por no haber sido atendida una solicitud del ejercicio de los derechos contenidos en los arts. 15 al 22 del RGPD. El plazo para resolver es de seis meses contados desde el acuerdo de admisión, y ante la falta de resolución expresa se entenderá resuelta en sentido positivo[535]. El segundo de los procedimientos podrá iniciarse, por acuerdo de la AEPD, o como consecuencia un procedimiento de ejercicio de derechos. También podrá iniciarse por medio de una solicitud de otra autoridad de control, en el caso

[532] Art. 54 de la LOPDGDD.
[533] De acuerdo con lo establecido en el art. 55 de la LOPDGDD.
[534] F.J. 8 *in fine* de la STC (Pleno) 290/2000, de 30 de noviembre (RTC\2000\290; ECLI:ES:TC:2000:290). En este mismo sentido también el F.D. 6 de la STS de 16 de febrero de 2007 (RJ 2007\739: ECLI:ES:TS: 2007:954).
[535] Cfr. Arts. 63.1, 64.1 y 65 de la LOPDGDD.

de que la AEPD sea la autoridad principal en tratamientos transfronterizos, tendrá como finalidad llevar a cabo una investigación para comprobar una posible infracción, bien contenida en el RGPD o en esta LO; la duración máxima del procedimiento será de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, desde el proyecto de acuerdo de inicio. Si no se resuelve en ese plazo producirá caducidad y se archivarán las actuaciones[536].

En algunos casos, como consecuencia de las investigaciones realizadas por la AEPD, la Presidencia podrá dictar un acuerdo por el que inicie el ejercicio de la potestad sancionadora, que deberá contener los hechos, la identificación de la persona o entidad contra la cual se dirija, la infracción y su posible sanción[537]. También podrá dictar medidas provisionales que estime oportunas y proporcionadas durante la fase previa de investigación, con fin de garantizar el derecho a la protección de datos[538].

La LOPDGDD traslada el régimen sancionador establecido en el art. 83 del RGPD a la normativa española, especificando los supuestos contemplados de manera genérica en el RGPD. Los sujetos intervinientes en el tratamiento de datos personales que podrán ser responsables de la comisión de una infracción y, por tanto, susceptibles de ser sancionados son: a) los responsables del tratamiento, b) los encargados del tratamiento, c) los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la UE, d) las entidades de certificación y, e) las entidades de supervisión acreditadas[539]. El art 83.2 incluye dentro de los factores agravantes o atenuantes aplicables a una situación concreta: «*a) El carácter continuado de la infracción, b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales, c) Los beneficios obtenidos como consecuencia de la comisión de la infracción, d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la*

536 Cfr. Arts. 63.1, 64.2 y 66 de la LOPDGDD.
537 Art. 68.1 de la LOPDGDD.
538 Art. 69.1 de la LOPDGDD. Se podrán dictar también incluso antes del inicio del procedimiento sancionador en procedimientos iniciados con motivo de una reclamación, en este caso, se le deberá dar audiencia al responsable del tratamiento, pero en todo caso deberá determinarse mediante resolución motivada la obligación de atender el derecho solicitado, conforme a lo establecido en el art. 69.3 de la LOPDGDD.
539 Art. 70 de la LOPDGDD.

infracción, e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente, f) La afectación a los derechos de los menores, g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos y, h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado»[540].

Además, realiza una escala de graduación de las infracciones, clasificándolas en: muy graves, graves y leves. Son consideradas como muy graves las contenidas en los apartados 5 y 6 del RGPD, y descritas con mayor detalle en el art. 72 de la LOPDGDD; este tipo de infracciones prescriben a los tres años. Las infracciones consideradas como graves son aquellas descritas en el apartado 4 del art. 83, detalladas por el art. 73 de la LOPDGDD; y prescribirán en dos años. Las infracciones graves y muy graves se cometen por la vulneración sustancial de lo descrito en los apartados 4, 5 y 6 del art. 83, en cambio la LOPDGDD las considera como leves pues infringen formalismos relacionadas con las establecidas en los apartados 4 y 5 del art. 83, y contenidas en el art. 74 de la LOPDGDD; este tipo de infracciones prescriben al año. Interrumpe en todo caso el plazo de prescripción la iniciación del procedimiento sancionador siempre que tenga conocimiento el interesado. También interrumpirá el plazo de prescripción el conocimiento del proyecto de decisión por el interesado, siempre que la AEPD actúe como autoridad principal cuando se realice un tratamiento trasfronterizo, y sea conforme con el procedimiento de cooperación y coherencia del RGPD[541]. En todo caso, cuando la infracción sea superior a un millón de euros, y la AEPD haya actuado como autoridad de control y, el infractor sea una persona jurídica, se publicarán en el BOE los datos identificativos del responsable, la infracción y la sanción impuesta[542].

El art. 77 de la LOPDGDD, en relación con el contenido de los arts. 83.7 y 84 del RGPD, establece el régimen aplicable a «*determinadas categorías de responsables o encargados*», cuando actúen como tales, a las Administraciones públicas

[540] Art. 76.2 de la LOPDGDD.
[541] Art. 75 de la LOPDGDD.
[542] Art. 76.4 de la LOPDGDD.

territoriales, al sector público institucional, órganos constitucionales, instituciones de las comunidades autónomas, órganos jurisdiccionales, autoridades administrativas independientes, universidades, corporaciones de derecho público, y demás descritas en el apartado 1 del art. 77, no estando en estos casos sujetas a una sanción de tipo pecuniario por la realización de alguna de las infracciones contenidas en el RGPD y en la LO. En este caso la autoridad de control competente emitirá una resolución sancionando las conductas con apercibimiento, y establecerá las medidas para hacer cesar la conducta infractora o en su caso para que se corrijan los efectos de la infracción[543]. Lo anterior deberá ser notificado al responsable o encargado del tratamiento, a su superior jerárquico y si los hubiere a los afectados si tuviesen carácter de interesados.

Además del apercibimiento y las medidas a adoptar, se podrá proponer por la autoridad de control competente la iniciación de un procedimiento disciplinario si existiesen indicios para ello[544]. En el caso que se trate de personal laboral o funcionarial, se seguirá con lo establecido en el Título VII del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público. Si se tratase de algún alto cargo se aplicará lo dispuesto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

1.5.2 Las Autoridades de control autonómicas

La LORTAD ya preveía en su art. 40.1 la creación de Agencias autonómicas de protección de datos personales, encargadas de supervisar la aplicación de dicha LO, cuando los ficheros de datos personales fueran creados y gestionados por las Comunidades Autónomas. El mismo apartado de este artículo determinaba que estas tenían las mismas funciones que la agencia estatal, las cuales estaban contempladas en el art. 36, con excepción de la remisión de su memoria al Ministerio de Justicia, velar por la publicidad de la existencia de ficheros y en asuntos

[543] Art. 77.2 de la LOPDGDD.
[544] Art. 77.3 de la LOPDGDD.

relacionados con movimientos internacionales de datos [545]. La LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por la que se deroga la LO 5/1992, también preveía la creación de Agencias autonómicas de protección de datos encargadas de supervisar la correcta aplicación de esta, cuya competencia estaba también delimitada a los ficheros creados y gestionados por las CCAA.

Antes de abordar lo que establece la nueva LOPDGDD, en relación con el contenido del RGPD, consideramos necesario realizar un recorrido esquemático de las Agencias de protección de datos autonómicas, desde su creación hasta el día de hoy.

La primera Agencia autonómica de protección de datos fue la de la Comunidad Autónoma de Madrid, creada por la Ley 13/1995, de 21 de abril, de regulación del uso de la informática de datos personales por la Comunidad de Madrid, como ente de derecho público de los previstos en el art. 6 de la Ley 9/1990, de 8 de noviembre, reguladora de la Hacienda de la Comunidad de Madrid [546]. Que finalmente, en el año 2012 se extingue por mandato de los arts. 61 y ss. de la Ley 8/2012, de 28 de diciembre, de Medidas Fiscales y Administrativas, revirtiendo sus competencias y funciones al ámbito estatal, atribuyéndolas así a la AEPD.

La segunda autoridad de control autonómica puesta en marcha fue la catalana, se creó por la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos, de acuerdo con esta ley su ámbito competencial estaba limitado a los tratamientos de datos llevados a cabo en Cataluña y específicamente a los realizados por el sector público de esa Comunidad Autónoma, a los tratamientos llevados a cabo por parte de la administración territorial local en su territorio, y por el sector público institucional, incluidas las Universidades. Su competencia también

[545] Es decir, velar por la publicidad de la existencia de ficheros por medio de una publicación periódica de todos los existentes, el ejercicio de del control y autorizaciones por movimientos internacionales de datos (incisos j), k), l), f) y g) del art. 36), así como en las transferencias internacionales de datos requerir a los responsable y encargados de adecuarse a la normativa bajo la pena de cesar su tratamiento o cancelar sus ficheros e informar de carácter perceptivo en este tipo de transferencias a los responsables y encargados los proyectos de disposiciones generales por los que desarrollen esa LO (arts. 45 y 48).

[546] Posteriormente esta norma queda derogada por la Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal en la Comunidad de Madrid, por la que se crea igualmente una agencia autonómica en materia de protección de datos en esta Comunidad Autónoma. Con esta ley se pretendía actualizar el marco jurídico y adaptarlo al contenido de la Directiva 95/46/CE y de la entonces vigente LO 15/1999, de 13 de diciembre.

se extendía a los entes públicos o privados que gestionaran los ficheros del sector público catalán y sus entidades locales en la prestación de servicios públicos cuando fuesen llevados a cabo por cuenta de una administración de la Generalitat[547]. Se le asignaban competencias de «*registro, control, inspección, sanción y resolución, así como la adopción de propuestas e instrucciones*»[548]. Con la reforma del Estatuto de Autonomía del año 2006 por Ley Orgánica 6/2006, de 19 de julio, se incorpora como competencia ejecutiva de la Generalitat la protección de datos personales, en relación con distintas autoridades públicas de su competencia[549]. En esta misma ley se prevé la creación de una autoridad independiente en la materia[550]. La cual se crea de manera posterior por la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, otorgándole independencia sustancial y formal, reconociéndole competencia de control, inspección, sanción y resolución, así como de aprobación de propuestas, recomendaciones e instrucciones[551]. Su ámbito de actuación se limita a tratamientos y ficheros del sector público catalán, los realizados por las Universidades públicas y privadas, también por entidades de derecho privado siempre que, su capital pertenezca a entes públicos, o sus órganos directivos hayan sido designados por mayoría por entes públicos, o que sus ingresos provengan del sector público; también se incluyen entidades de derecho privado que realicen la gestión directa o indirecta de servicios, personas físicas y jurídicas que cumplan funciones públicas que sean competencia de la Generalitat y corporaciones de derecho público que actúen en exclusiva en el ámbito territorial de la CA[552].

En el año 2004 la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos, por medio de la cual se prevé la regulación de los ficheros cuyos titulares sean la Comunidad Autónoma, los órganos forales de los territorios históricos, las administraciones locales de la CA, el Parlamento Vasco, el Tribunal Vasco de Cuentas Públicas, el Ararteko, el Consejo de Relaciones Laborales, el

[547] Art. 3 de la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos.
[548] Art. 4.1 de la Ley 5/2002, de 19 de abril, de la Agencia Catalana de Protección de Datos.
[549] De acuerdo con el art. 156 de la LO 6/2006, de 19 de julio.
[550] Inciso d) del art. 156 en relación con el art. 31 de la LO 6/2006, de 19 de julio.
[551] Art. 4 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.
[552] Art. 3 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos.

Consejo Económico y Social, el Consejo Superior de Cooperativas, la Agencia Vasca de Protección de Datos, la Comisión Arbitral, las corporaciones de derecho público, representativas de intereses económicos y profesionales, de la Comunidad Autónoma del País Vasco y, cualesquiera otros organismos o instituciones, con o sin personalidad jurídica, creados por Ley del Parlamento Vasco, salvo que esta disponga lo contrario[553]. Mediante esta ley, como su propio título indica, también se crea la Agencia Vasca de Protección de Datos, a la cual también se le atribuyen garantías formales y sustanciales para asegurar su independencia[554]. Sin embargo, como observamos la Agencia Vasca de Protección de Datos, no es creada por mandato estatutario sino de manera legal.

En el caso de Navarra, se prevé la cooperación con otras Administraciones para la tramitación y resolución de procedimientos cuya competencia sea de la Autoridad requirente, sin embargo, el art. 96 de la Ley Foral 11/2019, de 11 de marzo, de la Administración de la Comunidad Foral de Navarra y del Sector Público Institucional Foral, no determina a qué Administraciones públicas se refiere, entendiéndose en ese caso a la totalidad de las Administraciones públicas que tengan esas competencias conferidas en un sentido amplio. Existen otras Comunidades Autónomas que, hasta finales del 2018, no habían regulado legal ni estatutariamente lo relativo a la competencia descrita en el art. 37 de la LO 15/1999, como el caso de Asturias, Galicia, Cantabria, Castilla-la Mancha, Extremadura, La Rioja, Murcia y Valencia. De hecho, a fecha del nuevo marco jurídico no han considerado necesaria la existencia de una autoridad en su respectivo ámbito competencial. Ahora bien, hay CCAA que tienen asumidas competencias de desarrollo legislativo y ejecución de la legislación estatal en la materia como: Aragón[555], Baleares[556] y Castilla y León[557]. En los Estatutos de Autonomía de las CCAA de Aragón y Castilla y León también se prevé la posibilidad de crear su

[553] Art. 1.1 y art. 2.1 de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.
[554] *Vid.* art. 10 y ss. de la Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.
[555] Art. 75. 5ª de la LO 5/2007, de 20 de abril, de reforma del Estatuto de Autonomía de Aragón.
[556] Art. 31.14 de la LO 1/2007, de 28 de febrero, de reforma del Estatuto de Autonomía de las Illes Balears.
[557] Arts. 12. d) y 71.1.2º de la LO 14/2007, de 30 de noviembre, de reforma del Estatuto de Autonomía de Castilla y León.

correspondiente autoridad autonómica de control, sin embargo, no se ha materializado. En el caso de Canarias no se fija un título competencial específico en materia de protección de datos y, por tanto, tampoco prevé la creación de su propia autoridad autonómica[558].

Hemos dejado para el final el caso de Andalucía, CA que prevé estatutariamente su competencia ejecutiva en los arts. 32 y 82 de su Estatuto de Autonomía. En este mismo instrumento jurídico no se dispone que deba crearse una autoridad de control. Sin embargo, el artículo 43 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía, crea el Consejo de Transparencia y Protección de Datos de Andalucía, atribuyéndole garantías formales que procuran asegurar su independencia, en cuanto al personal y presupuesto. Sin embargo, es parte de la Administración institucional autonómica, ya que la ley referida anteriormente remite al contenido de la DA 2ª de la Ley 9/2007, de 22 de octubre, por la que se consideran dentro de la administración institucional aquellos entes a los cuales se les reconozca independencia funcional.

Sin embargo, posteriormente, como bien lo evidencia el Profesor NEIRA BARRAL ocurre que: «*la asunción efectiva por parte de este Consejo de la competencia en materia de protección de datos ha quedado diferida en virtud de lo establecido en la Disposición Transitoria tercera del Decreto 434/2015, de 29 de septiembre, por el que se aprueban los estatutos del Consejo de Transparencia y Protección de Datos de Andalucía y hasta que las instituciones autonómicas no aprobasen y ejecutasen las disposiciones legales o reglamentarias a las que hace referencia la citada Disposición Transitoria tercera, la Agencia Española de Protección de Datos continuaría siendo la única autoridad de control en materia de protección de datos en el ámbito territorial de la Comunidad Autónoma de Andalucía. Pues bien, en el BOJA de 17 de septiembre de 2018, se ha publicado el Acuerdo de 11 de septiembre de 2018, del Consejo de Gobierno, por el que se determina la asunción de las funciones en materia de protección de datos por el Consejo de la Transparencia y Protección de Datos de Andalucía y en la disposición final primera de este Acuerdo, faculta a la persona titular de la Consejería competente en materia de transparencia para dictar las disposiciones*

[558] Art. 113 de la LO 1/2018, de 5 de noviembre, de reforma del Estatuto de Autonomía de Canarias.

y realizar cuantas actuaciones sean necesarias en desarrollo y ejecución de lo dispuesto en el presente Acuerdo y, en particular, para dictar la Orden que establezca el inicio del ejercicio las funciones en materia de protección de datos de carácter personal »[559]. Esta previsión va en contra a lo establecido en el propio RGPD, pues impide el deber objetivo de supervisión en el cumplimiento de la normativa en materia de protección de datos[560].

En todo caso, es evidente que las agencias o autoridades autonómicas establecidas hasta el momento, y con las cualidades requeridas en el RGPD, solo serán competentes a grandes rasgos cuando el tratamiento sea llevado a cabo por el sector público de su Comunidad Autónoma, pues como bien menciona el Profesor TRONCOSO REIGADA: «*En el caso de la Agencia Española estas facultades de control no se extienden únicamente a los ficheros privados o a los ficheros de los que es titular la Administración General del Estado sino también a los de la Administración Autonómica cuando ésta no haya configurado todavía una Autoridad Autonómica de control»*[561].

Ahora bien, la nueva LOPDGDD prevé tres secciones del Capítulo II Título VII dedicadas a la regulación de las autoridades autonómicas de protección de datos. En su art. 57 establece un marco competencial en el que estas puedan ejercer los poderes y funciones atribuidas a todas las autoridades de control según el RGPD. Serán competentes en tres supuestos: en primer lugar, cuando el responsable del tratamiento sea un ente u organismo del sector público autonómico o entidades locales situadas en su territorio o aquellos entes que presten servicios mediante cualquier forma de gestión sea directa o indirecta. En segundo lugar, cuando el tratamiento de datos personales sea realizado por personas físicas o jurídicas que

559 NEIRA BARRAL, D., *op. cit.,* pp.695-696.
560 En relación con el establecimiento de autoridades autonómicas de control VALÍN LÓPEZ determina que: «*Parece claro, pues, que el legislador autonómico tiene en su ámbito competencial libertad de decidir si crea o no una autoridad de control, pero una vez creada, no es libre del elenco de funciones y poderes de esta, pues el RGPD es de aplicación directa y no permite reducción alguna del tal sentido, antes al contrario, lo que sí les permite a los Estados es la ampliación de los poderes que el Reglamento expresamente relaciona*», Cfr. VALÍN LÓPEZ, M., «Las autoridades autonómicas de protección de datos», RALLO LOMBARTE, A. (Dir.), *Tratado de protección de datos. actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, Tirant lo blanch, Valencia, 2019, p.524.
561 TRONCOSO REIGADA, A., «Las agencias…» *op. cit.,* p. 123.

lleven a cabo funciones públicas competencia de la Administración autonómica o local en esa Comunidad Autónoma. Finalmente, serán competentes para tratar datos personales si están previstos de manera expresa en alguna norma, o en su Estatuto de Autonomía[562]. Este último supuesto le es aplicable a las CCAA de Andalucía, Aragón, Baleares, Canarias, Castilla y León y Cataluña, que prevén en sus respectivos EEAA. este tipo de competencias.

Las autoridades autonómicas de protección de datos también tienen potestad de regulación, es decir, podrán emitir circulares siguiendo el procedimiento establecido en sus correspondientes Estatutos y publicarlas en su correspondiente Boletín Oficial[563]. Las autoridades autonómicas de control cooperarán con la autoridad de control a nivel estatal por lo que constituye un deber para estas intercambiar información y cumplir con sus respectivas funciones. Celebrarán reuniones de manera semestral y serán llamadas por la AEPD o por petición de alguna de las autoridades autonómicas para la aplicación coherente del RGPD[564].

Si la AEPD considerase que se está efectuando un tratamiento contrario a lo establecido por el RGPD dentro del marco competencial de una autoridad autonómica de control, le requerirá a esta última para que en el plazo de un mes adopte las medidas necesarias para el cese de este tratamiento. En el caso de que la autoridad autonómica no atendiese a tal requerimiento, la AEPD podrá ejercer acciones que estime pertinentes ante la jurisdicción contencioso-administrativa[565]. Con motivo de este tema hay que recordar dos cosas, por una parte, lo establecido en el art. 58.2 b) del RGPD, por el cual se faculta a las autoridades de control para sancionar a todo responsable con apercibimiento cuando las operaciones hayan infringido el contenido del RGPD, y que antes de acudir a la jurisdicción administrativa la Agencia podrá en su caso instar el procedimiento de carácter disciplinario previsto para el personal laboral o funcionarial, en el Título VII del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto

[562] Art. 57.1 de la LOPDGDD.
[563] Art. 57.2 de la LOPDGDD.
[564] *Vid.* art. 58 de la LOPDGDD.
[565] Art. 59 de la LOPDGDD.

refundido de la Ley del Estatuto Básico del Empleado Público. En caso de que el requerimiento esté dirigido a un alto cargo autonómico, por ejemplo, al Director de la Agencia Vasca de Protección de Datos o al Director de la Autoridad Catalana de Protección de datos en aplicación de lo establecido en el art. 25.2 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, y el requerimiento no sea atendido podrá ajustarse a la infracción en materia disciplinaria del art. 29.1 f) de la L 19/2013, por «*El notorio incumplimiento de las funciones esenciales inherentes al puesto de trabajo o funciones encomendadas*», y ser sancionado por la misma conforme al art. 30.3 de esa misma ley.

Finalmente, se establece un marco de actuación de las autoridades de control autonómicas si estas son consideradas como autoridades principales y se vean involucradas: a) en tratamientos transfronterizos dentro de la UE o, b) si la autoridad autonómica de control le requiere la emisión de un dictamen al CEPD, para dirimir un conflicto, o si le remite un proyecto de decisión o si le solicita el examen de un asunto en particular. En estos casos, la AEPD debe actuar como representante común ante el CEPD, pero deberá ser asistida por un representante de la correspondiente autoridad de control autonómica [566] . Lo relatado anteriormente en relación con el nuevo panorama en la materia evidencia que se ha robustecido el sistema de cooperación entre las autoridades de control, permitiendo que el ciudadano pueda presentar reclamaciones en el territorio de su residencia, reduciendo así las cargas que hasta ahora esta acción traía aparejadas. en relación.

[566] Arts. 60, 61 y 62 de la LOPDGDD.

CAPÍTULO IV

LA ADMINISTRACIÓN PÚBLICA COMO RESPONSABLE DEL TRATAMIENTO DE DATOS PERSONALES.

1. EL TRATAMIENTO DE DATOS PERSONALES LLEVADO A CABO POR LAS ADMINISTRACIONES PÚBLICAS. DELIMITACIÓN DEL CONTENIDO.

El contenido de este apartado se realiza a partir de lo establecido en el RGPD y de la LOPDGDD relacionando con la normativa sectorial, la doctrina y la jurisprudencia en la materia. Antes de comenzar con este apartado, es necesario delimitar el contenido de este Capítulo. Quedan al margen de este, el estudio de los tratamientos de datos llevado a cabo por las instituciones, órganos y organismos de la Unión Europea cuando actúen en calidad de responsables del tratamiento de datos personales. A estas instituciones se les aplica de manera específica el Reglamento 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se deroga el Reglamento 45/2001 y la Decisión 1247/2002/CE.

También quedan al margen de este estudio los tratamientos de datos personales cuyas finalidades específicas sean: la prevención, la investigación, la detección, el enjuiciamiento de ilícitos de naturaleza penal y su ejecución, así como la circulación de estos tipos de datos dentro de la Unión. Si bien es cierto que en este tipo de tratamientos intervienen autoridades públicas, tienen un régimen específico distinto al contenido del RGPD. A este tipo de tratamientos se les aplica el contenido de 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 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. Hasta en tanto no

se apruebe una ley que transponga su contenido a nuestro sistema jurídico, este tipo de tratamientos seguirán estando genéricamente sujetos al contenido de la Ley Orgánica 15/1999, de 13 de diciembre y, específicamente a su art. 22[567] dentro del territorio español[568]. Lo anterior se realiza con la finalidad de usar el mismo marco legal como parámetro aplicable a los tratamientos de datos realizados por la Administración pública en su sentido más amplio. Lo cual también deja fuera de este estudio también a los tratamientos de datos realizados por los órganos jurisdiccionales[569].

Como no podría ser de otra manera, el RGPD considera como responsables del tratamiento a las autoridades públicas, servicios u otros organismos si el Derecho de los Estados miembros determina los fines y los medios del tratamiento, conforme a lo establecido en su art. 4.7. En relación con lo anterior es menester señalar que a lo largo del contenido del RGPD no se determina qué debe entenderse como «autoridad u organismo público». Según el GT29 esa noción «*debe determinarse con arreglo a la legislación nacional. Por tanto, las autoridades y organismos públicos incluyen a las autoridades nacionales, regionales y locales, pero el concepto con arreglo a las leyes nacionales aplicables suele incluir un intervalo de otros organismos regidos por el derecho público*»[570]. Puede afirmarse entonces que entidades y organismos de nuestras Administraciones públicas están sometidas al

[567] De acuerdo con la D.T. 4ª de la LOPDGDD.

[568] En este sentido como bien apunta el Profesor BALLESTEROS MOFFA «*como reconoce el propio art. 22.1 de la LOPD 1999, no todos los tratamientos por las Fuerzas y Cuerpos de Seguridad persiguen fines policiales stricto sensu, debiéndose diferenciar en puridad entre ficheros policiales, entre los que los que tendrían por objeto este tratamiento especial, y no policiales, cuya responsabilidad por las Fuerzas y Cuerpos de Seguridad no es suficiente singularidad por su finalidad administrativa. Mientras los primeros, en la medida en que respondan a la represión penal, entran dentro del ámbito de aplicación de la Directiva de policía, aplicándose transitoriamente el art. 22 LOPD 1999, los segundos siguen rigiéndose por el régimen general de privacidad del RGPD y LOPDGDD*», cfr. BALLESTEROS MOFFA, L. Á., *Las fronteras de la privacidad. El conflicto entre seguridad pública y datos personales en una sociedad amenazada y tecnológica,* Comares, Granada, 2020, p. 136.

[569] Aunque se le aplica el nuevo marco normativo dado por el RGPD y por la LOPDGDD, además a los miembros integrantes de poder judicial se les aplica lo establecido en la LO 6/1985, de 1 de julio, del Poder Judicial (art. 230). En este marco, la vigilancia del correcto cumplimiento de la normativa en la materia por los Jueces y Tribunales en el desarrollo de sus funciones es llevada a cabo por el Consejo General del Poder Judicial, de acuerdo con el contenido del art. 560. 10ª y 19ª de la LO 6/1985. Cuestión que ha sido también refrendada por el F.D. 3 de la STS de 2 de diciembre de 2011: RJ\2012\2585; ECLI:ES:TS: 2011:8497).

[570] GT29, Directrices sobre delegados de protección de datos (DPD), de 13 de diciembre de 2016, p. 7.

contenido y principios del RGPD[571], es decir, que la aplicación de la normativa también es obligatoria al sector público institucional en términos del art. 2.2 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, esto es aquellos entes y organismos vinculados o dependientes de las Administraciones públicas territoriales, al igual que a las entidades de derecho privado vinculadas o dependientes de las Administraciones públicas cuando ejerzan potestades administrativas y a las Universidades públicas.

1.1 La base jurídica de su licitud.

No debemos olvidar que la Administración pública persigue intereses generales. En este sentido, el tratamiento de datos debe entonces basarse en una causa de licitud que sea compatible con las finalidades y principios a los que está sometida la Administración. Recientemente el TJUE ha determinado que «*todo tratamiento de datos de carácter personal debe, por una parte, respetar los principios enunciados en el artículo 5 de dicho Reglamento y, por otra, cumplir las condiciones de licitud enumeradas en el artículo 6 del mismo*»[572], es por eso que aunque los tratamientos de datos que realiza la Administración resulten lícitos ya que devienen del cumplimiento de una norma jurídica o algún interés general, este nuevo marco jurídico obliga al responsable a determinar de manera específica cuál es la razón que motiva el tratamiento de los datos personales; obligación que a su vez está vinculada a otras a su cargo y con el ejercicio de los derechos de los ciudadanos contemplados en el RGPD y en la LOPDGDD. En relación con lo anterior el considerando 45 del RGPD determina que una sola norma puede servir como base de licitud para varias operaciones de tratamiento de datos.

La razón por la cual los tratamientos de datos realizados por la Administración no pueden basarse genéricamente en el consentimiento de los interesados resulta obvia: el ciudadano interesado está en una situación de desigualdad frente a la administración responsable del tratamiento, pues esta

[571] Sin perjuicio de seguir cumpliendo con los principios constitucionales que rigen su actuación: eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Ley y al derecho. Principios que son aplicables tanto a Administraciones públicas territoriales como a entes del sector público institucional, de acuerdo con el F.J.8 de la STC 85/1983 de 25 octubre (RTC\1983\85; ECLI:ES:TC:1983:85).

[572] Cfr. Apdo. 208 de la STJUE de 6 de octubre de 2020 (ECLI:EU:C: 2020:791).

última cuenta con prerrogativas y potestades para hacer cumplir sus fines en aras de los intereses generales, tal y como establece el art. 103.1 de la CE. En vista de este manifiesto desequilibrio y de la posición de sujeción en la que se sitúan los ciudadanos es imposible basar ese tratamiento de datos personales en el consentimiento, ya que este no sería otorgado por el ciudadano de manera libre, esta circunstancia incluso se prevé así en el considerando 43 del propio RGPD. Para que el tratamiento de datos llevado a cabo por la Administración sea considerado lícito sin estar basado en el consentimiento, se debe fundar en al menos una de las bases de licitud de tratamiento previstas en el art. 6 del RGPD.

Las bases de licitud del tratamiento como ya se ha señalado están contempladas en el apartado primero del artículo 6 del RGPD. De manera general, son tres los motivos en los que la Administración pública basa el tratamiento de datos: el primero de ellos en la necesidad del cumplimiento de un deber legal, el segundo se basa en el cumplimiento de una misión realizada en interés público, y el tercero se realiza como consecuencia del ejercicio de los poderes públicos que tiene conferidos.

Como observamos son tres supuestos perfectamente diferenciados. En el primero, el tratamiento de datos personales debe estar contemplado como una obligación legal para la Administración, conforme con el contenido del inciso c) del art. 6.1 del RGPD. Parecería que esta sería la base de licitud principal de la Administración pública, ya que como mencionamos anteriormente conforme al art. 103.1 de la CE, esta última está sometida plenamente al cumplimiento de la ley. Sin embargo, esta norma podrá contener las condiciones generales y especiales del tratamiento de datos. Como bien apunta el Profesor FERNÁNDEZ RODRÍGUEZ se entiende en este caso que «*la ley aborda de manera directa el tratamiento de datos por parte de una determinada entidad*»[573]. La ley que prevea de manera específica el tratamiento por una Administración deberá determinar la o las finalidades del tratamiento, el tipo de datos que se van a tratar, si se van a realizar o no

[573] FERNÁNDEZ RODRÍGUEZ, J. J., «Aproximación general a la reforma normativa: El Reglamento Europeo y la Ley Orgánica española. Principios generales», CAMPOS ACUÑA Mª C., *Aplicación práctica y adaptación de la protección de datos en el ámbito local. Novedades tras el RGPD y la LOPDGDD.* 2ª ed., Madrid, 2019, p. 56.

comunicaciones de datos y los plazos de conservación. También se podrán imponer en la misma, condiciones especiales del tratamiento «*tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679*»[574]. Así como todas aquellas medidas que el legislador nacional estime pertinentes para asegurar que el tratamiento sea llevado a cabo con licitud y equidad[575].

Como se mencionaba antes, el RGPD contempla en el inciso e) del art. 6.1 las otras dos bases jurídicas en las que la administración podría basar el tratamiento de datos personales para que este resultase lícito, es decir, el interés público o el ejercicio de competencias, tal y como lo determina también el contenido del art. 8.2 de la LOPDGDD, ya que establece que el tratamiento de datos solo podrá fundarse en alguna de estas dos bases si la competencia de la Administración se encuentra regulada en una norma con rango de ley.

En el primero de los casos, la Administración pública podrá tratar datos personales siempre que esa actividad sirva para cumplir una misión cuyo objeto sea precisamente el interés público; en relación con esto es pertinente señalar qué se entiende como tal y a qué se puede referir en este contexto. El interés público es un concepto jurídico indeterminado, que alude a un interés general de una colectividad y que por obvias razones se contrapone a los intereses de carácter privado. Constitucionalmente el art. 103 prevé que «la Administración sirve con objetividad los intereses generales», los cuales son «*intereses sociales o colectivos que el Estado asume como propios*»[576]. De hecho, la distribución de competencias entre las

[574] Art. 80.1 de la LOPDGDD.
[575] Conforme al considerando 45, art. 6.3 del RGPD y art. 8.1 de la LOPDGDD.
[576] SÁNCHEZ MORÓN, M. *Derecho administrativo. Parte general.* 18ª edición, Madrid, 2019, p. 74. En este mismo sentido el Profesor TRAYTER JIMÉNEZ determina que «*La Administración sólo puede ejercer sus potestades, su poder para fines de interés público y, en concreto, para atender al fin previsto por las normas que regulan cada actividad*», Cfr. TRAYTER JIMÉNEZ, J. M., *Derecho administrativo. Parte general,* Cuarta edición, Atelier, 2019, p. 86. Al hilo de lo anterior, el Profesor PEMÁN GAVÍN establece que: «*La Administración no se sirve a sí misma sino que tiene un fin que está fuera de ella, es una organización instrumental creada para atender los "intereses generales" de la respectiva comunidad en la que se inserta; concepto equivalente con bastante aproximación a los también tradicionales de "bien común" o de "interés público" y que, de acuerdo con el conjunto del texto constitucional, hay que entender referido no solo a los interese colectivos supra-individuales, sino también al interés de cada uno de los ciudadanos, cuya dignidad intrínseca es "fundamento del orden político"*», Cfr. PEMÁN GAVÍN, J. M., «Lección 1. El Derecho administrativo en España. Una introducción», MENÉNDEZ, P. y EZQUERRA, A. (Dirs.), *Lecciones de Derecho administrativo,* Thomson Reuters Civitas, 2019, p. 73.

diversas administraciones, órganos y organismos garantiza el cumplimiento de esos fines de interés general. Al hilo de lo anterior, el interés público deberá precisarse entonces «*casuísticamente con motivo de su aplicación*»[577] en cada tratamiento de datos.

El tercer supuesto, es decir, cuando el tratamiento de datos personales se realizase en ejercicio de las facultades y competencias atribuidas a las administraciones, su actuar estaría limitado a las mismas. De acuerdo con lo establecido en el art. 8.2 de la LOPDGDD, deberán en todo caso de ser conferidas por medio de una norma con rango legal. En el caso de la Administración no puede ser de otra manera ya que deben cumplir con el principio de legalidad, en este sentido GARCÍA DE ENTERRÍA y FERNÁNDEZ determinan que «*La legalidad otorga facultades de actuación, definiendo cuidadosamente sus límites, apodera, habilita a la Administración para su acción confiriéndola al efecto poderes jurídicos. Toda acción administrativa se nos presenta así como ejercicio de un poder atribuido previamente por la Ley y por ella delimitado y construido*»[578]. Esta última base de licitud se diferencia de la primera en cuanto a que la ley no le obliga a tratar datos de manera directa, sino que de sus facultades conferidas se deriva de manera indirecta dicho tratamiento.

Aunque se han analizado por separado las tres posibles bases de licitud, sería posible que una sola norma las contenga para sustentar el tratamiento de datos realizado por las Administraciones públicas, en este contexto el Profesor VALERO TORRIJOS señala que «*es necesario enfatizar que la licitud del tratamiento exige que efectivamente se cumplan las previsiones normativas sobre las condiciones en que ha de llevarse a cabo, no bastando simplemente con la mera habilitación legal*»[579], es decir el cumplimiento de los principios y obligaciones a su a cargo de acuerdo con el nuevo marco normativo. En relación con la norma habilitante para la realización del tratamiento de manera licita, es importante señalar que el considerando 45 del

[577] FERNÁNDEZ RODRÍGUEZ, J. J., *op. cit.,* p. 55
[578] GARCÍA DE ENTERRÍA, E. y FERNÁNDEZ, T-R., *Curso de Derecho Administrativo I,* Decimoctava edición, Tomo I, Thomson Reuters Civitas, Navarra, 2017, p. 487.
[579] VALERO TORRIJOS, J., «Protección de datos de carácter personal, datos abiertos y reutilización de la información del sector público», MARTÍN DELGADO, I. (Dir.), *El procedimiento administrativo y el régimen jurídico de la Administración pública desde la perspectiva de la innovación*, Iustel, Madrid, 2020, p. 419.

RGPD establece que «*una norma puede ser suficiente como base para varias operaciones de tratamiento de datos basadas*» en estos tres supuestos.

Existen otras bases de licitud en las que las AAPP pueden basar el tratamiento de datos, por ejemplo, en el sector sanitario puede realizarse para proteger los intereses vitales del interesado o de terceros. También podrá basarse en el consentimiento por mandato legal, por ejemplo, en la investigación biomédica. Estos dos supuestos se desarrollarán de manera específica posteriormente en el presente trabajo de investigación.

1.2 Principales obligaciones de las Administraciones derivadas del nuevo marco jurídico en materia de protección de datos personales.

Como se ha mencionado anteriormente, cuando la Administración pública actúe como responsable del tratamiento estará obligada a cumplir genéricamente con lo establecido en el RGPD y en la LOPDGDD, sobre todo lo relativo a los principios del tratamiento, además de tener la capacidad de demostrar dicho cumplimiento, lo cual se denomina como «responsabilidad proactiva» (*accountability*). En relación con el nuevo modelo sobre el cumplimiento de la normativa por parte de los responsables el Profesor PIÑAR MAÑAS determina que: «*A partir de ahora será necesario adoptar decisiones propias en función de los tratamientos de datos que se lleven a cabo y la naturaleza de estos*»[580] .De manera específica, la Administración pública deberá cumplir con determinadas obligaciones particulares derivadas de su posición como responsable, relacionadas principalmente con la seguridad de los datos y con las medidas técnicas y organizativas que aseguren un correcto cumplimiento de la normativa en la materia.

1.2.1 El delegado de protección de datos personales.

Antes de la entrada en vigor del RGPD ya se preveía la existencia de esta figura en la legislación comunitaria[581]. Sin embargo, a partir de la fecha de aplicación

[580] PIÑAR MAÑAS, J. L., «I. Introducción. Hacia un nuevo modelo europeo de protección de datos», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos,* Reus, Madrid, 2016, p. 17.
[581] En la Directiva 95/46/CE se preveía en el art. 18.2 la designación de un encargado del tratamiento de datos, el cual se encargaría de: «*hacer aplicar en el ámbito interno, de manera independiente, las*

del RGPD, una de las principales obligaciones a cargo de las Administraciones públicas es contar con un «delegado de protección de datos personales» (en adelante DPD), sin importar la forma en que sean tratados los datos. Y una de sus principales notas características es la independencia.

El documento de trabajo de la Comisión que acompañaba al RGPD, determinaba que el DPD debía ser una persona encargada «*de supervisar y monitorear de manera independiente la aplicación interna y el respeto de las normas sobre protección de datos. El DPD puede ser tanto un empleado interno como un consultor externo*»[582]. Este concepto de DPD al final se positiviza en la Sección 4 del Capítulo IV del RGPD, en la cual se regulan aspectos como su designación, posición y funciones. Por tanto, la definición de DPD en este marco se puede deducir de su contenido, integrando aquellos elementos que no se incluyen en la definición anterior, como aquella persona con conocimientos especializados en derecho y práctica en la materia de protección de datos, designado por el responsable o el encargado del tratamiento, dotado con plena independencia y cuyas funciones

disposiciones nacionales adoptadas en virtud de la presente Directiva», posteriormente fue el TJUE por sentencia de 9 de noviembre de 2010 quien determina que: «*al encargado de la protección de los datos personales le incumbe ejecutar diversas tareas destinadas a garantizar que el tratamiento de los datos no pueda ocasionar una merma de lo derechos y libertades de los interesados»*, *vid.* Apartado 98 de la STJUE (Gran Sala) de 9 de noviembre de 2010 (ECLI:EU:C:2010:662). También esta figura se preveía en el hoy derogado Reglamento 45/2001 del Parlamento y del Consejo, de 18 de diciembre de 2000, relativo a la protección de datos de las personas físicas en los que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de esos datos. Esta figura encuentra continuidad también en el nuevo Reglamento 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) nº45/2001 y la Decisión nº1247/2002/CE. Su existencia también estaba prevista en 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 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. Al margen de lo anteriormente expuesto, de acuerdo con el Profesor RECIO GAYO: «*El origen de la figura de delegado de protección de datos se encuentra en una ley nacional sobre protección de datos. En concreto, Alemania fue el primer país del mundo en incluir esta figura en su ley federal de protección de datos (BDSG 1977) denominándola "Beauftragten für den Datenschutz"», vid.* RECIO GAYO, M., «XXII. El Delegado de Protección de Datos», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad,* Reus, Madrid, 2016, p. 369.

[582] Trad. del inglés: «*A person responsible within a data controller or a data processor to supervise and monitor in an independent manner the internal application and the respect of data protection rules. The DPO can be either an internal employee or an external consultant*», Cfr. Commission Staff Working Paper, *Impact Assessment,* /* SEC/2012/0072 final */ Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012SC0072 (consulta: 30 de abril de 2020).

principales son supervisar que el tratamiento de datos sea conforme al contenido del RGPD así como asesorar al responsable y al encargado (si lo hubiese), incluso antes de que estos comiencen a realizar el tratamiento, e igualmente se encargará de la formación y concienciación del personal, de tal manera que, todos los agentes intervinientes en el tratamiento conozcan los bienes jurídicos que se protegen, las obligaciones a cumplir y cómo puede afectar el incumplimiento de la normativa. En este sentido, para el Profesor SÁNCHEZ ORS la persona que realiza la función de DPD no solo ayuda a proteger los datos personales también debe apoyar la innovación y hacer preservar las libertades individuales[583]. El delegado de protección de datos también es la persona que hace de enlace o interlocutor entre la autoridad de control y el responsable y/o encargado, y de estos últimos con los ciudadanos.

El G29 en sus «Directrices sobre el Delegado de Protección de Datos» determina que la designación del DPD con base en el art. 37.1.a) del RGPD es obligatoria para las autoridades nacionales, regionales y locales con arreglo a las leyes nacionales de los Estados miembros, e incluso también es obligatorio para otros organismos regidos por el derecho público[584]. La AEPD ha determinado que las AA.PP. podrán designar a *«un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño»*[585], así también lo ha determinado la AEPD en su guía «El delegado de protección de datos en las Administraciones» [586]. Este último supuesto es plenamente compatible con los principios constitucionales de eficacia (art. 103 CE) y estabilidad presupuestaria (art. 105 CE), y también con el principio legal de

[583] Cfr. SÁNCHEZ ORS, C., «Capítulo 20. El Delegado de Protección de Datos (Arts. 37-39 RGPD. Arts. 34-37 LOPDGDD», LÓPEZ CALVO, J. (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, p. 497.

[584] GT29, Directrices sobre delegados de protección de datos (DPD), de 13 de diciembre de 2016, p. 5. En este sentido podría interpretarse también que es obligatorio para quienes gestionen servicios públicos, pues tanto en su contratación como en dicha gestión están sometidos al derecho público, sin que en la actualidad sea obligatorio, salvo para las entidades que presten servicios o exploten servicios de comunicaciones electrónicas (si tratan datos a gran escala) y para los centros sanitarios, de acuerdo con el art. 34 de la LOPDGDD.

[585] *Vid.* apartados 1,3 y 6 del art. 37 del RGPD.

[586] Sin embargo, la AEPD considera poco aconsejable su designación «*respecto a grandes unidades u órganos con entidad y tareas claramente diferenciadas*». Se establece que su adscripción dentro de la estructura de la organización «*debe hacerse a órganos o unidades con competencias y funciones de carácter horizontal*», Cfr. AEPD, «*El Delegado de Protección de Datos en las Administraciones públicas»(*en línea), pp. 1-2. Disponible en: https://www.aepd.es/sites/default/files/2019-09/funciones-dpd-en-aapp.pdf (consulta: 20 de septiembre de 2020).

sostenibilidad financiera previsto en el art. 4 de la LO 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, de acuerdo con «*el ejercicio de las competencias que para la gestión de sus intereses respectivos les correspondan*»[587], en específico cuando se requiera personal necesario para hacer frente a este deber legal. En este sentido podrá entonces ser parte del cuerpo de funcionarios o un asesor externo, lo importante es que «*en la práctica sea apreciado como una de las personas clave para asegurar la gobernanza*»[588] en la materia.

Será habitual que los DPD desempeñen su labor a tiempo completo en organizaciones de gran tamaño. En este sentido, por ejemplo, el art. 34 de la LOPDGDD, establece que en todo caso contarán con un delegado los centros docentes de todos los niveles, las universidades públicas y privadas, las empresas que presten servicios de comunicaciones y los centros sanitarios[589]. Su falta de designación de acuerdo con el art. 73.v) de la LOPDGDD constituiría una infracción grave, sancionada con apercibimiento[590]. Sin embargo, para entidades de menor tamaño incluso se puede compaginar esta labor con otras, siempre que no suponga un conflicto de intereses[591]. Al hilo de lo anterior, el informe 2018-0170 de la AEPD determina que «*deben diferenciarse la figura del delegado de protección de datos y del responsable de seguridad*» [592] dentro de las AAPP, pues el responsable de seguridad se encarga de tomar «*las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios*»[593] del Esquema Nacional de Seguridad, por tanto, recibe instrucciones del responsable del tratamiento, de manera que nombrar a una misma persona para desempeñar las dos funciones «*supondría, negar el principio de independencia y segregación de funciones del ENS (art. 10) y, una negación del principio de independencia que determina el RGPD (Art. 38.3)*» [594]. Incluso la naturaleza de las funciones que desempeñan estos dos agentes son distintas, ya que «*la función de seguridad de la información es una herramienta que permite abordar el cumplimiento de lo previsto en el artículo 32 del RGPD, pero no*

[587] F.J. 2 de la STC (Pleno) 27/1987, de 27 de febrero (RTC\1987\27; ECLI:ES:TC:1987:27).
[588] Cfr. RECIO GAYO, M., *op. cit.,* p. 381.
[589] Incisos a), b), c) y l) del apartado 1.
[590] Art. 77.2 de la LOPDGDD.
[591] AEPD, «*El Delegado de Protección…» op. cit.,* p. 2.
[592] AEPD, informe 2018-0170, p. 10.
[593] Art. 10 del 3/2010, de 8 de enero por el que se regula el Esquema Nacional de Seguridad.
[594] AEPD, informe 2018-0170, p. 11.

puede entenderse como una herramienta que garantice el pleno e íntegro cumplimiento del RGPD. En consecuencia, las funciones del RSEG tienen un alcance limitado en el RGPD frente al alcance de las competencias del DPD»[595]. Por lo anterior, de manera general estas dos funciones deberán ser desempeñadas por dos personas distintas, salvo en situaciones excepcionales en corporaciones que por su tamaño y recursos no puedan asumir dicha separación[596].

En cuanto a la idoneidad del DPD la autoridad pública designará a personas que cuenten con experiencia y conocimientos especializados en materia de protección de datos personales[597], tal y como lo establece el apartado 5 del art. 37 del RGPD. Añade el art. 35 de la LOPDGDD que para demostrar la suficiencia profesional se podrán tomar en cuenta «*mecanismos voluntarios de certificación que tendrán particularmente en cuenta la obtención de una titulación universitaria que acredite conocimientos especializados en el derecho y en la práctica en materia de protección de datos*». Actualmente la AEPD y la Entidad Nacional de Acreditación cuentan con un esquema de certificación, de manera conjunta con se encargan de autorizar a las entidades de certificación para que estas últimas a su vez, valga la redundancia, acrediten si una persona cuenta con conocimientos teóricos y prácticos en protección de datos personales, con base en la norma UNE-EN ISO/IEC 17024:2012 y el propio Esquema de certificación de Delegados de protección de datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD)[598]. A este respecto SÁNCHEZ ORS determina que la certificación opera como «*un sello de*

---

[595] *Ib.*, p. 14.

[596] Se determina que en esta circunstancia excepcional el encargado de seguridad podrá asumir las funciones del delegado de protección de datos, siempre que «*concurran los requisitos de formación y capacitación previstos en el RGPD. Además, resultaría imprescindible adoptar todas las medidas organizativas, debidamente reflejadas en su Política de seguridad de la información, que garantice la necesaria independencia y la ausencia de conflicto de intereses, por lo que no podría recibir instrucciones respecto al desempeño de sus funciones como delegado de protección de datos, deberá responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. En todo caso, esta circunstancia, que como decíamos, tiene carácter excepcional, deberá evaluarse caso por caso, y deberá dejarse documentada dicha designación haciendo constar los motivos por lo que el organismo correspondiente no ha podido observar dicha separación de funciones así como las medidas que garantizan la necesaria independencia del delegado de protección de datos*», Cfr. *Ib.*, p. 16.

[597] Considerando 97 del RGPD.

[598] Cfr. AEPD, «*Esquema de certificación de Delegados de protección de datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD)*». Disponible en: https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf (consulta: 4 de mayo de 2020).

calidad» que «*ayuda a identificar a los candidatos con ciertos niveles de conocimiento desmostrables*»[599] que puede servir como parámetro para su elección.

Es necesario puntualizar que la labor de los DPD de la Administración pública «*sean o no empleados del responsable del tratamiento, deben estar en condiciones de desempeñar sus funciones y cometidos de manera independiente*»[600], de acuerdo con establecido así por el contenido del art. 38. 3 del RGPD. Por tanto, el DPD no debe admitir instrucciones de quien lo haya designado en el desempeño de sus funciones y no podrá ser sustituido ni sancionado como consecuencia del desempeño de estas, salvo que incurra en dolo o negligencia grave[601]. Para que esta independencia sea real no debe existir ningún tipo de conflicto de intereses que ponga en riesgo su labor, específicamente sus deberes de confidencialidad y secreto hacia el responsable o encargado según sea el caso[602]. En este sentido el Profesor JIMÉNEZ ASENSIO determina que la atribución de rol de DPD «*siquiera sea como función adicional o adjetiva, puede suponer una vulneración de esa regla recogida en el artículo 38.6 RGPD. Todos aquellos puestos de trabajo que intervengan, directa o indirectamente, en el tratamiento de datos personales, así como tanto los puestos de representación jurídica (en cuanto pueden implicar objetivamente la defensa ante los tribunales de los responsables o encargados) y en especial los puestos de estructura directiva o de jefatura, son ámbitos en los que pueden surgir potencial u objetivamente conflictos de intereses. Lo razonable es no acumular esas tareas con las propias del DPD*»[603]. Ahora bien, en relación con la participación del DPD en los asuntos relacionados con el tratamiento dentro de las AAPP, en este caso los responsables del tratamiento deberán proveer los recursos materiales necesarios para el cumplimiento de sus funciones[604].

Las AAPP deberán publicar los datos de contacto del DPD y comunicarlos también a la autoridad de control competente, para que el DPD sea el punto de

[599] SÁNCHEZ ORS, C., *op. cit.,* p. 504.
[600] Considerando 97 del RGPD.
[601] Cfr. Apartado 3 del art. 38 del RGPD y apartado 2 del art. 36 de la LOPDGDD.
[602] *Vid.* apartado 2 del art. 36 de la LOPDGDD y, apartados 5 y 6 del art. 38 del RGPD.
[603] JIMÉNEZ ASENSIO, R., «La figura del delegado de protección de datos en las organizaciones públicas» (en línea). Disponible en: https://rafaeljimenezasensio.files.wordpress.com/2018/03/articulo-dpd-4.pdf (consulta: 29 de diciembre de 2020).
[604] Cfr. Apartados 1 al 3 del art. 38 del RGPD.

contacto entre estos [605]. Esta obligación accesoria permite a los interesados relacionados con la Administración pública [606], conocer ante quien puede ejercer sus derechos, y si lo estimase pertinente hacer del conocimiento al DPD su inconformidad con el tratamiento de los datos para que este último se lo haga saber al responsable incluso antes de acudir a la autoridad de control de manera potestativa. En este sentido deberá recibir y atender a las reclamaciones presentadas ante la autoridad de control si así lo estimase conveniente [607]. De acuerdo con el G29 no se requiere que se incluya el nombre del DPD, sin embargo, esta autoridad considera que su publicación es una práctica recomendable. De cualquier forma, determina necesario que se incluya *«información que permita a los interesados y a las autoridades de control comunicarse con este de forma sencilla (dirección postal, un número de teléfono específico y/o una dirección de correo electrónico específica). Cuando corresponda, a efectos de comunicación con el público, podrían facilitarse otros medios de comunicación, por ejemplo, una línea directa específica o un formulario de contacto específico dirigido al DPD en el sitio web de la organización»* [608].

Lo anterior cobra especial relevancia cuando particulares traten datos personales por cuenta del responsable con motivo de la prestación de un servicio público, llámese transporte, servicios sanitarios, vivienda pública, etc., en cuyo caso las medidas que deberán adoptar estos agentes privados tendrán que ser similares a las que deba adoptar la Administración responsable, pues como apuntan las GT29: «*En estos casos, los interesados pueden encontrarse en una situación muy similar a la que se da cuando sus datos son tratados por una autoridad u organismo público. En particular, los datos pueden tratarse con fines similares y las personas suelen tener igualmente poca o ninguna opción sobre si sus datos se tratarán y cómo se tratarán,*

[605] Cfr. Apartado 7 del art. 37 del RGPD.
[606] El GT29 recomienda como buena práctica dentro de la organización de los responsables informar los datos de contacto del DPD, haciendo uso de «*la intranet de la organización, en el directorio telefónico interno y en el organigrama»,* GT29, Directrices sobre delegados (…) *op. cit.,* p. 14.
[607] *Vid.* art. 37 de la LOPDGDD.
[608] GT29, Directrices sobre delegados de protección de datos (DPD), de 13 de diciembre de 2016., p. 14.

por lo que pueden necesitar la protección adicional que puede aportar la designación de un DPD»[609].

El DPD al supervisar la implantación de las medidas técnicas y organizativas antes del tratamiento, durante y después, corrobora que el personal cuenta con la información suficiente acerca de sus funciones y responsabilidades, incluso podrá recomendar su formación en la materia para concienciar al mismo. La AEPD en relación con lo anterior determina como aconsejable «*establecer con carácter permanente actividades de formación en protección de datos para empleados públicos que deseen especializarse en la materia y optar eventualmente a ocupar los puestos de DPD*»[610]. También asistirá al responsable cuando sea necesaria una evaluación de impacto[611].

El DPD deberá en todo momento cooperar con las autoridades de control y de manera específica, en lo relativo a procedimientos iniciados por posibles incumplimientos de la normativa comunitaria y nacional[612], pues conforme al art.

[609] *Ib.,* p. 7.
[610] AEPD, «*El Delegado de Protección de Datos en las Administraciones públicas*» (en línea), p. 3. Disponible en: https://www.aepd.es/sites/default/files/2019-09/funciones-dpd-en-aapp.pdf (consulta: 20 de septiembre de 2020).
[611] De acuerdo con la AEPD las labores genéricas establecidas por el RGPD, pueden ser traducidas en la ejecución de tareas relacionadas con: 1) la comprobación del cumplimento de los principios aplicables al tratamiento, 2) la identificación de las bases jurídicas de los tratamientos, 3) la valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos, 4) el examen de la normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos, 5) el diseño e implantación de medidas de información a los afectados por los tratamientos de datos, 6) el establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados, 7) la valoración de las solicitudes de ejercicio de derechos por parte de los interesados, 8) la contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado, 9) el Diseño e implantación de políticas de protección de datos, la realización de auditorías en materia de protección de datos, 10) la gestión de los registros de actividades del tratamiento, 11) llevar a cabo análisis de riesgos, 12) la implementación de medidas que protejan los datos desde el diseño y por defecto adecuadas a los riesgos a la naturaleza tanto de los datos como del tratamiento, 13) poner en funcionamiento medidas de seguridad adecuadas a los riesgos y a la naturaleza de los datos y los tratamientos, 14) implementar protocolos en caso de posibles violaciones de seguridad, 15) determinar si es necesaria la realización de evaluaciones de impacto dependiendo las finalidades y los tipos de datos que trate el responsable, 16) realizar dichas evaluaciones de impacto, 17) mantener contacto con la autoridad de control competente, y 18) implementar programas de formación dirigidas al personal del órgano o entidad, incluidos los que tengan que ver con sensibilización en el tratamiento de datos de carácter personal. De acuerdo con lo establecido en: AEPD, «*El Delegado de Protección de Datos en las Administraciones públicas*» (en línea), pp. 3-4. Disponible en: https://www.aepd.es/sites/default/files/2019-09/funciones-dpd-en-aapp.pdf (Consulta: 20 de septiembre de 2020).
[612] Cfr. Incisos c) y d) del apartado 1 del art. 39 del RGPD.

36 de la LOPDGDD debe actuar como «*interlocutor*» entre la AEPD y los responsables[613].

En cuanto a la relación del DPD con los interesados, la Profesora BOTELLA PAMIES determina que en este caso el RGPD introduce «*la vertiente de la figura del "Delegado-Mediador", como agente que tiene la función de resolución de conflictos del ámbito del proceso administrativo, o en su caso judicial. De esta manera, se otorga al DPD un papel de "interlocutor" entre el afectado que se ve menoscabado en su derecho de protección de datos y la organización con el objetivo de que pueda solventar o resolver todo tipo de reclamaciones, ejercicios de derecho, y cualquier incidencia en materia de protección de datos*»[614]. Pues con carácter previo a la presentación de una reclamación contra el responsable o encargado ante una autoridad de control, los interesados podrán dirigirse al DPD para hacer saber a este último la posible existencia de la vulneración de alguno de sus derechos contemplados en la normativa de la materia, en cuyo caso deberá ser resuelta y comunicada en un plazo máximo de dos meses a contar desde su recepción[615]. Sin embargo, también tendrá conocimiento una vez presentada una reclamación ante la autoridad de control, «*siempre que se hubiera presentado con carácter previo ante este la misma reclamación, en cuyo caso le requerirán para que remita la respuesta dada, si ésta fue emitida en su momento»*[616]*.* En caso de no obtener respuesta del DPD pasado el plazo de un mes se seguirá con el procedimiento del art. 65.5 de la LOPDGDD según el cual la autoridad de control deberá de admitir o inadmitir a trámite la reclamación. Considero que el objeto principal que lleva a cabo el DPDP en este caso es intentar que el responsable cese de la realización de las conductas que el interesado estima que lesionan su derecho a la protección de datos a través de medidas técnicas y organizativas adecuadas para corregirlas antes de que se le cause al interesado un perjuicio que suponga una difícil reparación, y en su caso la iniciación de un

[613] Apartado 1 del art. 36 de la LOPDGDD.
[614] BOTELLA PAMIES, E., «Artículo 37. Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos», ARENAS RAMIRO, M. y ORTEGA GIMÉNEZ, A. (Dirs.), *Protección de datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*, Sepín, Madrid, 2019, p. 199.
[615] Art. 37.1 de la LOPDGDD.
[616] Cfr. TERRÓN SANTOS, D. y DOMÍNGUEZ ÁLVAREZ, J.L, *Nueva regulación de la protección de datos y su perspectiva digital,* Comares, Granada, 2019, p. 130.

procedimiento sancionador si tales conductas constituyesen también una infracción.

1.2.2 Evaluación de impacto, evaluación de riesgos y medidas de seguridad.

El RGPD cuenta con varios mecanismos dirigidos a preservar la seguridad de los datos personales de los interesados. La evaluación de impacto es una medida de responsabilidad proactiva que debe realizarse por los responsables del tratamiento antes de iniciar dicha actividad, en palabras de RIVAS LÓPEZ es: «*un tipo de análisis de riesgos*»[617]. Su obligatoriedad depende en gran parte de la existencia o no de un «*alto riesgo para los derechos y libertades de las personas físicas*»[618]. Al hilo de esto el MARÍN JIMÉNEZ determina que: «*es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se lleva a cabo con los mismos*»[619].

La evaluación de impacto en la protección de datos (EIPD) parte del análisis de la base de licitud, los medios utilizados en el tratamiento de datos, los tipos de tratamientos, la naturaleza y categorías de los datos personales, el alcance del tratamiento y la cantidad de datos que se traten. Para el caso que nos ocupa, el considerando 93 del propio Reglamento determina que las autoridades u organismos públicos de los Estados miembros podrán realizar una evaluación de impacto previa al inicio del tratamiento de datos basada en el desempeño de sus funciones, y así se establece también en el apartado 10 del art. 35 del RGPD. En relación con lo anterior, el GT29 en sus «Directrices sobre la EIPD» determina que no se requiere utilizar esta medida si no es *«"probable que el tratamiento entrañe un alto riesgo", exista una EIPD similar, el tratamiento se haya autorizado antes de mayo*

[617] RIVAS LÓPEZ, J.L., «Auditoría y seguridad de datos: Análisis de riesgos», CAMPOS ACUÑA, C., *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, segunda edición, Wolters Kluwer, 2019, p. 673.
[618] Cfr. 35.1 del RGPD.
[619] MARÍN JIMÉNEZ, R., «Evaluación de impacto en la Protección de Datos. Paralelismos» (en línea), *Revista de la Sociedad española de informática y salud*, núm. 134, abril 2019, p. 24. Disponible en: https://seis.es/is-134-abril-2019/ (consulta 1 de enero de 2021).

de 2018, tenga base jurídica o se encuentre en la lista de operaciones de tratamiento para las que no se requiere una EIPD»[620].

En este sentido, de manera genérica esta medida se exceptúa si se reúnen los siguientes requisitos: 1) que la base de licitud del tratamiento se funde en el apartado c) o e) del art. 6.1 del RGPD; 2) que el tratamiento de datos tenga su base jurídica en el derecho del Estado miembro; 3) que ese derecho regule las operaciones del tratamiento o la operación específica del mismo; 4) o que ya se haya realizado una evaluación de impacto general.

Por su parte la AEPD ha publicado una «*Lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos según el Artículo 35.5 RGPD*»[621] que complementa las Directrices del GT29; en esta lista se establece que no será necesario tampoco una EIPD en los siguientes casos: 1) tratamientos de datos llevados a cabo y conformes con las circulares o decisiones de las Autoridades de control, especialmente las de la AEPD, siempre que el tratamiento no haya sido modificado; 2) tratamientos de datos que se ciñan a códigos de conducta aprobados por la Comisión, por alguna autoridad de control incluida la propia Agencia, y se haya llevado a cabo una EIPD para la validación del referido código de conducta; 3) los tratamientos de datos que deban realizarse en cumplimiento de una obligación legal, con motivo de un interés público o derivado de las competencias atribuidas a una autoridad pública, siempre que la ley no obligue a los responsables a realizar una EIPD y ya se haya realizado de manera completa en la adopción de dicha base de licitud; 4) tratamientos de datos efectuados por trabajadores autónomos salvo que se cumplan dos o más de los once tipos de tratamientos incluidos en la lista «*de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)*» elaborada por la propia AEPD[622]; 5) lo mismo para aquellos datos de las PYMES relacionados con su gestión interna, salvo los relativos a sus clientes; 6) ni a datos relacionados

[620] GT29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679, p. 14.
[621] Basada en las Directrices del GT29 en la materia, antes referidas.
[622] Cfr. AEPD, «*Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)*». Disponible en: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf (consulta: 11 de noviembre de 2020).

con las comunidades y subcomunidades de propietarios; 7) finalmente no se requerirá una EIPD para los tratamientos de datos de asociaciones y colegios profesionales, salvo que incluyan datos de categorías especiales y no se les aplique alguna de las excepciones previstas en el art. 9.2 del RGPD[623].

En relación con el objeto de nuestra investigación la evaluación de impacto en principio no será obligatoria de manera previa al tratamiento de datos llevado a cabo por administraciones públicas, salvo que estas lo consideren necesario. Hasta el momento la LOPDGDD solo hace referencia a la evaluación de impacto para los tratamientos que sean llevados a cabo con fines de investigación científica de la salud[624], lo cual es aplicable a instituciones y organismos públicos que realicen tal actividad.

En el contexto social en el que vivimos podríamos afirmar que es necesaria una evaluación de impacto en caso de que las administraciones implementen y hagan uso de aplicaciones o medios electrónicos para conocer la localización de las personas o su estado de salud[625]. Por tanto, deberán aplicar a sus EIPD los documentos orientativos de la AEPD para facilitar tal labor, como el «*Listado de cumplimiento normativo*»[626] y el «*Modelo de evaluación de impacto en la protección de datos (EIPD) para Administraciones Públicas*», para adoptar las medidas técnicas y organizativas adecuadas al caso concreto que garanticen el pleno cumplimiento del RGPD y de la LOPDGDD durante todo el ciclo de vida del tratamiento de datos.

Sin perjuicio de lo anterior la valoración de riesgos es otra medida encaminada a preservar la seguridad de los datos, especialmente cuando las administraciones públicas actúan como responsables del tratamiento, en este

---

[623] Cfr. AEPD, «*Lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos según el art. 35.5 RGPD*». Disponible en: https://www.aepd.es/sites/default/files/2019-09/ListasDPIA-35.5l.pdf (consulta: 11 de noviembre de 2020).

[624] Inciso f), apartado 2 de la D.A. 17ª.

[625] Por ejemplo, el uso de tarjetas de transporte público o la utilización de aplicaciones como las recientemente desarrolladas con motivo de la COVID-19.

[626] En el que la AEPD señala un listado a modo de tabla en la que se describen «*las cuestiones mínimas de obligado cumplimiento a tener en cuenta en los tratamientos de datos según lo previsto por el articulado del RGPD*», de manera que los responsables comprueben su grado de cumplimiento y puedan abordar las deficiencias detectadas por los mismos, *vid.* AEPD, «*Listado de cumplimiento normativo*». Disponible en: https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf (consulta: 11 de noviembre de 2020).

contexto «*antes de poner en marcha nuevas actividades de tratamiento o modificar servicios ya prestados que hagan uso de nuevas tecnologías, deberán identificar aquellos riesgos a los que pueda estar expuesto el tratamiento*»[627]. El análisis de riesgos en palabras de RIVAS LÓPEZ se lleva a cabo cuando el producto o servicio «*ya está desarrollado o en producción»*, por tanto, tiene «*un alcance temporal diferente»* a las EIPD[628]. En este sentido el Profesor ROMEO RUÍZ determina que: «*El análisis debe dirigirse, fundamentalmente, a parámetros de la seguridad de la información. Se trata de una evaluación de riesgos que no va dirigida a analizar las amenazas que pudiera causar en la organización, sino que debe centrar el foco en la prevención de posibles vulneraciones de los derechos y libertades de los ciudadanos y ciudadanas*»[629] De acuerdo con la «*Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*» de la AEPD, esta tarea implica «*considerar todos los posibles escenarios en los cuales el riesgo se haría efectivo. La evaluación de riesgos consiste en valorar el impacto de la exposición a la amenaza, junto con la probabilidad de que esta se materialice*»[630]. De manera que, la finalidad de esta medida es la identificación de los riesgos, el impacto que podrían tener en los derechos y libertades de las personas y determinar la eficacia de las medidas de seguridad adoptadas hasta el momento de dicha evaluación.

Así pues, la AEPD en su guía «*Protección de datos y Administración Local*» entiende que el RGPD obliga a los responsables a llevar a cabo la valoración del riesgo en el tratamiento de datos[631], a fin de determinar si las medidas de seguridad que han sido adoptadas aún resultan idóneas y eficaces para cada tipo de tratamiento. Lo anterior es extrapolable a entonces a todas las administraciones públicas y al sector público institucional; sobre todo cuando se lleve a cabo

---

[627] AEPD, «*Tecnologías y protección de datos en AA.PP.*», p. 8. Disponible en: https://www.aepd.es/sites/default/files/2020-11/guia-tecnologias-admin-digital.pdf (consulta: 8 de enero de 2021).

[628] RIVAS LÓPEZ, J.L., *op. cit.,* p. 673.

[629] ROMEO RUÍZ, A., «La responsabilidad proactiva de las administraciones públicas en protección de datos personales» (en línea), *Revista Vasca de Gestión de Personas y Organizaciones Públicas,* núm. 18, 2020, pp. 146. Disponible en: https://www.ivap.euskadi.eus/contenidos/informacion/18_revgp/eu_def/Romeo_138_153.pdf (consulta: 1 de enero de 2021).

[630] AEPD, «*Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*», p. 4.

[631] AEPD, «*Guía Protección de datos y Administración Local*», p. 19.

tratamientos de datos que desvelen situaciones de vulnerabilidad de determinados colectivos[632], y, en general, si la recogida de datos se realiza en grandes cantidades. En este sentido el Profesor ROMEO RUÍZ establece que la revisión de las medidas de seguridad es una consecuencia del análisis del riesgo «*según las características de los tratamientos, sus riesgos, el contexto en el que se desarrollan, las posibilidades técnicas y los costes que entrañen*»[633]. Por su parte la AEPD ha determinado que en este caso «*La actitud correcta es conocer el riesgo, evaluar sus consecuencias, tomar medidas para minimizarlo y controlar su efectividad en el contexto cambiante*»[634], sobre todo si las AA.PP. pretenden implementar en su actividad o en la prestación de servicios algún tipo de tecnología disruptiva.

Todos los responsables del tratamiento, incluidas las administraciones públicas deberán garantizar un nivel adecuado de seguridad en el tratamiento de datos personales, según sea el caso. La cual se traduce en medidas técnicas y organizativas que deberán adoptar los responsables con el fin de garantizar la confidencialidad, integridad y disponibilidad de los datos en los sistemas de tratamiento, como la seudonimización y el cifrado. También podrán adoptarse aquellas medidas que permitan hacer posible la accesibilidad y disponibilidad de los datos en caso de incidentes de seguridad. En relación con lo anterior, los responsables del tratamiento podrán acudir a técnicas de verificación, evaluación y valoración para conocer la eficacia de sus medidas de seguridad en el tratamiento de los datos[635].

La D.A. 1ª de la LOPDGDD señala que, en el ámbito del sector público, los responsables incluidos en el art. 77.1 de la misma ley y cuando terceros presten servicios bajo el régimen de concesión, encomienda de gestión o contrato se deberán adoptar las medidas de seguridad según sea el caso establecidas en el Esquema Nacional de Seguridad (ENS), con la finalidad de cumplir con lo establecido en el art. 32 del RGPD. En este sentido como bien apunta el Profesor SIMÓN CASTELLANO el apartado segundo de esta D.A. 1ª antes señalada implica que «*las actividades de*

[632] Como podría ser el caso de las solicitudes a determinadas subvenciones o ayudas y programas sociales.
[633] ROMEO RUÍZ, A., «La responsabilidad proactiva de las administraciones…» *op. cit.,* p. 146.
[634] AEPD, «*Tecnologías y protección…*», *op. cit.,* p. 8.
[635] Cfr. Art. 32.1 del RGPD.

tratamiento que se relacionen con el ejercicio de potestades de derecho público quedarán de facto sujetas al ENS»[636].

La hoy derogada Ley 11/2007, de 22 de junio de acceso electrónico de los ciudadanos a los Servicios Públicos, estableció el Esquema Nacional de Seguridad, el cual fue aprobado por medio del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Actualmente se encuentra previsto en el apartado segundo del art. 156 la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El ENS tiene por objeto «establecer *la política de seguridad en la utilización de medios electrónicos*»[637]. En relación con el tratamiento automatizado de los datos personales, el ENS determina medidas de protección cuyo propósito global es garantizar la seguridad de los datos personales, los sistemas de tratamiento que los tratan, la seguridad de las comunicaciones de esos datos y, en general garantizar la seguridad durante el ciclo de vida de los datos asociados a un tratamiento automatizado llevado a cabo por cualquier administración pública que esté sometida al mismo. Entonces las AA.PP. adicionalmente tendrán que respetar los principios de: a) seguridad integral, b) gestión de riesgos, c) prevención, reacción y recuperación, d) líneas de defensa, e) reevaluación periódica y, f) función diferenciada, contemplados en el art. 4 y desarrollados en los artículos comprendidos del 5 al 10 del mismo ENS[638].

Igualmente, las AA.PP. deberán cumplir con los requisitos mínimos de seguridad acordes al contenido del art. 11.1 del ENS. Estos requisitos mínimos deberán contenerse en la política de seguridad que adopten los órganos superiores de las AA.PP., entendidos como tales aquellos «*responsables directos de la ejecución de la acción del gobierno, central, autonómico o local*»[639]. Para el caso de los

[636] SIMÓN CASTELLANO, P., «La protección de datos en el sector público: efectos y transformaciones tras la LOPDGDD», *Actualidad Administrativa* (en línea), núm. 9, septiembre 2020. Disponible en: smateca.es (consulta: 4 de enero de 2020).
[637] Cfr. Art. 156.2 de la LRJSP.
[638] Para un estudio más en profundidad *vid.* ALAMILLO DOMINGO, I., «Capítulo 16. Esquema Nacional de Seguridad: La administración electrónica y la seguridad de la información», CAMPOS ACUÑA, C. (Dir.), Aplicación práctica y adaptación de la protección de datos en el ámbito local, Segunda edición, Wolters Kluwer, 2019, pp. 607-639.
[639] *Vid.* art. 11.2 del ENS.

Municipios, se podrá realizar una política de seguridad común elaborada en su caso por la Diputación, Cabildo, Consejo Insular u órgano unipersonal de carácter representativo que corresponda.

Para entender las medidas específicas adoptadas para asegurar la seguridad de los datos de carácter personal, primero tenemos que conocer cómo se deben seleccionar las medidas de seguridad según el ENS, en este sentido tendremos que evaluar de manera conjunta los medios y las medidas de seguridad. En este marco, lo primero será identificar los tipos de archivos con los que cuente la administración pública, posteriormente se debe identificar la categoría del sistema, la cual está basada en la valoración del impacto que tendría un incidente en la seguridad de la información o en los sistemas de la Administración pública, siempre que tenga repercusión en los distintos aspectos de la capacidad organizativa de la misma. Por lo que es necesario conocer las diferentes dimensiones de seguridad en la disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad de la información o del sistema, con el fin de determinar el impacto que tendría en la Administración pública en caso de producirse un incidente. Posteriormente se requiere que la Administración pública sea la que, en caso de producirse un incidente, en el que la información o servicio ofrecido electrónicamente puede verse afectado en esas diferentes dimensiones de seguridad, deberá graduar la intensidad del posible incidente dependiendo de su afectación pudiendo catalogarla en niveles: bajo, medio y alto, en función de los parámetros dados para cada nivel[640]. Lo que corresponderá también a la determinación del sistema de información y a la secuencia de actuaciones para determinar la categoría de cada sistema[641], para con todo ello ser capaces de por fin, catalogar las medidas de seguridad.

En cuanto a la previsión de medidas de seguridad específicas en el ENS para los datos de carácter personal, se determina en el apartado 2 del Anexo II del mismo esquema, que el impacto sobre la organización de la Administración en cuestión afectaría en la capacidad organizativa, en la protección de los activos, en el cumplimiento de las obligaciones, en el respeto a la legalidad vigente y a los

[640] Los cuales se encuentran en el apartado 3 del Anexo I del ENS.
[641] Lo descrito anteriormente se basa en el contenido del Anexo I del SNS.

derechos de las personas, con lo cual se deberán adoptar las medidas de seguridad del nivel bajo en los tres niveles: bajo, medio y alto, es decir, las de un perjuicio limitado, cuyas medidas de seguridad específicas se traducen en el cumplimiento de medidas de protección llevadas a cabo en relación con la normativa en materia de protección de datos, ahora contenido en el RGPD y en la LOPDGDD, «*sin perjuicio de cumplir, además con las medidas establecidas*» [642] en el ENS. No obstante, debe cumplirse con la totalidad de las medidas de seguridad en el marco organizativo, operacional y de protección contenidas en el ENS tal y como lo determina la LOPDGDD.

En el propio sistema de seguridad se prevé un sistema de métricas «*para conocer el grado de implantación de las medidas de seguridad que apliquen de las detalladas en el Anexo II y, en su caso, para proveer el informe anual requerido por el artículo 35*», lo cual ha traído consigo la implementación de la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad [643], con el objeto de «*establecer las condiciones relativas a la recopilación y comunicación de datos que permita conocer las principales variables de la seguridad de la información de los sistemas comprendidos en el ámbito de aplicación del Esquema Nacional de Seguridad, y confeccionar un perfil general del estado de la ciberseguridad en las Administraciones públicas*» [644]. Debe señalarse que el riesgo de las herramientas y medidas de seguridad desarrolladas e implementadas por las AA.PP., tienen un nivel más que óptimo en cuanto a seguridad. El riesgo en materia de protección de datos para las AA.PP. radica en la posibilidad de utilizar tecnologías que no sigan el ENS por ser desarrolladas por agentes privados, y estar por tanto sometidas a sus condiciones de servicio.

Finalmente, las AA.PP. tienen la obligación de notificar tanto a la autoridad de control como a los interesados si ha habido una violación de la seguridad de los datos personales. En relación con la notificación realizada a la autoridad de control,

[642] De acuerdo con el apartado 5.7.1 del Anexo II del ENS.
[643] Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2016-10108 (consulta: 25 de septiembre de 2020).
[644] Apartado I de la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad.

esta debe llevarse a cabo lo antes posible y a más tardar en un plazo máximo de setenta y dos horas contadas desde que se haya producido ese suceso, de manera contraria las AA.PP. deberán justificar dicha dilación temporal. Estas no estarán obligadas a notificar a la autoridad las violaciones de seguridad que no afecten o puedan afectar a los derechos y libertades de las personas físicas. El responsable le hará saber a la autoridad de control su naturaleza, las categorías de datos personales que han sido afectados, el número de afectados y los registros que han sido perjudicados. En cuanto al encargado, este debe comunicar al responsable de forma inmediata si ocurre alguna violación de la seguridad.

1.2.3 Registro de actividades de tratamiento.

Otra de las obligaciones que deberán cumplir las AA.PP. en la materia, es llevar un registro del tratamiento de datos personales, con la particularidad de dar a conocer su base legal y hacerlo público y accesible por medios electrónicos[645]. Esta obligación sustituye la de registrar los ficheros de datos ante la autoridad de control competente[646]. De acuerdo con el contenido del art. 30 del RGPD estos registros deben estar a disposición de la autoridad de control competente y contener los siguientes datos: los datos de contacto del responsable del tratamiento y del DPD, las finalidades del tratamiento, las categorías de los interesados, de los datos y de los destinatarios (en este último caso si se prevé la comunicación de estos), el plazo previsible para la supresión por categorías, y la descripción de las medidas técnicas y organizativas relacionadas con su seguridad de los datos. De manera que «*debe arrojar luz sobre cuestiones muy diversas relacionadas con esa operación o actividad que implica el procesamiento de datos. Así debe ayudar a contextualizar el uso de*

[645] Apartado 2 del art. 31 de la LOPDGDD.

[646] Establecida en tanto en la Directiva 95/46/CE como en la LO 15/1999, de 13 de diciembre (arts. 26 y ss. para los ficheros de titularidad privada y para los ficheros de titularidad pública (arts. 20 y ss.). En este sentido SANZ MARCO en relación con el marco jurídico anterior que obligaba a los responsables a registrar sus ficheros determina que: «*De esta forma, si hasta ahora se ha venido realizando la declaración de los ficheros a la autoridad de control de acuerdo con las obligaciones de la LOPD estaríamos en condiciones de aprovechar con muy poco esfuerzo el trabajo ya realizado. También nos serviría de lista de comprobación para garantizar que todos los tratamientos identificativos se asocian a alguno de los ficheros ya declarados*», Cfr. SANZ MARCO, LL., «Capítulo 8. Medidas organizativas para la implantación del marco legal de protección de datos personales. El registro de actividades de tratamiento», CAMPOS ACUÑA, C. (Dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, Segunda edición, Wolters Kluwer, 2019, p. 336.

nuevas tecnologías en el marco de esa concreta actividad y aportar información necesaria para valorar si las mismas son especialmente invasivas para la privacidad. Debe aportar también claridad sobre las relaciones entre los diferentes actores implicados en el tratamiento, esto es, las relaciones entre responsables y encargados, la existencia de corresponsables o de cadenas complejas de encargados del tratamiento»[647].

La AEPD considera que este registro es una herramienta que permite «*tener una perspectiva general de todas las actividades de tratamiento de los datos personales que una organización está llevando a cabo. Es, por tanto, un requisito previo para la observancia de las normas y, como tal, una medida efectiva de rendición de cuentas*»[648]. Por su parte el GT29 establece que nada impide a los responsables y encargados asignar esta tarea al DPD, ya que «*dicho registro debe considerarse una de las herramientas que permiten al DPD realizar sus funciones de supervisión de la observancia de las normas y de información y asesoramiento al responsable o al encargado del tratamiento*»[649]. En este sentido el Profesor ROMEO RUIZ determina que «*El registro de actividades de tratamiento es un elemento esencial para el cumplimiento del principio de responsabilidad proactiva, puesto va a ser el instrumento que va a permitir poder demostrar en cada momento el cumplimiento efectivo de los principios del RGPD*»[650]. En este sentido esta obligación a cargo de los responsables del tratamiento implica «*acotar muy bien los conceptos de tratamiento y la necesidad de disponer de herramientas para la gestión del registro de actividades de tratamiento*»[651], es decir, un portal de internet o una sede electrónica[652] que este

[647] SIMÓN CASTELLANO, P., «La protección de datos en el sector público…» *op. cit.,*
[648] GT29, Directrices sobre los delegados…*op. cit.,* p. 21.
[649] *Ib.,* p. 9.
[650] ROMEO RUÍZ, A., «La responsabilidad proactiva de las administraciones…» *op. cit.,* p. 147.
[651] SANZ MARCO, LL., *op. cit.,* p. 331.
[652] Recordemos que según establece el contenido del art. 38.2 de la LRJSP su contenido debe ser integro, veraz y actualizado. En este sentido el Profesor FONDEVILA ANTOLÍN determina que este artículo establece la responsabilidad de las AAPP «*por los posibles perjuicios causados por una deficiente o insuficiente información proporcionada en su sede electrónica, pues recordemos que la administración titular debe responder de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de la misma, y consecuencia de ello, surge la posibilidad de exigencia de responsabilidad patrimonial de la administración, en el caso de que la información facilitada desde la sede pueda originar un daño o incluso por su funcionamiento anormal*», *Vid.* FONDEVILA ANTOLÍN, J., «Capítulo III. La Administración electrónica en la Ley 40/2015, de Régimen Jurídico del Sector Público», PINTOS SANTIAGO, J. (Dir.), *La implantación de la administración electrónica y de la e-factura,* Wolters Kluwer, Madrid, 2017, p. 160.

constantemente actualizado e intuitivo para los ciudadanos donde se publique la información relativa al tratamiento de los datos como parte de la transparencia activa.

Como consecuencia de esta obligación, se ha introducido el art. 6 bis en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[653]. Esta inclusión visibiliza otra herramienta que resalta, por una parte, la importancia del tratamiento de datos de carácter personal y por otra, el acto de publicidad activa llevado a cabo por las AA.PP. con el cual se pretende dar a conocer a los ciudadanos que es llevada a cabo esa actividad y cómo. Todo lo anterior posibilita el escrutinio público de las obligaciones que deben cumplir las AA.PP. en la materia y mejora a su vez el ejercicio de derechos de los ciudadanos en materia de protección de datos, en relación con la información que tienen en su poder las AA.PP.

1.3 Efectos del incumplimiento de la normativa en materia de protección de datos: las sanciones administrativas al sector público y su responsabilidad patrimonial.

Como se adelantó anteriormente[654], el RGPD y la LOPDGDD estructuran un marco de infracciones y sanciones alrededor del incumplimiento de la normativa de protección de datos. Sin embargo, existen algunas peculiaridades dependiendo del sujeto que infrinja este marco jurídico[655].

El art. 83.7 del RGPD determina que deberán ser los Estados miembros los que establezcan en sus normas la posibilidad de imponer multas de carácter administrativo a Autoridades y organismos públicos establecidos en su territorio y en qué medida, en este sentido «*se mantiene así el régimen jurídico de responsabilidad por vulneración de la normativa de protección de datos, por parte de las Administraciones Públicas, cuyo comportamiento puede ser sancionado, al margen*

[653] Por la D.F. 11ª de la LOPDGDD.
[654] *Vid.* El epígrafe 1.1. Autoridades de control en España del Capítulo III.
[655] En la derogada LO 15/1999, de 15 de diciembre, las infracciones eran también se graduaban en leves, graves y muy graves en su artículo 44.

de poder exigir la responsabilidad disciplinaria de las autoridades, a las que a título individual pudiera imputárseles la comisión de la infracción»[656].

En la LOPDGDD el legislador ha optado como venía haciendo desde la LORTAD por la adopción de medidas para hacer cesar conducta o corregir los efectos de la infracción[657] y por sanciones al estilo del «apercibimiento» a las Autoridades públicas enumeradas en el art. 77.1 de la Ley, por las infracciones cometidas en los arts. 72 al 74 de la misma. Como bien ha señalado el Profesor HUERGO LORA «*el mecanismo de sanciones contra las Administraciones públicas no cumple la función de una sanción porque no sirve para imponer sanciones sino para establecer, en el mejor de los casos, las medidas que deben adoptarse para ajustar la actuación administrativa a la legalidad*»[658]. En relación con lo anterior, la Profesora MARZAL RAGA determina que este tipo de sistema en cierta manera «*alienta una cierta impunidad en la actuación de la Administración pública, que goza de una posición privilegiada injustificada en este punto de acuerdo con los fines reconocidos en el artículo 103 CE, que puede verse además agravada con una actuación continuada consistente en reiterados procedimientos de incumplimiento por un mismo ilícito, sin ninguna consecuencia jurídica más allá de la mera comunicación del incumplimiento al Defensor del Pueblo*»[659]. Sin lugar a duda, este tipo de sanciones de índole no económica están dirigidas a las Administraciones públicas que no cumplan con sus obligaciones respecto a la normativa vigente en la materia en una posición totalmente antagónica a la de los responsables de ficheros «particulares», quienes deberán de soportar sobre sí mismos todo el peso de la Ley, sobre todo, en relación con las consecuencias de la no observancia de la nueva normativa. Esta desigualdad, justificada en razones presupuestarias, no deja de suponer un perjuicio para los particulares, que se enfrentan a sanciones económicas, frente a las meramente

[656] TERRÓN SANTOS, D. y DOMÍNGUEZ ÁLVAREZ, J.L, *op. cit.,* 171.
[657] La LORTAD regulaba en su art. 45 hablaba de medidas a adoptar para cesar o corregir los efectos de la infracción si los responsables fuesen Administraciones públicas, en su caso propondrían la iniciación de un procedimiento de carácter disciplinario y se daría cuenta de ellos al Defensor de Pueblo. En la LOPD 15/1999, de 13 de diciembre, este tipo de sanciones estaban previstas en su art. 46, en iguales condiciones que la LORTAD.
[658] HUERGO LORA, A., «Peculiaridades de la potestad sancionadora en materia de protección de datos», *La potestad sancionadora de la Agencia Española de Protección de Datos*. Thomson Aranzadi-AEPD, Navarra, 2008, p. 152.
[659] MARZAL RAGA, R., *El apercibimiento: una nueva sanción en materia de protección de datos.* (en línea), Tirant lo Blanch, 2015, pp. 61 (consulta: 12 de octubre de 2020).

declarativas que se efectúan a las AAPP[660]. En este sentido la Profesora BOTO ÁLVAREZ se ha pronunciado al respecto determinando que «*La doctrina ha justificado esta exclusión con base en el trasvase de fondos y la repercusión última en el contribuyente, aunque la configuración orgánica independiente de la Agencia permitiría justificar otras soluciones técnicas que quizás haya llegado el momento de plantearse*»[661].

La resolución de apercibimiento de acuerdo con el apartado segundo del art. 77 de la LOPDGDD irá acompañado de las medidas que la AEPD estime necesarias para hacer cesar la conducta o corregir los efectos de la infracción. Como novedad se incluyen otras dos medidas dirigidas a las AA.PP. infractoras. La primera de ellas es la propuesta realizada por la AEPD para el inicio de un procedimiento de carácter disciplinario si existiesen motivos suficientes. La segunda de las medidas está relacionada con la falta de observancia de informes técnicos o recomendaciones que no hubieran sido atendidos por la autoridad infractora, en este caso se incluirá con la resolución de apercibimiento «*una amonestación con denominación del cargo*

[660] Igualmente, FERNÁNDEZ SALMERÓN, M. y VALERO TORRIJOS, J. entienden que (el entonces vigente) art. 46 de la LOPD 15/1999, de 13 de diciembre preveía «*una reacción sólo equivalente al ejercicio de una verdadera potestad punitiva, que culmina con la que ha terminado por denominarse "declaración de infracción", adquiriendo dicha expresión carta de naturaleza normativa*». Por lo que concierne a los motivos que han motivado en la antigua LOPD y se haya extrapolado al contenido de la nueva LOPDGDD, de acuerdo con estos dos autores atiende al "trasiego de fondos públicos", sin embargo, este motivo podría ser impugnable de acuerdo con estos autores, ya que el sistema permite a todas las Administraciones publicas alimentarse «*en mayor o menor medida de los recursos del Estado*», dando como solución con determinados matices, que reforzara el cumplimiento normativo sería la proyección de esa responsabilidad «soportada por el sujeto público en los autores personales de la infracción, siempre que hubiera actuado con dolo o culpa», aunque bien apuntan por la cuantía de las multas, la acción de regreso sería excesiva y «escasamente operativo», Cfr. FERNÁNDEZ SALMERÓN, M. y VALERO TORRIJOS, J. «Las infracciones de las Administraciones Públicas», TRONCOSO REIGADA, A. (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal,* Civitas-Thomson Reuters, Navarra, 2010, pp. 2188-2194. Hasta ahora se han emitido para el año de 2018: 7 resoluciones de la AEPD, seis de ellas apercibiendo a distintas AA.PP. (PS: 00361/2018, 00365/2018, 00374/2018, 00393/2018, 00406/2018, 00410/2018) y una declarando la no existencia de responsabilidad (PS/00430/2018); para el año 2019 han sido emitidas diecisiete resoluciones de las cuales dieciséis aperciben a distintas AA.PP. (PS: 00009/2019, 00012/2019, 00066/2019, 00106/2019, 00171/2019, 00201/2019, 00222/2019, 00241/2019, 00252/2019, 00318/2019, 00347/2019, 00363/2019, 00376/2019, 00380/2019, 00381/2019, 00382/2019) y 1 de archivo del procedimiento(PS/00073/2019); solo se ha apercibido hasta septiembre de 2020 a una Administración pública (PS/00001/2020).

[661] BOTO ÁLVAREZ, A., «Capítulo 19. La determinación administrativa de derechos fundamentales: Autoridades independientes y órganos de resolución de recursos especiales», PUNSET BLANCO, L. y ÁLVAREZ ÁLVAREZ, L. (Coords.), *Cuatro décadas de una constitución normativa (1978-2018). Estudios sobre el desarrollo de la Constitución Española,* Thomson Reuters- Civitas y Universidad de Oviedo, Navarra, 2018, p. 482. En este mismo sentido *vid.* GUICHOT REINA, E., «La potestad sancionadora en materia de protección de datos: aproximación general», *La potestad sancionadora de la Agencia Española de Protección de Datos*, Thomson Reuters Aranzadi, Navarra, 2008, p. 71.

responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda»[662]. En cualquier caso, cuando las AA.PP. sean sancionadas, la AEPD deberá comunicárselo al Defensor del Pueblo de manera preceptiva[663].

Visto el tema de la sanción, es necesario hablar de la reparación del daño. Se debe partir del hecho de que a la autoridad de control de carácter estatal competente para ejercer la potestad sancionadora [664], es decir, la AEPD tiene entre sus competencias la de vigilar el correcto cumplimiento de la normativa que vendría siendo una actividad de policía y otra de tutela de derechos, pues es la encargada de tramitar las solicitudes a este respecto realizadas por los ciudadanos[665].

Sin embargo, no se le ha atribuido legalmente la competencia en la normativa específica aplicable de determinar las indemnizaciones derivadas por el incumplimiento de la normativa de protección de datos, ni por lo dispuesto en el RGPD o ni en la LOPDGDD, por tanto, los ciudadanos deberán acudir a la vía de responsabilidad patrimonial de las Administraciones públicas[666]. Esta cuestión ya ha sido abordada por la jurisprudencia, la cual ha establecido que «*la Agencia Española de Protección de datos puede imponer una sanción a los responsables o encargados del tratamiento y el afectado obtener no obstante una indemnización en vía judicial o administrativa a través de un procedimiento diferenciado del que se ha seguido ante la propia Agencia*»[667], lo cual excluiría a la AEPD de la aplicación del art. 28.2 de la LRJSP y obligaría a los interesados a iniciar un procedimiento de responsabilidad administrativa por los cauces administrativos y si estos no son

[662] Art. 77.3 de la LOPDGDD. En este mismo sentido Cfr. VALERO TORRIJOS, J., «Protección de datos…» *op. cit.*, p. 437.
[663] Art. 77.5 de la LOPDGDD.
[664] Sin perjuicio de las competencias de las Autoridades de control autonómicas.
[665] En este mismo sentido el F.D. 8º de la SAN (Sala de lo Contencioso-Administrativo, Sección 1ª) de 1 de octubre de 2008 (RJCA\2009\310; ECLI: ES:AN:2008:5744).
[666] Tal y como se establecía en el art. 19.2 de la LOPD 15/1999, de 13 de diciembre. Que conforme con la propia AEPD «*en la reclamación del derecho a la indemnización no interviene la Agencia Española de Protección de Datos por lo que el ciudadano afectado deberá, en su caso, acudir a la jurisdicción que corresponda en función de la indemnización se reclama ante el responsable de un fichero de titularidad pública o ante el responsable de un fichero de titularidad privada*», Cfr. F.D. IV del Recurso de Reposición N.º RR/00606/2016 (Procedimiento nº.: A/00118/2016) de la AEPD.
[667] F.D. 6º de la SAN (Sala de lo Contencioso-Administrativo, Sección 1ª) de 1 de octubre de 2008 (RJCA\2009\310; ECLI:ES:AN:2008:5744).

atendidos por vía jurisdiccional [668]. Es decir, se deberán de seguir dos procedimientos diferentes, uno para reclamar el cumplimiento de las obligaciones de protección de datos y otro para exigir la indemnización correspondiente a los años que el incumplimiento ha causado.

1.4 El ciclo de vida del tratamiento de los datos personales en la Administración electrónica.

El hecho de que se hayan implementado nuevas tecnologías en las Administraciones territoriales y en el sector público no parece haber dejado indiferentes a muchos. Este ciclo de acuerdo con lo establecido en la AEPD tiene varias etapas: 1) captura de los datos, «*proceso de obtención de datos para su almacenamiento y posterior procesado*» [669]; 2) clasificación/ almacenamiento; 3) uso/tratamiento; 4) cesión o transferencia de los datos a un tercero para su tratamiento y, 5) destrucción [670].

Antes de comenzar un análisis desde la perspectiva en materia de protección de datos, específicamente, en relación el ciclo de vida de los datos personales [671], primero parece pertinente contextualizar el actual panorama de la llamada «administración electrónica». Es preciso indicar que esta parte del estudio no

[668] En vía administrativa por medio de una solicitud basada en el art. 67 de la LPAC y en vía jurisdiccional ante la jurisdicción contencioso-administrativa de acuerdo con el art. 9.4 de la LOPJ, por medio de un procedimiento ordinario o uno de protección de los derechos fundamentales de la persona, o incluso de manera simultánea (F.J.2 de la TC (Sala Primera) núm. 98/1989 de 1 junio. RTC 1989\98; ECLI:ES:TC: 1989:98) de acuerdo con la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa. De acuerdo con TERRÓN SANTOS Y DOMÍNGUEZ ÁLVAREZ «*si la indemnización se pretende respecto a ficheros de titularidad pública, el marco de actuación será en el integrante del concepto de funcionamiento anormal de los servicios públicos y para tramitación se debe atender a la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas*», Cfr. TERRÓN SANTOS, D. y DOMÍNGUEZ ÁLVAREZ, J.L, *op. cit.,* p. 178. Al hilo de lo anterior, la Profesora BOTO ÁLVAREZ se pronunció al respecto en este sentido estableciendo que con la normativa anterior la posibilidad general de determinar en el acto administrativo sancionador la responsabilidad civil derivada de la infracción no era operativa en materia de protección de datos personales, ya que de acuerdo con el antiguo art. 19 de la LO 15/1999 esta previsión se remitía a « *la acción de responsabilidad a la jurisdicción ordinaria en el caso de ficheros de titularidad privada y al sistema de responsabilidad patrimonial de las Administraciones públicas cuando el fichero sea de titularidad pública*», cfr. BOTO ÁLVAREZ, A., *op. cit.*, p. 481.

[669] AEPD, «*Guía Práctica de análisis de riesgos…*», *op. cit.,* p. 25.

[670] *Íd.*

[671] Esta expresión ha sido sacada de la «*Guía Práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*» de la AEPD en el cual se refiere a todas las etapas del tratamiento de datos: «*captura de datos, clasificación/almacenamiento, uso/tratamiento, cesión o transferencia de los datos a un tercero para su tratamiento y destrucción*», p. 25.

pretende ser ni mucho menos un estudio exhaustivo de todos los cambios tecnológicos implementados hasta la ahora, ni tampoco analizar todos los efectos que ha tenido procesalmente hablando la implementación de estas tecnologías en el procedimiento administrativo, lo que se hará es proceder al análisis de determinados aspectos de las leyes 39 y 40/2015 que considero tienen una mayor importancia desde la perspectiva de protección de datos y su nueva regulación.

De acuerdo con lo establecido por la Comisión Europea, debe entenderse como «administración electrónica» al «*uso de las tecnologías de la información y las comunicaciones en las administraciones públicas, combinado con cambios organizativos y nuevas aptitudes, con el fin de mejorar los servicios públicos y los procesos democráticos y reforzar el apoyo a las políticas públicas»*[672]. El Profesor BALLESTEROS MOFFA por su parte determina que «*La Administración electrónica se traduce en trámites y actos de formato electrónico, de uso generalizado en todas las fases de iniciación, ordenación, instrucción y finalización, en torno al concepto de expediente administrativo común electrónico (art. 70 LPAC) y notificación electrónica. Al que se suma ahora el concepto más avanzado e incipiente de Administración inteligente, que redimensionará el principio de buen gobierno en cambios estructurales*»[673]A propósito de la administración electrónica entonces se derivan diversas cuestiones nada baladís.

En principio queda claro el carácter instrumental del uso de tecnologías de la información y comunicación. La implementación de estas últimas en las AA.PP. pretende contribuir al cumplimiento de los intereses generales de forma eficaz y compatible con lo establecido en el art. 103 de la CE[674]. Ahora bien, su puesta en marcha supone un cambio *ad intra* de las mismas, sobre en su organización, en la disponibilidad de medios, en la gestión administrativa, en las nuevas aptitudes que deberán tener sus empleados públicos e incluso tendría reflejo en sus relaciones con otras administraciones. En este sentido el Profesor MARTÍN DELGADO establece que:

---

[672] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. *El papel de la administración electrónica en el futuro de Europa,* COM (2003) 567 final, p. 7.

[673] BALLESTEROS MOFFA, L. Á., *op. cit.,* p. 35.

[674] No debemos olvidar que el principio de eficacia tiene gran envergadura en cuanto a que las AA.PP. tendrán que realizar cuanto estime necesario para la materialización y el cumplimiento de sus finalidades.

«*Las TIC no son un fin en sí mismo, sino una herramienta imprescindible para la innovación del interior de la Administración y para la eficacia en la prestación de servicios a los ciudadanos*»[675]. Sin duda estas medidas pueden ser proyectadas *ad extra* en determinadas situaciones, entre las que quizás tiene una mayor trascendencia el ejercicio de derechos por parte de los ciudadanos. Derechos que no tendrán afectación directa, pues su sustancia no se vería afectada, como bien apunta el Profesor GAMERO CASADO «*lo electrónico siempre es relativo a las formas, nunca la sustancia, aunque su aplicación a la Administración traiga consigo algunas transformaciones importantes. Por eso, los derechos del ciudadano ante la Administración electrónica seguir haciendo derechos, nuevos o viejos, más o menos ampliados, pero derechos al fin y al cabo, entendidos como situaciones de poder frente a la Administración que facultan aquél para exigir de ésta una actuación legalmente prevista y que constituyen medidas de garantía de su posición jurídica. En definitiva, considero más conveniente hablar de derechos del ciudadano ante la administración electrónica o derechos del ciudadano administrado electrónicamente; de ahí el título de este trabajo*»[676]. Por tanto, no solo hablamos de derechos también podríamos hablar de intereses generales o de servicio público, dónde lo importante reside en la sustancia no en la forma.

1.4.1 Evolución normativa.

En la derogada ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo común, en su art. 45 ya se contemplaba la incorporación de medios electrónicos en las AA.PP. que ayudasen a llevar a cabo su actividad y el ejercicio de sus competencias. Este mismo artículo dejaba abierta la posibilidad a los ciudadanos de comunicarse por estos medios con las AA.PP. siempre que fuese compatible con los medios técnicos de estas últimas.

---

675 MARTÍN DELGADO, I., «El acceso electrónico a los servicios públicos: hacia un modelo de administración digital auténticamente innovador», QUADRA-SALCEDO, T. DE LA y PIÑAR MAÑAS, J. L. (Dir.). *Sociedad digital y Derecho*. BOE, Madrid, 2018, p. 183. En este mismo sentido MENÉNDEZ SEBASTIÁN, E. Mª, *Las garantías del interesado en el procedimiento administrativo electrónico. Luces y sobras de las nuevas leyes 39 y 40/2015.* Tirant lo Blanch, Valencia, 2017, p. 16-18.

676 GAMERO CASADO, E., «Objeto y ámbito de aplicación de la ley 11/2007», MURILLO DE LA CUEVA, P.L. (Dir.), *La protección de datos en la administración electrónica,* Aranzadi, Navarra, 2009, pp. 149-150.

Años más tarde se aprobó la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), la cual tenía carácter básico y a su vez regulaba parte del procedimiento administrativo. Esta ley supuso un claro avance en relación con el contenido del art. 45 de la LRJPAC, el cual no establecía las garantías técnicas ni organizativas de esos medios electrónicos ni como se tendría que llevar a cabo la comunicación. Otra cuestión destacable de esta ley referente a los derechos de los ciudadanos lo encontramos en el contenido de su art. 6, este reconocía de manera expresa como un derecho subjetivo de los ciudadanos a relacionarse con las Administraciones públicas a través de medios electrónicos, es decir, se positiviza «*por primera vez nuestro ordenamiento jurídico interno de forma clara y universal, el derecho de los ciudadanos a relacionarse con todas las Administraciones de manera electrónica*» [677]. Otro de los avances que supuso esta Ley pero que estudiaremos más tarde es la implementación tanto del Esquema Nacional de interoperabilidad, como el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

Actualmente la administración electrónica está regulada por las leyes 39 y 40/2015, tanto las medidas técnicas y organizativas que deben adoptar las AA.PP. *ad intra* como aspectos procesales con efectos *ad extra,* especialmente en su relación con los ciudadanos. Se ha considerado casi de manera unánime para la doctrina que el contenido de la Ley 39/2015 supone un retroceso en relación con la LAECSP [678],

[677] TERRÓN SANTOS, D. y DOMÍNGUEZ ÁLVAREZ, J.L., *op. cit.*, p. 185. Este apartado también enlistaba una serie de acciones que podía realizar por ese mismo canal de comunicación, como: obtener informaciones, realizar consultas, alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones, y oponerse a las resoluciones a actos administrativos. El apartado segundo de este mismo artículo enumeraba también otros derechos relacionados con la utilización de los medios electrónicos en la actividad administrativa y su apartado tres hacía referencia a la tramitación a través de ventanilla única, por vía electrónica en los procedimientos de relativos al acceso a una actividad de servicios y su ejercicio, así como la información que las AA.PP. debían proporcionar en relación con lo anterior a los ciudadanos a través de medios electrónicos.

[678] En ese sentido MARTÍN DELGADO determina en relación con el derecho a comunicarse con las Administraciones públicas a través de un Punto de Acceso General electrónico contenido en el art. 13.a) de la LPAC que: «*resulta evidente que la ausencia del reconocimiento de un derecho general a relacionarse con la Administración por medios electrónicos con sustantividad propia y no meramente instrumental hace perder fuerza a la posición del ciudadano ante la Administración*», Cfr. MARTÍN DELGADO, I., *op. cit.,* p. 194. En el mismo sentido, Cfr. VALERO TORRIJOS, J., «Implicaciones de la protección de datos de carácter personal para la Administración electrónica», QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, T. DE LA y PIÑAR MAÑAS, J. L. (Dirs.). *Sociedad Digital y Derecho*. BOE, Madrid, 2018.; CAMPOS

en relación los derechos de los ciudadanos, así como respecto a los efectos que pueden desplegar estas nuevas tecnologías en los mismos. Esto último se da de forma especial, respecto a los registros electrónicos y las notificaciones efectuadas por este medio[679]. El Profesor MARTÍN DELGADO deja de manifiesto que para poder ser efectivo el derecho que tienen los ciudadanos a relacionarse con la Administración esta tiene que realizar una transformación al interior de su organización, en las aptitudes de su personal e integrarlo en el procedimiento. Es importante mencionar que este autor considera que las TIC no son un fin en sí mismo, que estas pueden ayudar a quitarle rigidez a la relación entre administración y ciudadano en cuanto al acceso a determinados trámites[680]. En este mismo sentido el Profesor GAMERO CASADO determina que este fenómeno se proyecta «*sobre el ámbito interno o doméstico de cada organización pública promoviendo un cambio en la gestión administrativa, así como sobre las relaciones interadministrativas agilizando los procesos multifásico y el intercambio de información*»[681].

1.4.2 Presupuestos para el funcionamiento de la Administración electrónica.

En este epígrafe se tratarán dos presupuestos que consideramos tienen un papel angular en la administración electrónica, con efectos *ad intra:* la interoperabilidad y la seguridad. El contenido del apartado 2 del art. 3 de la LRJSP establece que las AA.PP. deberán relacionarse electrónicamente con otras Administraciones y en sus relaciones internas con sus organismos, órganos y entes. La utilización de unos medios electrónicos u otros depende en buena parte de su

---

ACUÑA, C., «El procedimiento administrativo electrónico en la Ley 39/2015», PINTOS SANTIAGO, J. (Dir.). *La implantación de la administración electrónica y de la e-factura*. Wolters Kluwer, Madrid, 2017, entre otros.

679 Para un estudio en más profundad sobre este tema *vid.* MENÉNDEZ SEBASTIÁN, E. Mª. *op. cit.*

680 En su trabajo «El acceso electrónico a los servicios públicos: hacia un nuevo modelo de administración digital auténticamente innovador». Además, establece que la Administración en sus tres niveles debe buscar soluciones comunes que permitan la interoperabilidad entre ellas desde la colaboración. Sin olvidar que aun cuando el procedimiento eche mano de las TIC las garantías procedimentales deben ser de observancia obligatoria para las AAPP, situando los ciudadanos en el centro de esa relación, procurando entre otras cosas no trasladarles cargas derivadas de la implementación de las TIC en el procedimiento. El autor finalmente de manera más que atinada recuerda que no es lo mismo modernizar la administración que innovarla, literalmente determina que «*Incorporar las tecnologías en los procesos de actuación y en la estructura organizativa es simplemente modernizar; aprovechar esas mismas tecnologías para cambiar procesos y estructuras, explorando y explotando todas las posibilidades que conllevan y adaptándolas a las necesidades de los ciudadanos es innovar*», *vid.* MARTÍN DELGADO, I., *op. cit.,* p. 200.

681 *Vid.* GAMERO CASADO, E., «Objeto y ámbito…», *op. cit.,* pp. 109-110.

interoperabilidad y de su seguridad que garanticen la protección de datos a los interesados y que a su vez de manera preferente faciliten la prestación conjunta de servicios a estos. Según prevé el art. 156.2 de la LRJSP, los criterios de interoperabilidad deben ser tenidos en cuenta por las AA.PP. para tomar decisiones en materia de tecnologías para que a su vez no coarten relaciones interadministrativas.

La interoperabilidad de acuerdo con la doctrina supone uno de los principales desafíos de la gestión administrativa[682] y a su vez, supone el motor de la Administración electrónica[683]. Que ahora más que nunca no solo tiene efectos *ad intra* y como bien apunta el Profesor FONDEVILA ANTOLÍN «*la interoperabilidad extiende su ámbito de aplicación tanto a la esfera o dimensión ad extra, regulada en la LPACAP con múltiples referencias a la interoperabilidad, como en la esfera o vertiente ad intra, como demuestran las innumerables referencias a su garantía y aseguramiento en la LRJSP*»[684]. Además, no debemos perder de vista la importancia que supone para la reutilización de la información del sector público[685].

Pero ¿qué es la interoperabilidad? De acuerdo con el apartado I del Preámbulo del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica (ENI), «*es la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos. Resulta necesaria para la cooperación, el desarrollo, la*

---

[682] El Profesor GAMERO CASADO determina que la interoperabilidad es: el desafío más grande que se plantea a la gestión administrativa en la primera mitad del siglo XXI, Cfr. GAMERO CASADO, E., «Interoperabilidad y Administración electrónica: conéctese, por favor», *Revista de Administración pública.* Núm., 179, Madrid, 2009, p. 294; Cfr. FONDEVILA ANTOLÍN, J., «Capítulo III. La Administración electrónica en la Ley 40/2015, de Régimen Jurídico del Sector Público», PINTOS SANTIAGO, J. (Dir.), *La implantación de la administración electrónica y de la e-factura¸* Wolters Kluwer, Madrid, 2017, pp. 223-224. En este sentido la Comisión Europea también se ha pronunciado estableciendo que «*La interoperabilidad es un elemento esencial para hacer posible una transformación digital*», Cfr. Comisión Europea, Marco Europeo de Interoperabilidad, COM (2017) 134 final, p. 2. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:134:FIN (consulta: 8 de enero de 2021).

[683] CERRILLO I MARTÍNEZ, A., «Cooperación entre Administraciones públicas para el impulso de la administración electrónica», GAMERO CASADO, E. y VALERO TORRIJOS, J. (Coords.), *La Ley de administración electrónica. Comentario sistemático a la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos*. Thomson-Aranzadi, Navarra, 2008, p. 497.

[684] FONDEVILA ANTOLÍN, J., *op. cit.,* pp. 223-224.

[685] *Vid.* Comisión Europea, Marco Europeo de Interoperabilidad, *op. cit.*

integración y la prestación de servicios conjuntos por las Administraciones públicas; para la ejecución de las diversas políticas públicas; para la realización de diferentes principios y derechos; para la transferencia de tecnología y la reutilización de aplicaciones en beneficio de una mejor eficiencia; para la cooperación entre diferentes aplicaciones que habiliten nuevos servicios; todo ello facilitando el desarrollo de la administración electrónica y de la sociedad de la información». Dicho de otra manera, es la capacidad de los sistemas electrónicos de comunicarse entre sí permitiendo el envío y recepción de información, así como su utilización[686]. Como bien señala el Profesor GAMERO CASADO «*expresado en términos más familiares, y salvando las distancias, la interoperabilidad podría equipararse a un proceso de normalización que permite a un programa o sistema informático compartir la información con otros programas y sistemas y establecer comunicaciones con ellos*»[687]. Por su parte el Profesor FONDEVILA ANTOLÍN determina que «*Asegurar la interoperabilidad y conectividad de los sistemas y plataformas tecnológicas es una obligación para las administraciones que se materializa en la exigibilidad y el carácter básico del ENI*»[688].Este sistema que menciona está basado en normas generalmente técnicas, pero también organizativas contenidas en el ENI, así como en las resoluciones que lo desarrollan sobre determinados aspectos, soportes e informaciones[689]. En

[686] Otros autores nos ofrecen otras definiciones más exactas y compresibles, por ejemplo, para los Profesores TERRÓN SANTOS y DOMÍNGUEZ ÁLVAREZ la interoperabilidad «*Hace posible que los datos situados en un punto del sistema (por ejemplo, los que contengan un expediente administrativo) puedan ser utilizados de manera electrónica por el conjunto de dicho sistema (por ejemplo, todos los órganos de una misma Administración) y cruzarse así mismo por medios electrónicos para su uso por los interesados y por otras entidades públicas y privadas*», en TERRÓN SANTOS, D. y DOMÍNGUEZ ÁLVAREZ, J.L. *op. cit.,* p. 204.

[687] GAMERO CASADO, E. «Interoperabilidad…» *op. cit.,* p. 292.

[688] FONDEVILA ANTOLÍN, J., *op. cit.,* p. 225.

[689] En un esfuerzo de transparencia activa en el Portal de la administración electrónica están publicadas las normas técnicas de interoperabilidad que desarrollan el ENI, en la actualidad existen normas técnicas para los catálogos de estándares, los documentos electrónicos, aplicables a la digitalización de documentos, al expediente electrónico, sobre la política de firma y de certificados de la Administración, sobre los protocolos de intermediación, sobre la relación de modelos de datos, la política de gestión, etc. Los cuales están disponibles en: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html#CATALOGOESTANDARES (consulta: 29 de septiembre de 2020). En relación con las normas técnicas del ENI es necesario precisar que fueron emitidas por la Secretaría de Estado de Administraciones Públicas (normas técnicas de interoperabilidad: Política de Firma y Sello Electrónicos y de Certificados de la Administración, Protocolos de intermediación de datos, relación de modelos de datos, gestión de documentos electrónicos y reutilización de recursos de la información) y por la Secretaría de Estado para la Función Pública (normas técnicas de interoperabilidad: documento electrónico, digitalización de

relación con lo anterior, el Profesor MARTÍNEZ GUTIÉRREZ establece que las normas técnicas de interoperabilidad además de ser de obligado cumplimiento se aprueban «*sin contar en muchas ocasiones con unos cauces adecuados de colaboración y cooperación interadministrativas para consensuar este mínimo común denominador necesario*»[690].

Otro de los requisitos que deben cumplir las AA.PP. en relación con los sistemas de gestión de información e incluso en el tratamiento de datos de carácter personal, es la seguridad. Estas medidas en materia de seguridad están contempladas en el Esquema Nacional de Seguridad; el cual tiene por objeto de acuerdo con apartado 2 del art. 156 de la LRJSP «*establecer la política de seguridad en la utilización de medios electrónicos*» utilizados por las AA.PP. y por el sector público[691]. Está constituido por principios básicos y requisitos mínimos que están contenidos en Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica[692]. Para determinar las medidas de seguridad que deben implementarse en cada Administración en el marco organizativo[693], operacional[694] y las medidas de

documentos, expediente electrónico, de requisitos de conexión a la red de comunicaciones de las Administraciones públicas españolas, de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, de Modelo de Datos para el Intercambio de asientos entre las entidades registrales) para desarrollar algunos aspectos del ENI, estas son de obligado cumplimiento para todas las AAPP de acuerdo con la D.A. Primera del RD 4/2010, de 8 de enero.

[690] Además, estas son «*normas reglamentarias de tercer o cuarto nivel, situación que no parece la más adecuada para la seguridad jurídica ni tampoco como instrumento normativo que debiera ser el producto del principio de colaboración y cooperación*», Cfr. MARTÍNEZ GUTIÉRREZ, R., «El régimen jurídico de la Administración digital: aspectos procedimentales», MARTÍN DELGADO, I. (Dir.), *El procedimiento administrativo y el régimen jurídico de la Administración pública desde la perspectiva de la innovación*, Iustel, Madrid, 2020, pp. 163-164.

[691] De acuerdo con el Profesor ALAMILLO DOMINGO quienes también están obligados a cumplir con el ENS de forma indirecta son los contratistas que presten servicios de tecnologías de la información y la comunicación «*aunque estas entidades no se encuentren formalmente sujetas a la norma, sus servicios deben permitir a la Administración contratante el cumplimiento del RDENS, por lo que lógicamente deberían trasladar el contenido de las correspondientes obligaciones legales al contrato en forma de prescripciones técnicas reglamentarias, incluida cualquier obligación de certificación técnica exigible a la propia Administración*», Cfr. ALAMILLO DOMINGO, I., «Capítulo 16. Esquema Nacional de Seguridad: La administración electrónica y la seguridad de la información», CAMPOS ACUÑA, C. (Dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, Segunda edición, Wolters Kluwer, 2019, p. 614.

[692] El ENI y el ENS fueron implementados por la hoy derogada LAECSP, específicamente por el contenido de su art. 42.

[693] El marco organizativo está comprendido de «*medidas relacionadas con la organización global de la seguridad*», Cfr. Anexo II, Sección 1, apartado 2, inciso a).

[694] Está formado por: «*las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin*», Cfr. Anexo II, Sección 1, apartado 2, inciso b).

protección [695], deben identificarse el tipo de archivos con los que cuente, y determinar conforme al Anexo I: las dimensiones de seguridad relevantes, el nivel de cada dimensión de seguridad y la categoría del sistema, que servirán como base para seleccionar y determinar las medidas que resulten apropiadas para su implementación en las AA.PP. Para hacer más fácil esta labor y entendimiento de la normativa, el anexo II del referido esquema detalla la correspondencia entre los niveles de seguridad en una tabla como guía para las AA.PP.

Resulta también de especial importancia en el entono tecnológico, especialmente si las AA.PP. utilizan la web como canal de comunicación con el ciudadano, la neutralidad de la red. De acuerdo con lo establecido por la Profesora FUERTES LÓPEZ es «*el presupuesto del adecuado ejercicio de los derechos de los ciudadanos*» [696]. La neutralidad en la red existe cuando no se da preferencia ni bloqueo de contenidos «*aplicaciones o servicios que circulan por la red, y donde los mismos, ya sean ofertados por prestadores de servicios o volcados por meros particulares, no requieren de una previa remuneración al operador de telecomunicaciones, propietario de las redes por las cuales circulan aquellos*»[697] que devengan lícitos.

Otra cuestión que tiene que ver con el diseño de los medios que utilizan las AA.PP. como los portales, sedes electrónicas, incluso los registros, es su accesibilidad, estos tienen que estar diseñados de manera que los ciudadanos puedan cumplir obligaciones y ejercer sus derechos. La Ley 10/2014, de 3 de diciembre, de accesibilidad, determina criterios encaminados a garantizar el acceso a las personas con discapacidad en condiciones de igualdad de oportunidades «*en relación con la accesibilidad universal y el diseño para todos respecto a los entornos, procesos, bienes, productos y servicios, así como en relación con los objetos o instrumentos, herramientas y dispositivos, de modo que los mismos se hagan*

[695] Centradas en «*proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas*», Cfr. Anexo II, Sección 1, apartado 2, inciso c).
[696] *Vid.* FUERTES, M., «Defensa de Derechos y neutralidad de la red», QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO T. DE LA y PIÑAR MAÑAS, J. L. (Dirs.), *Sociedad Digital y Derecho*, BOE, Madrid, 2018, p. 242.
[697] ARJONEZ GIRÁLDEZ, D., «La neutralidad de la red desde su arquitectura por capas ¿de transportistas públicos a gestores de contenidos?», CERRILLO I MARTÍNEZ, A., *et al.* (Coords.), *Neutralidad de la red y otros retos para el futuro de internet. Actas del VII Congreso Internacional internet, derecho y política. Universitat oberta de Catalunya*, España, 2011, p. 54.

comprensibles, utilizables y practicables por todas las personas, en igualdad de condiciones de seguridad y comodidad y de la manera más autónoma y natural posible»[698]. Sin embargo, recientemente en el año 2016 se aprueba la Directiva 2016/2102 del Parlamento Europeo y del Consejo, de 26 de octubre de 2016, sobre la accesibilidad de los sitios web y aplicaciones para dispositivos móviles de los organismos del sector público, en la cual se pormenorizan aquellos elementos que deben tomarse en cuenta a la hora de diseñar sitios web y aplicaciones de titularidad pública, con especial atención a las necesidades de las personas con algún tipo de discapacidad. En este contexto, se ha transpuesto el contenido de la Directiva 2016/2102 al ordenamiento jurídico español por medio del Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.

Como se refirió anteriormente, en esta parte del trabajo se analizará el ciclo de vida de los datos personales en la Administración electrónica, utilizando tanto el RGPD y la LOPDGDD en lo referente a la materia de protección de datos y principalmente, las Leyes 39 y 40/2015 en relación con las medidas tecnológicas, técnicas, organizativas y funcionales implementadas como consecuencia de la administración electrónica y que bajo nuestra consideración pueden tener mayor incidencia e importancia en el tratamiento de datos según la etapa. El ciclo de vida del tratamiento de datos al que hacemos referencia comienza con la recogida de los datos personales, posteriormente se almacenan en un soporte que pueda permitir su tratamiento, ya en el soporte se pueden usar los datos para las finalidades por las cuales fueron recogidos ahora bien durante ese tratamiento de datos puede que se realicen comunicaciones de datos de carácter personal a otras AA.PP. y, finalmente, su ciclo de vida termina con la destrucción de los datos personales, lo anterior desde la óptica del nuevo marco jurídico en materia de protección de datos personales.

1.4.3 Recogida de datos.

De acuerdo con el Profesor RAZQUIN LIZARRAGA el tratamiento de datos «*comienza desde el momento de presentación de una solicitud (o cualquier otro*

[698] Cfr. Art. 1 de la Ley 10/2014, de 3 de diciembre, de accesibilidad.

documento) en el Registro Electrónico General de cada Administración Pública»[699]. De este acto realizado por el interesado, se obtienen una serie de datos que serán los que se sometan a tratamiento. Ya que cualquier tipo de solicitud dirigida a cualquier tipo de administración, incluso la inscripción de una persona al Registro civil[700], primeramente, hace del conocimiento sobre una petición concreta que un ciudadano desea obtener de la administración o del sector público; y, en segundo lugar, la autoridad pública ante la que se presenta tiene la obligación de conocer la identidad de la persona que presenta la solicitud, a través de los medios de identificación aceptados. A través de la identificación como bien señala el Profesor PIÑAR MAÑAS se «*hace referencia a esos atributos o elementos que son necesarios para las relaciones jurídicas: el nombre, una imagen o dato biométrico (fotografía, huella dactilar, imagen del iris…), la edad, quizá un domicilio, y un número o código identificativo y diferenciado. La identificación no debe hacer referencia a elementos distintos, y a estos efectos superfluos, que no son necesarios para esas relaciones jurídicas*»[701]. Es por lo que, en el marco de este estudio, se debe abordar el tema de la identificación de los ciudadanos, pues son estos los que permiten una relación jurídica segura, incluyendo los medios y sistemas de identificación que deben proveerse a los ciudadanos para que puedan ejercer sus derechos y cumplir con sus obligaciones. En este sentido la Profesora BOTO ÁLVAREZ determina que «*la identificación individual es clave en el desarrollo de actividades clásicas de los poderes públicos: en la actividad prestacional porque, desde luego, son afectaciones particulares de un individuo las que van a determinar, por ejemplo, su condición de beneficiario de un servicio público; en la otra cara de la moneda, también será fundamental identificar la forma correcta al destinatario de una medida de policía o, en último término, al preceptor de una determinada subvención*»[702] Es importante mencionar al respecto que correlativamente a este derecho a que les sean expedidos

[699] RAZQUIN LIZARRAGA, M. M., «El necesario equilibrio entre transparencia y protección de datos personales», ZEGARRA VALDIVIA, D. *La proyección del Derecho Administrativo* Peruano. Ed. Palestra, Lima, 2019, p. 146.
[700] El cual tiene carácter administrativo.
[701] PIÑAR MAÑAS, J. L., «Identidad y persona en la sociedad digital», QUADRA-SALCEDO, T. y PIÑAR MAÑAS, J. L. (Dirs.), *Sociedad digital y derecho*. B.O.E., Madrid, 2018, p. 105.
[702] BOTO ÁLVAREZ, A., «La protección administrativa de la identidad personal: desafíos jurídicos y dilemas sociales», BARRIO ALONSO, C., *et al.* (Eds.), *Fronteras de la ciencia: dilemas,* Biblioteca nueva, Madrid, 2014, p. 76.

medios y sistemas para su identificación, existe la obligación de proveerlos. Para finalizar, se verá como la implementación de la administración electrónica también han cambiado o restringido el uso de determinadas tecnologías en las que se basan.

Tradicionalmente el medio de identificación más utilizado pero no el único es el Documento Nacional de Identidad (D.N.I.), este documento público permite a los nacionales acreditar su identidad y la autenticidad de los datos contenidos en el mismo, de acuerdo con la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana (LOPSC), establece que el D.N.I. es el «*único documento con suficiente valor por sí solo para la acreditación, a todos los efectos, de la identidad y los datos personales de su titular*»[703], además «*permite a los españoles mayores de edad que gocen de plena capacidad de obrar y a los menores emancipados la identificación electrónica de su titular, así como la firma electrónica de documentos*»[704].

Los datos personales que se incluyen y hacen identificables a los ciudadanos son: su nombre y apellidos, así como el número de este documento[705]. Es pertinente recordar en este punto que el TJUE ha determinado que el apellido de las personas «*es un elemento constitutivo de su identidad y de su vida privada, cuya protección está consagrada por el artículo 7 de la Carta de los Derechos Fundamentales de la Unión Europea, así como por el artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Aunque el artículo 8 de dicho Convenio no lo mencione expresamente, el apellido de una persona afecta a su vida privada y familiar al constituir un medio de identificación personal y un vínculo con una familia*»[706]. Al hilo de lo anterior y en relación con el derecho al nombre el Profesor Tolivar Alas determina que este derecho «*se ejerce, se manifiesta y, por*

[703] Art. 8.1 de la Ley Orgánica 4/2015, de 30 de marzo, de protección de la seguridad ciudadana. Modificación introducida por el art. 1 del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.
[704] Apartado 3 de la LOPSC.
[705] Art. 11.1 del Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica. El número de D.N.I se ha determinado por la AEPD «*por sí solo no constituye un dato de carácter personal, si lo será en cuanto resulte adscrito al titular del mismo*», en F.D. III de la Resolución de la AEPD de 20 de abril de 2005 (Expediente N.º: E/00561/2004).
[706] Apartado 52 de la STJUE de 22 de diciembre de 2010 (ECLI:EU:C: 2010:806).

tanto, guarda una estrecha relación operativa con las competencias identificadoras de los poderes públicos»[707].

Continuando con lo relativo al D.N.I., este también permite identificar a su titular de manera electrónica a través del certificado de identificación que es insertado en el mismo. Junto con este también se inserta un certificado de firma electrónica, que también puede ser utilizado para identificarse y además hacer constar la voluntad de su titular[708], en este sentido, la Profesora PÉREZ VELAZCO establece que «*El DNI electrónico se configura así como una poderosa herramienta de identidad en el entorno digital. A las funcionalidades del DNI "analógico" se incorporan las funcionalidades de la biometría digitalizada y de la firma electrónica*»[709]. Además, este documento en su chip contiene la digitalización tanto de la imagen del titular, así como su firma[710].

El artículo 9.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, también lo contempla como principal medio para la comprobación de los datos identificativos de las personas físicas, por tanto como bien señala el Profesor ALAMILLO DOMINGO el DNI supone la principal estrategia de identificación en España, sin embargo, se complementa con otros medios, entre los que se encuentran «*el proyecto CERES de la FNMT-RCM, el reciente aprobado sistema Cl@ve, u otras iniciativas, en el ámbito autonómico y local*»[711]. Sin perjuicio del sistema de identificación de personas extranjeras que tengan su residencia en nuestro país[712].

---

[707] TOLIVAR ALAS, L., «¿Debe sustantivarse el derecho al nombre en la constitución? Reflexiones sobre el *Ius nomine* y el deber de identificación», BAÑO LEÓN, J. Mª (Coord.), *Memorial para la reforma del Estado. Estudios en homenaje al Profesor Santiago Muñoz Machado,* Tomo I, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, p. 512.

[708] De acuerdo con el art. 15.2 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

[709] PÉREZ VELAZCO, M. M., «Intercambio de datos entre administraciones públicas», *IDP: revista de Internet, derecho y política. Revista d'Internet, dret i política*, núm. 2, 2006, p. 50.

[710] Art. 11.4 del Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica.

[711] ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autenticación de los ciudadanos», GAMERO CASADO, E. (Dir.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*. Tomo I. Tirant lo Blanch, Valencia, 2017, p. 676.

[712] El Número de Identificación de extranjero (N.I.E.) tiene por objeto de acuerdo con el contenido del art. 206.1 del Real Decreto 557/2011, de 20 de abril, por el que se aprueba el Reglamento de la

Otros medios de identificación electrónicos que son aceptados por las Administraciones públicas se prevén en el apartado 2 del art. 9 de la LPAC, son los sistemas identificativos que estén basados en un certificado electrónico cualificado, los cuales son expedidos de acuerdo con el Reglamento 910/2014, del Parlamento Europeo y del Consejo, de 23 de junio de 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 (eIDAS). Este documento tiene aplicabilidad directa en nuestro país y obliga a los Estados miembros a notificar los sistemas de identificación electrónica que deban ser reconocidos en los demás Estados miembros[713]. Una de las características indispensables de estos sistemas es la interoperabilidad, dentro de ese marco se prevé el respeto y el adecuado procesamiento de datos personales[714], además se prevé como obligación para los prestadores cualificados de servicios de confianza que presten servicio de confianza cualificados[715], la obligación de contar con personal con adecuada formación en materias de seguridad y protección de datos[716], así como garantizar durante todo el tratamiento su adecuación a la normativa en materia de protección de datos[717] y en general, se establece en su art. 5.1 que los tratamientos de datos personales se llevarán a cabo con arreglo a la Directiva 95/46/CE, sin embargo, como bien sabemos esta ha sido Derogada y sustituida por el contenido del RGPD, por tanto, los prestadores de servicios de confianza cualificados deberán contar un

Ley Orgánica 4/2000, sobre derechos y libertades de los extranjeros en España y su integración social, tras su reforma por Ley Orgánica 2/2009, la identificación de personas extranjeras y la asignación de único y exclusivo de carácter secuencial; su asignación corresponde a la Dirección General de Policía y de la Guardia Civil. Esta documentación inserta por defecto ningún tipo de certificado electrónico.

[713] Art. 7 del eIDAS.

[714] Incisos b) y f) del art. 7.2 del eIDAS. Incluso el considerando de este reglamento en su considerando 19 establece que: «*la interoperabilidad transfronteriza exige que los Estados miembros no impongan tales requisitos y los costes asociados a las partes usuarias establecidas fuera de su territorio*». En este mismo sentido continua el considerando 20 estableciendo que: «*La cooperación de los Estados miembros debe contribuir a la interoperabilidad técnica de los sistemas de identificación electrónica notificados con vistas a fomentar un nivel de confianza y seguridad elevados, adaptados al grado de riesgo. El intercambio de información y de las mejores prácticas entre los Estados miembros con miras a su reconocimiento mutuo debe facilitar dicha cooperación*».

[715] Se refiere a aquella «*una persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado de servicios de confianzas*» y se entiende como servicio de confianza como certificados de firma electrónica, certificados de firma electrónica, sellos electrónicos y certificados de sellos, que cumplen con los requisitos del eIDAS.

[716] Art. 24.2. b) del eIDAS.

[717] Art. 24.2. j) del eIDAS.

una persona que se encargue del correcto cumplimiento del principio de integridad y confidencialidad de los datos en este caso hablaríamos del encargado de seguridad del ENI[718]y, también deberán contar con un delegado de protección de datos, el cual se encargará de «*garantizar los derechos y libertades de las personas cuyos datos son tratados con independencia rindiendo cuentas directamente al más alto nivel jerárquico del responsable o del encargado del tratamiento*»[719], quien asesorará al responsable sobre el correcto cumplimiento tanto del RGPD como de la LOPDGDD.

Finalmente, el esquema de identificación aceptados por las AA.PP. contemplan los sistemas de clave concertada o análogo que lleven a cabo un registro previo del usuario como el sistema «Cl@ve PIN» y «Cl@ve permanente». Ambas han sido desarrolladas a partir de sistemas prexistentes y gestionados respectivamente por la Agencia Estatal de Administración Tributaria (AEAT) [720] y el Instituto Nacional de Seguridad Social (INSS)[721]. La primera tiene carácter temporal, pues se basa en un código único que se envía a un dispositivo móvil de los usuarios, para obtenerla se necesita el número de identificación fiscal y una contraseña creada por el usuario, que es utilizada sobre todo para acceder de manera puntual a los servicios que la admiten. El sistema de cl@ve permanente, como se puede deducir de su nombre tiene una vigencia más prolongada, exactamente de dos años, además de estar creada para utilizarse de manera frecuente, su contraseña la establece el

[718] De acuerdo con el art. 10 del ENI. En este sentido la AEPD ha determinado que las funciones del encargado de seguridad de acuerdo con el precepto anteriormente señalado que: «*proporciona directrices encaminadas a garantizar la seguridad de la información, sean datos personales o simplemente información de las Administraciones Públicas*», Cfr. AEPD, informe 2018/0170, p. 11.
[719] *Íd.*
[720] Creada por medio de la Resolución de 17 de noviembre de 2011, de la Presidencia de la Agencia Estatal de Administración Tributaria, por la que se aprueban sistemas de identificación y autenticación distintos de la firma electrónica avanzada para relacionarse electrónicamente con la Agencia Estatal de Administración Tributaria.
[721] Se creó bajo el amparo del art. 13.2.c) de la LAECSP. Específicamente en el ámbito de la SS se implementa por medio de las resoluciones del INSS de 4 de junio de 2014, por la que se aprueban sistemas de identificación y autenticación de los ciudadanos para relacionarse electrónicamente con el Instituto Nacional de la Seguridad Social y la de fecha 24 de julio de 2014, de la Tesorería General de la Seguridad Social, por la que se aprueba el sistema de identificación, autenticación y firma electrónica previsto en el art. 12.2 letra c) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, para relacionarse electrónicamente con la Tesorería General de la Seguridad Social.

propio usuario[722]. En cualquier caso, los sistemas de identificación con registro previo se debían autorizar por la Secretaría General de Administración Digital del Ministerio de Política Territorial y Función Pública[723]. Autorización que estaba condicionada por motivos de seguridad pública[724] entendiéndose en sentido negativo ante su falta de resolución en el plazo de tres meses.

La redacción original del apartado 2 del art. 9 de la LPAC, establecía que correspondía a cada Administración determinar la admisión de alguno de los sistemas de identificación: sello, firma (ambos basados en certificados electrónicos cualificados) o de clave concertada para determinados trámites y procedimientos y, que en su caso la admisión de los sistemas de registro previo suponía la aceptación de los sistemas basados en certificado electrónicos o cualificados de sello o firma. Actualmente con los cambios introducidos por el Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones, las AA.PP. solo se pueden aplicar el sistema de identificación basado en certificados electrónicos para todo procedimiento, incluso cuando se admitan los sistemas de registro previo. Por este mismo RDL se obliga en todo caso a las AA.PP. a situar dentro de la UE los recursos técnicos para la recogida, almacenamiento, tratamiento y gestión de estos, restringiendo también su transferencia a un tercer país[725]. En relación con este supuesto, esta adición se entiende que refuerza la aplicabilidad de la normativa de protección de datos aun si

[722] Tiene que contener 8 caracteres como mínimo y estará integrada por caracteres alfanuméricos con distinción entre mayúsculas y minúsculas, sin embargo, no podrá utilizarse el nombre del usuario como contraseña ni su D.N.I., Cfr. https://clave.gob.es/clave_Home/Clave-Permanente/Seguridad.html (consulta: 3 de octubre de 2020).

[723] A día de hoy es la misma Secretaría la que lleva a cabo dichas autorizaciones, sin embargo debido a al cambio de la estructura de los Ministerios y a su estructura orgánica, esta Secretaría depende orgánicamente de la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, de acuerdo con el contenido del art. 15 del Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

[724] Si se emitía un informe vinculante en ese sentido por la Secretaría de Estado de Seguridad del Ministerio del Interior, cfr. Art. 9.2.c de la LPAC.

[725] Salvo que así se haya establecido por una decisión de adecuación de la Comisión Europea o cuando ello requiera el cumplimiento de las obligaciones internacionales asumidas por España.

se acudiese a un encargado externo a las AA.PP., no dejando margen de duda sobre la aplicabilidad del RGPD[726].

Una cuestión quizás más controvertida sea la añadida en el apartado cuatro, que a la letra dispone que: «*En todo caso, la aceptación de alguno de estos sistemas por la Administración General del Estado servirá para acreditar frente a todas las Administraciones Públicas, salvo prueba en contrario, la identificación electrónica de los interesados en el procedimiento administrativo*», lo cual condiciona la aceptación de alguno de los sistemas establecidos en el apartado 2 del art. 9 por las demás AA.PP. a la aceptación de alguno por la AGE como forma de identificación.

Es necesario señalar que los sistemas de identificación del apartado 2 del art. 9, también son admitidos como medios para acreditar «*la autenticidad de la expresión*» de la voluntad de los interesados y su consentimiento, de acuerdo con el apartado 2 del art. 10 de la LPAC. De acuerdo con el art. 11 de esta misma ley se señala que los interesados de manera general podrán realizar cualquier actuación en el procedimiento administrativo siempre que acrediten su identidad por cualquiera de los medios de identificación del art. 9. Sin embargo, establece el uso obligatorio de firma electrónica para: 1) formular solicitudes, 2) presentar declaraciones responsables o comunicaciones, 3) interponer recursos, 4) desistir de acciones y 6) renunciar a derechos. En relación con esto la Profesora MENÉNDEZ SEBASTIÁN señala que «*parece hasta lógico que en una decisión responsable o comunicación o, sobre todo una renuncia de un derecho, pueda exigirse un sistema de firma de mayor seguridad, mientras que para otros actos del administrado que impliquen consecuencias menos relevantes para el mismo, puedan admitirse otros sistemas, como el de claves concertadas*»[727].

Con respecto a lo anterior y no menos importante es lo relativo al contenido en la D.A. Sexta por la que se establece la imposibilidad de autorizar sistemas de registro previo como medios de identificación o como firma electrónica si están basados en tecnologías de registro distribuido, en tanto no sean regulados por el Estado en el marco de la UE y que en caso de ser autorizados será la AGE quién actúe

[726] En concordancia con lo establecido en el art. 3 del RGPD.
[727] MENÉNDEZ SEBASTIÁN, E. Mª., *op. cit.,* 66.

como intermediaria ya que «*ejercerá las funciones que corresponda para garantizar la seguridad pública*». Estos sistemas facilitan «*una lista en crecimiento, ordenada cronológicamente de registros transaccionales irrevocables firmados criptográficamente, compartidos por todos los integrantes de una red*»[728]. De hecho, estos sistemas están basados en lo que hoy se conoce como *Blockchain* o sistema de cadena en bloque[729], cuyas características principales son la descentralización y su naturaleza colaborativa. Actualmente, esta previsión legal anula la posibilidad de llevar a cabo las facultades ejecutivas de la ley por las CC.AA., de manera que el sistema de cadena en bloque no podrá ser utilizado hasta que no sean reguladas por el legislador comunitario o sea incorporado dentro del Reglamento eIDAS como medios de identificación electrónica seguros. Además, la D.A sexta de este RDL condiciona la existencia de la normativa nacional a la regulación de estos sistemas en el ámbito comunitario, por lo que el legislador declina la oportunidad de regular, aunque sea de manera provisional este tipo de tecnologías dada su complejidad técnica[730]. Finalmente, poniéndonos en el hipotético caso de la existencia de la

[728] ALLESSIE, D., SOBOLEWSKI, M. and VACCARI, L., «Blockchain for digital goverment. An assessment of pioneering implementations in public services» (en línea), *Publications Office of European Union, Luxembourg*, 2019, p. 8. DOI: 10.2760/942739 (consulta y descarga: 22 de febrero de 2020).

[729] La AEPD ha abordado este tema explicándolo de manera muy clara en su documento «Tecnologías y protección de datos en las AA.PP.» como: «*una red de participantes (pares, peers o nodos) que comparten un registro de forma distribuida en el que se apunta quién posee qué (activos) y quién negocia con quién (transacciones). A diferencia de los tradicionales sistemas centralizados en los que las bases de datos están controladas por una única autoridad central, en blockchain todos los nodos mantienen una copia de este registro por lo que resulta extremadamente complicado manipular la información anotada sin que la red, entendida esta como el conjunto de los participantes, sean conscientes del intento de cambio. Blockchain toma su nombre por la forma en que se organiza ese registro: un conjunto de bloques en los que se agrupan las transacciones y que están enlazados unos con otros, en orden cronológico, a través de un mecanismo criptográfico llamado hash que garantiza la integridad y la inmutabilidad de la información registrada en la cadena*», cfr. AEPD, «*Tecnologías y protección …*», p. 44. El Profesora SWAN también explica de una sencilla su funcionamiento y el porqué de su denominación, ya que «*los bloques o lotes de transacciones se publican secuencialmente en un libro de registro, y cada nuevo bloque comienza haciendo referencia al bloque anterior, de modo que se crea una cadena de bloques. El resultado es que se crea una red segura en la que cualquier transacción puede ser confirmada independientemente como única y válida sin un intermediario centralizado como un banco, un gobierno u otra institución*», Cfr. SWAN, M., «Blockchain Temporality: Smart Contract Time Specifiability with Blocktime» (en línea), *Springer International Publishing Switzerland 2016*, p. 186. DOI: 10.1007/978-3-319-42019-6_12 (consulta: 8 de enero de 2021).

[730] En caso de implementar este tipo de sistemas como medios de identificación sería necesario delimitar qué AA.PP. se configurarían como responsables del tratamiento, qué datos personales serían tratados, quiénes podrían ser responsables del tratamiento, aquellas medidas técnicas y organizativas que los intervinientes deban cumplir con el fin de preservar la integridad y la seguridad de los datos, así como determinar qué derechos podrían ser ejercitables por los ciudadanos. Al ser una tecnología disruptiva en relación con las existentes se tendría que realizar una evaluación de

legislación estatal que regulen estos sistemas el apartado segundo de esta D.A. determina que la AGE deberá actuar como intermediaria por motivos de seguridad nacional.

Lo anterior supone un nuevo reto para el derecho administrativo no solo por la gestión de los sistemas de identificación, también en relación con las normas de seguridad que deban implementar los agentes colaboradores de este sistema de cadena en bloque, para que sea compatible con el actual Esquema Nacional de Seguridad. Por lo que se refiere a la interoperabilidad, estos sistemas de identificación deberán de seguir el esquema en la materia de tal forma que, puedan ser utilizados por todas las AA.PP. La oportunidad de abordar estas cuestiones como se ha señalado anteriormente se ha dejado pasar, ya que de acuerdo con el contenido del Real Decreto-ley 14/2019, de 31 de octubre, supedita la validez y existencia de este tipo de sistemas implementados en este ámbito a una normativa comunitaria aún inexistente. Ahora bien ¿cómo afectaría la implementación de esta tecnología en relación con los datos personales identificativos de las personas? Partiendo de la base de que las AA.PP. deben tratar los datos desde el diseño y por defecto utilizando medidas técnicas y organizativas de minimización y, de la necesidad de un registro previo para que se compruebe la identidad de los interesados, esta actividad seguiría suponiendo el tratamiento de datos personales. Lo que podrían hacer las AA.PP. sería realizar ese tratamiento utilizando la seudonimización de manera que los datos identificativos no se incluyeran en la clave pública[731] o llave para realizar

impacto antes de ser implementada, incluso esta medida también resultaría idónea por la cantidad ingente de datos que serían tratados. En este sentido la AEPD determina que las AA.PP. antes de implementar este tipo de tecnología deberán tener en cuenta de manera especial los siguientes aspectos: responsabilidad del tratamiento, el derecho al olvido, la conservación limitada de los datos, la seguridad de los datos y las transferencias internacionales de datos. En relación con la compatibilidad de estos sistemas con la normativa de protección de datos señala que: «*Es responsabilidad de la Administración Pública evaluar si la solución tecnológica adoptada es la más adecuada o, por el contrario, introduce riesgos que no permitan ser gestionados. En particular, es importante evaluar qué tipo de arquitectura de red blockchain se adapta mejor a la solución (públicas, privadas, permisionadas y no permisionadas) ya que no todas ellas representan el mismo nivel de riesgo, además de definir el modelo de gobernanza más adecuado. No debe perderse de vista que la no posibilidad de cumplir técnicamente con alguna de las obligaciones exigidas por el RGPD al responsable no debe ser considerada un riesgo susceptible de tratar sino un incumplimiento normativo*» cfr. *Ib.,* pp. 45-46 y 48-49.

[731] Actualmente, España utiliza un sistema de cifrado simétrico (*public key infraestructure)* y como bien señala el LÓPEZ ÁLVAREZ, la clave pública «*está asociada a nuestra identidad real de manera que se nos puede imputar el uso de la firma electrónica*», *Vid.* LÓPEZ ÁLVAREZ, L. F., «Blockchain y protección

este tipo de transacciones, además sería necesario que en el uso de la criptografía no se utilizaran otro tipo de datos que sirvieran como referencias cruzadas, como metadatos que pudieran identificar a la persona directamente, es pertinente aclarar que esto no supondría una decisión automatizada sino un medio electrónico por el cual se obtienen «llaves» para comunicarse con las AA.PP. y, por tanto, sujeto al ENS y la normativa de protección de datos personales vigente[732].

Otra cuestión nada baladí en relación con la recogida de datos personales dentro de la administración electrónica es lo relativo a los registros. Actualmente el art. 16 de la LPAC los regula y se establece como obligación para las AA.PP. disponer de un «Registro Electrónico General», en el que se puedan presentar documentos de carácter electrónico dirigidos a la propia Administración o a sus órganos o entidades quedando asentado en este el momento de su presentación a efectos de cumplir con los plazos si los hubiera. En este sentido los Profesores FERNÁNDEZ NIETO y RIVERO ORTEGA consideran que «*Aunque se prevé la posibilidad de registros electrónicos propios de los organismos públicos vinculados o dependientes, por su personalidad jurídica, propia, también se indica su necesaria interoperabilidad e interconexión con el de su Administración matriz, que habrá de funcionar "como un portal"*»[733]

Por medio del registro electrónico también podrá quedar plasmada la fecha de salida de documentos si la Administración dirigiese algún tipo de información de

de datos», LÓPEZ CALVO, J. (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, p. 1019.

[732] En este contexto el Profesor ALAMILLO DOMINGO determina que «*el ENS sí que encontramos un alineamiento general de los sistemas de identificación que pueden ser admitidos por las Administraciones Públicas con el Reglamento eIDAS, pero sólo por lo que se refiere a las exigencias de seguridad que deben cumplir dichos sistemas, y no a otras cuestiones que podrían resultar más conflictivas, como las relativas a la interoperabilidad, ya que el Reglamento eIDAS apuesta, en la actualidad, por una red de sistemas como Cl@ve, y no por sistemas de identificación basados en tecnologías de registro distribuido. Dado que uno de los fundamentos técnicos de las tecnologías de registro distribuido es, como hemos mencionado ya, es el empleo de firmas digitales, con carácter general podemos considerar que estos sistemas permitirán cumplir sin dificultad alguna los criterios del Reglamento eIDAS para el nivel sustancial, por lo que se podrán emplear en la mayoría de supuestos de procedimiento administrativo*», cfr. ALAMILLO DOMINGO, I., «Las tecnologías de registro distribuido (*blockchain*) y la transformación del procedimiento administrativo» (en línea), *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal,* núm. 1 (enero), 2019. Disponible en: smarteca.es (consulta 9 de enero de 2021).

[733] FERNÁNDEZ NIETO, A. y RIVERO ORTEGA, R., «La administración sin papel: registro, expediente, archivo electrónico, ¿Estamos preparados?», *Revista Vasca de Administración Pública*, núm. 105, 2016, p. 457.

carácter electrónico a otra Administración o a particulares[734]. Sin perjuicio de lo anterior, se prevé la posibilidad de que órganos y entidades dependientes cuenten con su propio registro electrónico siempre que fuera interoperable y estuviera interconectado con el registro electrónico general de la administración de la que depende. Estos funcionan como un portal, es decir, como un punto de acceso electrónico a través de internet a los registros dentro de su organización. Una cuestión directamente relacionada con la protección de datos personales es la constancia de los asientos que son realizados en los registros, y en particular si una persona física es la que utilizará estos medios para comunicarse con la administración. Como se mencionó anteriormente, es obligación de las AA.PP. cerciorarse de la identidad a través de medios electrónicos, por tanto, será necesario algún tipo de medios de identificación para poder presentar cualquier tipo de documentación. Entre los datos que deberán figurar en tales asientos está precisamente la forma de identificación del interesado, lo cual es necesario y proporcional, sin perjuicio de que en el posterior tratamiento de datos se utilice el número de expediente asignado a cada caso para referirse al tipo de trámite que ha instado el interesado. Es importante señalar en este punto que las previsiones legales contenidas en la LPAC en lo referente a los registros electrónicos no entrarán en vigor hasta el 2 de abril de 2021, fecha que se ha ido postergando desde la publicación de la referida ley, ya que a la fecha aún la totalidad de las administraciones no se han adaptado al cambio tecnológico para relacionarse por este tipo de medios con el ciudadano[735].

---

[734] En cuanto a lo anterior, la Profesora CAMPOS ACUÑA determina que: «*Es decir, que la redacción del precepto, en términos potestativos, parecería dejar al libre arbitrio de cada administración la decisión de utilizar el registro electrónico como registro de salida. En conclusión no parece ajustarse al modelo de funcionamiento de las AAPP, en cuanto a la seguridad y trazabilidad en sus actuaciones en la vigencia del expediente electrónico, sin que pueda entenderse discrecional la utilización del registro de salida para la tramitación de los procedimientos electrónicos sobre esta base, y que resultaría incongruente con las referencias posteriores a los asientos de salida, sin perjuicio de la existencia de normas propias de aplicación en función del nivel territorial de la administración que apostarían por entender la vigencia del mismo, como sucede en el ámbito local con el Real Decreto 2568/1986, de 28 de noviembre, de Organización, Funcionamiento y Régimen Jurídico de las Corporaciones Locales*», cfr. CAMPOS ACUÑA, C., «El procedimiento administrativo electrónico en la Ley 39/2015», PINTOS SANTIAGO, J. (Dir.), *La implantación de la administración electrónica y de la e-factura,* Wolters Kluwer, Madrid, 2017, pp. 103-104.

[735] En esta misma fecha también producirán efectos los preceptos relativos al registro electrónico de apoderamientos, el registro de empleados públicos habilitados el punto de acceso general electrónico

Además, no debemos olvidar los medios con los que cuentan las AA.PP. para relacionarse con los ciudadanos a través de internet, los cuales resultan cruciales en esta nueva era tecnológica, entre los que se encuentran la sede electrónica y los portales de internet. Por medio de estos los ciudadanos obtienen información de las diferentes Administraciones públicas, sin embargo, debemos de tener claro que la sede electrónica de acuerdo con el contenido del art. 38, es una herramienta tecnológica que permite a los ciudadanos relacionarse con la Administración pública, en la que es necesaria la identificación del ciudadano para que se pueda iniciar algún trámite, la prestación de un servicio o la iniciación de un procedimiento de forma no presencial. En cambio, los portales de internet (art. 39 LRJSP) son aquellas direcciones web por medio de las cuales se puede entrar a la sede electrónica, y dónde se encuentra todo tipo de información acerca de la AA.PP. titular. En este sentido, como bien señala el Profesor MARTÍNEZ GUTIÉRREZ entre ambos existe relación más no una correspondencia, «*se plantea una relación de género (portal de internet) y especie (sede electrónica) y, en definitiva, toda sede electrónica será necesariamente un portal de internet, pero no todo portal de internet será sede electrónica*»[736]. Estimamos que se encuentran regulados en la LRJSP por ser medios con los que deben contar las AA.PP. *ad intra,* sin embargo, consideramos oportuno al igual que el autor antes referido que hubiese sido importante incorporar la previsión de estas dos herramientas en la LPAC pues ambas constituyen dos medios que necesariamente debe conocer el ciudadano para relacionarse con las AA.PP.[737].

1.4.4 Almacenamiento y tratamiento de datos.

El almacenamiento de la información de manera tradicional ha sido relacionado con los medios físicos o tecnológicos que los responsables de los tratamientos de datos utilizan para guardar, almacenar y custodiar la información. Toda esa información puede contener datos de carácter sensible dependiendo de la finalidad del tratamiento o simplemente datos de carácter personal, es por ello, que

de la Administración y lo relativo al archivo único electrónico, de acuerdo con lo establecido en la Disposición Final Séptima de la LPAC que recientemente ha sido modificada por la Disposición Final 9 del Real Decreto-ley 28/2020, de 22 de septiembre, de trabajo a distancia.

[736] MARTÍNEZ GUTIÉRREZ, R., *op. cit.,* p. 172.

[737] Cfr. *Ib.,* p. 174.

estos soportes de información deberán ajustarse a la normativa de protección de datos, aun cuando el tratamiento de datos sea llevado a cabo en un tercer Estado[738]. Estos soportes deberán cumplir con determinadas medidas técnicas y organizativas, es por ello que deberemos acudir al contenido de los esquemas de seguridad e interoperabilidad.

La ubicación de los archivos es otra de las medidas organizativas previstas en el Real Decreto-ley 14/2019, de 31 de octubre, que cobra especial relevancia para los medios de almacenamiento de las formas de identificación y firma contenidos respectivamente en los art. 9.2 y 10.2 de la PAC, en relación con el registro previo, del art. 9.2 de la LPAC y con los medios de firma registro del apartado 2 del art. 10, que contengan datos de categorías especiales, estos medios tienen que estar situados en territorio de la UE. Sin perjuicio de que la totalidad de los datos personales deben estar disponibles en los dos supuestos para su acceso por autoridades administrativas y judiciales[739]. No obstante, también deberán cumplir con las medidas técnicas y organizativas de ambos esquemas previstos en el art. 156 de la LRJSP.

Otra restricción de la localización de los medios de almacenamiento se encuentra en el art. 46 bis de la LRJSP, el cual determina que los sistemas de información y comunicaciones para la «*recogida, almacenamiento, procesamiento y gestión del censo electoral, los padrones municipales de habitantes y otros registros de población, datos fiscales relacionados con los tributos propios o cedidos y los datos de usuarios del sistema nacional de salud, así como los correspondientes tratamientos de datos personales, deberán de ubicarse y prestarse dentro del territorio de la Unión Europea. Los datos a que se refiere el apartado anterior no podrán ser objeto de transferencia a un tercer país u organización internacional, con excepción de los que hayan sido objeto de una decisión de adecuación de la Comisión Europea o cuando así lo exija el cumplimiento de las obligaciones internacionales asumidas por el Reino de España».* Lo anterior nos sitúa en el siguiente panorama: por una parte, las AA.PP. no tendrán ningún tipo de problemas si el tratamiento y el almacenamiento de los

738 Cfr. Art. 3.1 del RGPD.
739 Cfr. Art. 9.3 y art 10.3 de la LPAC.

datos se realiza con medios propios[740] y acordes al contenido del ENI y del ENS[741]. Por otra parte, cuando el tratamiento de datos sea encargado a otra persona esta deberá situar los medios y llevar a cabo el tratamiento de datos dentro de la UE. De manera que, no podrá encargar esta labor a aquellos que no sitúen los medios materiales y su actividad en el territorio antes indicado. Pensemos, por ejemplo, en prestadores de servicios de *Cloud Computing* [742], ya que como bien señala la Profesora FUERTES LÓPEZ: «*el negocio mundial de los servicios en la nube está claramente dominado por muy pocos protagonistas y ninguno, por el momento, es europeo*» [743] En este último caso, también se deberá señalar en los pliegos de

[740] En este primer supuesto, es necesario señalar que el Centro Criptológico Nacional es el encargado de valorar y acreditar la capacidad de los sistemas de las TIC «*que incluyan medios de cifra, para procesar, almacenar o transmitir información de forma segura*» (Art. 2.2. d) del Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional) que sean implementados por la AGE, en este contexto ha implementado la herramienta AMPARO por la cual «*se identifican y valoran los activos del sistema, la infraestructura y el nivel de seguridad en el que se encuentra. Como resultado, AMPARO identifica las amenazas y riesgos presentes en el sistema así como el conjunto de salvaguardas de mitigación necesarias*» además esta herramienta también permite identificar los tratamientos de datos realizados por los organismos, Cfr. Centro Criptológico Nacional, Ficha técnica (AMPARO). Disponible en: https://www.ccn-cert.cni.es/pdf/documentos-publicos/4262-datasheet-amparo.html (consulta: 9 de enero de 2021).

[741] Actualmente el Real Decreto 806/2014, de 19 de septiembre, sobre organización e instrumentos operativos de las tecnologías de la información y las comunicaciones en la Administración General del Estado y sus Organismos Públicos, regula la posibilidad de que sean compartidos los medios y servicios tecnológicos por la AGE y sus organismos. En este contexto, de acuerdo con el art. 10 de este RD se entienden como medios y servicios a «*todas las actividades, infraestructuras técnicas, instalaciones, aplicaciones, equipos, inmuebles, redes, ficheros electrónicos, licencias y demás activos que dan soporte a los sistemas de información*». Uno de los servicios compartidos que es importante en relación con el almacenamiento de datos es el servicio de nube híbrida (SARA), es decir que «*mediante la configuración de nodos de consolidación tanto en CPDs de la Administración (nube privada) como de proveedores externos (nube pública) que permitirá a las unidades TICs clientes del servicio proveerse de capacidades tanto en nube privada como en nube pública, lo que decidirán para cada servicio que tengan que implantar atendiendo a sus características y los costes que puedan asumir*», cfr. Dirección de Tecnologías de la Información y las Comunicaciones (DTIC), Declaración de servicios compartidos, pp. 21-23, NIPO: 630-15-211-9.

[742] La AEPD ha fijado los aspectos a tener en cuenta por las AA.PP. al contratar servicios de *Cloud Computing*: 1) las garantías contractuales deberán estar determinadas en los pliegos de prescripciones, 2) debe formalizarse un contrato por escrito con el encargado del tratamiento, en este caso con el prestador del servicio en la nube, 3) en el contrato se deberá determinar el objeto, la finalidad, la base del tratamiento, las categorías de datos y los derechos y obligaciones del responsable, 4) al término de la prestación contractual a deberán ser devueltos al responsable o destruidos, 5) en caso de subcontratación de servicios de computación en la nube, se podrá llevar a cabo si se ha especificado en el contrato principal entre las AA.PP y el contratista, el tratamiento debe ajustarse a las instrucciones de la AA.PP. y, se deberá formalizar un contrato entre el contratista y el subcontratista, 6) se deben especificar las medidas técnicas y organizativa a adoptar por el encargado, así como todas las previsiones que se describen en el Apartado 3.1 de este trabajo de investigación. Cfr. AEPD, «*Guía para clientes que contraten servicios de Cloud Computing*» (en línea). 2018, pp. 19-24. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-cloud-clientes.pdf (consulta: 8 de octubre de 2020).

[743] FUERTES, M., «Soberanía digital europea», *El cronista del Estado Social y Democrático de Derecho,* núm. 90-91, diciembre 2020-enero 2021, 2021, p. 66.

cláusulas administrativas particulares que el contratista quedará sometido a la normativa de protección de datos vigente[744]. En consecuencia, cuando sea otra persona la que trate parte o la totalidad de datos personales se deberá llevar a cabo un riguroso y exhaustivo análisis de riesgos, con la finalidad de determinar las medidas específicas a adoptar, partiendo del hecho que solo podrán ser encargados del tratamiento aquellas personas que sean cualificadas y cumplan de manera escrupulosa las medidas de seguridad para llevar a cabo el tratamiento de datos personales.

Ahora bien, en relación con los documentos utilizados en las actuaciones administrativas de acuerdo con el art. 46 de la LRJSP, estos deberán ser almacenados en medios electrónicos de manera general, a menos que no sea posible. Los soportes y medios que alberguen este tipo de información deberán contar con medidas que establezca al efecto el ENS[745]. En el que se prevé una especial atención a la estructura y organización de la seguridad del sistema y de la información almacenada o en tránsito «a través de entornos inseguros», como «*equipos portátiles, asistentes personales (PDA), dispositivos periféricos, soportes de información y comunicaciones sobre redes abiertas o con cifrado débil*»[746]. En todo caso la seguridad se aplicará a la información almacenada y se incluirá en la política de seguridad de las AA.PP.[747].

En cuanto a las medidas de seguridad, el ENS en su Anexo V también prevé la inclusión en los pliegos de las cláusulas administrativas particulares en adquisición de productos de seguridad y la contratación de estos servicios[748]. En estos pliegos se deberá incluir la «*referencia precisa, documentada y acreditativa de que los productos de seguridad, servicios, equipos, sistemas, aplicaciones o sus componentes, cumplen con lo indicado en la medida op.pl.5 sobre componentes certificados, recogida*

[744] De acuerdo con el contenido del art. 122.2 de la LCSP.
[745] Cfr. Apartados 2 y 3 del art. 46 de la LRJSP.
[746] Cfr. Art. 21 del ENS. En relación con el cifrado de la información, se deberá realizar durante el almacenamiento y la transmisión de esta, cuando tenga un nivel alto de confidencialidad (5.7.3 del Anexo II del ENS). En cuanto a la protección de servicios y aplicaciones web, se prevendrán ataques de manipulación de la información que sea almacenada en los dispositivos de los usuarios en «*una página web a través de su navegador, a petición del servidor de la página, conocido en terminología inglesa como "cookies"*» y en la utilización de *proxies* y *caché* (5.8.2 del Anexo II del ENS).
[747] Cfr. Art. 11.1.j) del ENS. Sin perjuicio de aplicarles los principios del art. 4 del ENS.
[748] *Vid.* art. 18 del ENS.

en el apartado 4.1.5 del anexo II» del ENS[749]. Es decir, aquellos equipos, sistemas o productos «*cuyas funcionalidades de seguridad y su nivel hayan sido evaluados conforme a normas europeas o internacionales y cuyos certificados estén reconocidos por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Tendrán la consideración de normas europeas o internacionales, ISO/IEC 15408 u otras de naturaleza y calidad análogas. Una instrucción técnica de seguridad detallará los criterios exigibles*»[750].

El párrafo segundo del Anexo V alude directamente a la protección de datos en este caso se prevé que deberán incluirse en los pliegos de las cláusulas administrativas particulares cuando se adquieran productos de software destinados al tratamiento la «*descripción técnica el nivel de seguridad, básico, medio o alto*» para alcanzar las medidas de seguridad del ENS[751] y en lo establecido en el art. 32 del RGPD[752].

El uso de nuevas tecnologías en la actividad de las Administraciones es una de las cuestiones que les afecta de manera directa a los interesados. En los tiempos que hoy vivimos uno de los principales caballos de batalla es la toma de decisiones automatizada, no solo por el tratamiento de datos que realizan las Administraciones, sino más bien por la afectación de los derechos de los interesados dentro del procedimiento administrativo, sobre todo, por la falta de la transparencia de cómo se realiza[753].

---

[749] Cfr. Anexo V del ENS.

[750] *Íd.* Es menester señalar a que se refiere esta norma ISO. Esta norma está compuesta por tres partes que se refieren a las tecnologías de la información, específicamente a las técnicas de seguridad y a los criterios de evaluación de esta, específicamente al modelo en general, a los componentes funcionales de seguridad y a los de garantía de la misma, Cfr. Organización Internacional de Normalización, Publicly Available Standards. Disponibles en: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html (consulta 08 de octubre de 2020).

[751] Lo anterior, en consonancia con la Disposición Adicional Primera de la LOPDGDD.

[752] En relación con el contenido la D.A. única 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. Contenido que sigue vigente de acuerdo con la Disposición derogatoria única, ya que estas medidas no se contraponen a lo establecido en el RGPD ni a la nueva LOPDGDD.

[753] Los Profesores FERNANDO PABLO y TERRÓN SANTOS determinan que el RGPD «*ha establecido también ciertas bases para sujetar a alguna regla jurídica el desarrollo y la aplicación de la IA y de sus mecanismos de actuación. Las decisiones de organizaciones públicas o privadas que se confíen a estos*

El art. 41 de la LRSP define a la actuación administrativa automatizada como «*cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una Administración Pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público*». Normalmente este tipo de decisiones están basadas en datos de los interesados que los identifica o los hace identificables, por tanto, la actividad administrativa automatizada supone un tratamiento de datos personales al que le deberá ser aplicable como es lógico la normativa en la materia.

En este sentido, el art. 21 del RGPD regula las decisiones individuales automatizadas, incluida la elaboración de perfiles. De manera general establece como derecho del interesado «a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos» a este o le afecte de modo similar de forma significativa.

Sin embargo, se exceptúa lo anterior, si estas decisiones son autorizadas por el derecho nacional de los Estados miembros como es el caso de España, que autoriza en una norma básica la actuación administrativa automatizada, la cual en

mecanismos de automatización de última generación cuentan por tanto con un conjunto de principios centrados momentáneamente en la afectación singular a las personas y en la prohibición de resultados discriminatorios, que pueden dirigir soluciones futuras. Una gobernanza completa de los algoritmos, si es que tenemos que entregar a ellos decisiones trascendentes, requerirá establecer mediante normas de derecho positivo, mecanismos de autorización previa, comunicación o declaración de responsables, tal como sucede en otros ámbitos de riesgo», cfr. FERNANDO PABLO, M.M. y TERRÓN SANTOS, D., «Sobre la gobernanza de la Inteligencia Artificial» (versión electrónica), GUAYO CASTIELLA, I. DE y FERNÁNDEZ CARBALLAL, A. (Coords.), *Los desafíos del Derecho público en el siglo XXI. Libro conmemorativo del XXV Aniversario del acceso a la Cátedra del Profesor Jaime Rodríguez-Arana Muñoz,* Instituto de Administración Pública, Madrid, 2019, pp. 418. El Profesor HUERGO LORA realiza un estudio profundo y sistemático de las cuestiones relacionadas con este tipo de decisiones en su obra reciente obra «Una aproximación a los algoritmos desde el Derecho administrativo», Cfr. HUERGO LORA, A., Una aproximación a los algoritmos desde el Derecho administrativo», HUERGO LORA, A. (Dir.), *La regulación de los algoritmos,* Thomson Reuters Aranzadi, Navarra, 2020. En relación la información que debe proporcionarse a los ciudadanos la Profesora MENÉNDEZ SEBASTIÁN pone de relieve la importancia de que el interesado «*pueda conocer cómo y sobre todo porqué se ha tomado esa decisión, cuando ésta se adopte de forma automatizada será imprescindible que conozca los parámetros que se han introducido en la aplicación o sistema informático a tales efectos*», *vid.* MENÉNDEZ SEBASTIÁN, E. Mª, *op. cit.,* p. 88. En este sentido hay que recordar que «*el gobierno abierto se basa en la apertura de datos*», lo cual tiene como consecuencia directa la reutilización de datos por parte de otras personas sean físicas o jurídicas para la creación y mejora de servicios y productos, cfr. CERRILLO I MARTÍNEZ, A., «Capítulo V. El gobierno abierto» (formato electrónico), CERRILLO I MARTÍNEZ, A. (Coord.), *A las puertas de la administración digital. Una guía detallada para la aplicación de las leyes 39/2015 y 40/2015*, Instituto Nacional de Administración Pública, Madrid, 2016, pp. 113.

principio se le aplicarán los esquemas de interoperabilidad y seguridad, como salvaguarda de los interese legítimos de los interesados.

La problemática surge cuando las AA.PP. utilizan otros medios que no son propios o que no se ajusten a los esquemas antes descritos. Pensemos, por ejemplo, en la utilización de *cookies* en el portal de internet de una AAPP[754] y que a partir de estas se elabore un perfil sobre las preferencias en la navegación de los usuarios de estos sitios, sean o no gestionadas por las AA.PP. En este caso, tal y como lo establece la LRJSP no estaríamos ante un acto administrativo y menos frente a un procedimiento administrativo, más bien nos situaríamos en el plano de la transparencia activa por las informaciones que se publiquen en el portal y que deben darse a conocer a los ciudadanos por ese medio. Situación que está permitida por ley, de acuerdo con el art. 22.2 de la LSSI y requerirá el consentimiento explícito de los ciudadanos[755], acompañado de medidas adecuadas para salvaguardar los derechos de éstos e incluso oponerse a este tipo de tratamientos.

Otra cuestión de especial importancia en el tratamiento de datos en el procedimiento electrónico es la emisión de los documentos en formato electrónico por las administraciones públicas. Dejando al margen los efectos que pueda llegar a tener la notificación por medios electrónicos, la emisión de documentos de acuerdo con el art. 26 de la LPAC se requieren determinados requisitos para que sean considerados válidos. Se entiende por documento electrónico «*la suma de uno o varios ficheros contenido, uno o varios ficheros de firmas asociadas a dicho contenido, así como las estructuras de datos asociados a dicha información que albergan los metadatos en un determinado sistema de gestión documental, siendo a su vez posible que todo este conjunto de componentes sea encapsulado en otra estructura o fichero contenedor, de cara por ejemplo a facilitar los intercambios*»[756], deberán ser emitidos

[754] Los portales de internet están regulados actualmente por el art. 39 de la LRJSP, el que se determina que es un punto de acceso electrónico cuyo titular es alguna Administración pública o algún ente u organismo dependiente de una AAPP, y tiene como objetivo permitir el acceso a la información a los ciudadanos y a la sede electrónica.

[755] Cfr. Art. 22.2 c) del RGPD

[756] Dirección de Tecnologías de la Información y las Comunicaciones (DTIC), «Documento electrónico. Guía de aplicación de la Norma Técnica de Interoperabilidad» (en línea). 2ª ed., Ministerio de Hacienda y Administraciones Públicas, 2016, p. 14. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5881e773-6d5d-48b6-b4a6-

por la autoridad competente al efecto, y de acuerdo con la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica[757] de Interoperabilidad de Documento Electrónico, deberán incluir tres componentes: «*a) Contenido, entendido como conjunto de datos o información del documento, b) En su caso, firma electrónica, c) Metadatos del documento electrónico*»[758]. Los metadatos tienen entre otras funciones facilitar la creación, gestión uso y conservación del documento[759], entre los que no se encuentran datos identificativos de los interesados, lo cual ayuda a aminorar los riesgos en la vulneración de sus derechos y es acorde con los principios de minimización de datos.

Finalmente, en relación con la notificación y con la publicación de los actos y resoluciones, es necesario señalar que de acuerdo con el contenido del art. 40.5 de la LPAC[760], las AA.PP. deberán adoptar las medidas que consideren oportunas para salvaguardar el derecho a la protección de datos personales[761], sin perjuicio, del

7760e63fcfef/Guia_NTI_documento_electronico_PDF_2ed_2016.pdf (consulta: 10 de octubre de 2020).

[757] En relación con las normas técnicas del ENI es necesario precisar que fueron emitidas por la Secretaría de Estado de Administraciones Públicas (normas técnicas de interoperabilidad: Política de Firma y Sello Electrónicos y de Certificados de la Administración, Protocolos de intermediación de datos, relación de modelos de datos, gestión de documentos electrónicos y reutilización de recursos de la información) y por la Secretaría de Estado para la Función Pública (normas técnicas de interoperabilidad: documento electrónico, digitalización de documentos, expediente electrónico, de requisitos de conexión a la red de comunicaciones de las Administraciones públicas españolas, de Procedimientos de copiado auténtico y conversión entre documentos electrónicos, de Modelo de Datos para el Intercambio de asientos entre las entidades registrales), las cuales son de obligado cumplimiento de acuerdo con

[758] Apartado III de la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Documento Electrónico.

[759] En el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, se definía a los metadatos como «*cualquier tipo de información en forma electrónica asociada a los documentos electrónicos, de carácter instrumental e independiente de su contenido, destinada al conocimiento inmediato y automatizable de alguna de sus características, con la finalidad de garantizar la disponibilidad, el acceso, la conservación y la interoperabilidad del propio documento*», *vid.* art. 42. Esta definición es tomada en cuenta para la elaboración de las normas técnicas en la materia.

[760] En relación con el contenido de los arts. 44 y 45 de la LPAC.

[761] En su momento el Profesor VALERO TORRIJOS establecía que este tipo de publicaciones debían realizarse de manera que se cumpliese con esa obligación legal, sino que además debían cumplir con otros principios que rigieran su uso y difusión como el de proporcionalidad, *vid.* VALERO TORRIJOS, J., «Implicaciones de la protección de datos de carácter personal para la Administración electrónica», *La protección de datos en la administración electrónica,* Thomson Reuters Aranzadi AEPD, 2009, p. 183. En el contexto actual se debería tener especial atención al cumplimiento del principio de minimización y al de integridad y seguridad por parte de las AA.PP.

ejercicio del derecho de oposición (art. 21 RGPD) por parte de los interesados[762]. La D.A. 7ª de la LOPGDD establece que en el caso de la publicación de un acto podrán utilizar los datos identificativos relativos a nombres y apellidos de los interesados, «*añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse*»; para el caso de las notificaciones infructuosas del art. 44 de la LPAC que requieran un anuncio, «*se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos*».

Con respecto a lo anterior, la AEPD ha adoptado la «Orientación para la aplicación provisional de la Disposición Adicional séptima de la LOPDGDD», en la que se recomienda el uso de los parámetros de forma generalizada. Se seleccionan aleatoriamente las cuatro cifras numéricas para la publicación de los actos y las resoluciones antes descritas. Para el D.N.I. solo se publicarán contando de izquierda a derecha del digito cuarto al séptimo, omitiendo la letra de este (por ejemplo: ***4567**). Para los números de identificación de extranjeros (N.I.E) que cuentan con dos letras, una al inicio y otra al final y siete números de la totalidad de los caracteres alfanuméricos que lo integran se publicarán (contando de izquierda a derecha) de los caracteres quinto al octavo, incluidas ambas letras (por ejemplo, ****4567*). Para el pasaporte solo se publicarán los cuatro últimos dígitos de este, dado que solo cuenta con seis cifras numéricas (por ejemplo, *****3456).

Estas previsiones serán aplicables también para otro tipo de identificaciones. En aquellos casos que el documento en cuestión contenga una serie de al menos siete números se publicarán los cuatro primeros dígitos contados de izquierda a derecha sin tomar en cuenta las letras de estos. Cuando un número de identificación tenga menos de siete dígitos numéricos y esté acompañado de letras, estas se incluirán

[762] Ya que el anterior tratamiento no está basado en el consentimiento de los interesados, el ejercicio del derecho de oposición deberá basarse «*en circunstancias personales que deban prevalecer*», Cfr. VALERO TORRIJOS, J., «Protección de datos…» *op. cit.,* p. 435.

también en el cómputo y solo se publicarán los cuatro últimos dígitos, sean números o letras. Estas orientaciones de carácter provisional tendrán vigencia en tanto sean publicadas otras emitidas por las AA.PP. que desarrollen esta disposición. Por lo que, parecería apropiado que se aplicaran tanto para la publicación de actos o resoluciones como para la notificación si resulta fallida o se tiene que notificar a una pluralidad de interesados.

1.4.5 Comunicación de datos entre Administraciones.

De acuerdo con el art. 4.2 del RGPD, las comunicaciones de datos también deben considerarse tratamientos de datos y, por tanto, están sometidas a la normativa de la materia; cuando el tratamiento realizado por las AA.PP. y fundado en cualquiera de sus bases de licitud esta deberá ser establecida en el derecho nacional, ya sea por la norma que se deba cumplir, en razón de interés público o la que le otorga competencias y potestades a determinada Administración pública. esta ley deberá determinar también la finalidad del tratamiento, pudiendo prever las comunicaciones de datos[763].

[763] En relación con las comunicaciones de datos, inicialmente fueron reguladas a nivel estatal por el art. 21 de LOPD (LO 15/1999), este último precepto señalaba en su redacción original que: «*1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos*», de manera que la cesión estaba condicionada a las normas de creación del fichero o si estuviese previsto así en una norma de rango "superior" o para el cumplimiento de intereses públicos estadísticos o científicos. Este apartado fue objeto de debate y, finalmente la STS 292/2000, de 30 de noviembre lo declaró inconstitucional de hecho se declaró inconstitucional por hacer una remisión en blanco, ya que «*en este punto no ha fijado por sí misma, como le impone la Constitución (art. 53.1 C.E.), los límites al derecho a consentir la cesión de datos personales entre Administraciones Públicas para fines distintos a los que motivaron originariamente su recogida, y a los que alcanza únicamente el consentimiento inicialmente prestado por el afectado (art. 11 L.O.P.D., en relación con lo dispuesto en los arts. 4, 6 y 34.e L.O.P.D.), sino que se ha limitado a identificar la norma que puede hacerlo en su lugar. Norma que bien puede ser reglamentaria, ya que con arreglo al precepto impugnado será una norma de superior rango, y con mayor razón para el caso de que la modificación lo sea por una norma de similar rango, a la que crea el fichero (y ésta basta con que sea una disposición general, que no una Ley, publicada en un Boletín o Diario oficial —art. 20.1 L.O.P.D.) la que pueda autorizar esa cesión inconsentida de datos personales, lo que resulta ser, desde luego, contrario a la Constitución*» (Cfr. F.J. 14); en este sentido la Profesora BUEYO DÍEZ JALÓN determina que la redacción inicial del art. 21.1 de la LOPD facilitaba «*sin control alguno cesiones generalizadas y en masa de datos personales de los ciudadanos*», *Vid.* BUEYO DÍEZ JALÓN, M., «El tratamiento de datos de carácter personal por las Administraciones públicas versus el Derecho Fundamental a la Privacidad: los ficheros públicos», *Revista General de Derecho*

El art. 11 de la derogada LOPD requería de manera genérica para las comunicaciones de datos, sin embargo, también se preveía que pudieran realizarse este tipo de operaciones si la cesión estuviera autorizada por ley, cuando el destinatario de los datos fuese el Defensor del pueblo, el Ministerio Fiscal, el Tribunal de cuentas, jueces o tribunales. Tampoco necesitaban consentimiento si los fines del tratamiento fuesen históricos, estadísticos, científicos y sanitarios. En este último caso, cuando se requiriera solucionar una urgencia de carácter sanitario o epidemiológico. Lo anterior, evidentemente en transposición de la normativa entonces vigente dada por la Directiva 95/46/CE.

La LRJSP se ha adaptado al contenido del RGPD en relación con los tratamientos llevados a cabo por las AA.PP. por disposición del Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones[764]. El cual de manera específica actualiza el marco regulador de las comunicaciones de datos entre administraciones públicas[765]. En

Administrativo, núm. 23, 2010, p. 19. En relación con la comunicación de datos por medios electrónicos entre AA.PP. era regulada por el Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado en su art. 15 se establecía que las transmisiones de datos sustituían a los certificados administrativos en soporte papel, en cuyo caso se requería para dicha transmisión que se requiriera por una autoridad administrativa en la que se debía señalar su finalidad, la identificación de los datos que se requerían y si se realizaba con el consentimiento de los interesados, salvo que no se requiriera (apartado 4). Posteriormente, el RD antes señalado es derogado como consecuencia de la publicación de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, el cual posteriormente es desarrollado de manera parcial por el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos. Ha de ser destacado que, en principio, las Administraciones debían recabar el consentimiento de los interesados para que la Administración ante la cual se realizara el trámite pudiera recabar de otro órgano que contara con dicho documento, este último debía cederlo a través de medios electrónicos en un plazo máximo de diez días (art. 2.1.d del RD 1671/2009).

[764] Apartado 2 del art. 4 del RDL 14/2019, de 31 de octubre.

[765] Cuestión que se relaciona tanto con el Derecho contemplado en el art. 14.1 de la LPAC a relacionarse con las Administraciones públicas, si el ciudadano es una persona física, como con el derecho el derecho de estos a no aportar documentos que ya se encuentren en poder de otra Administración que los haya elaborado, en cuyo caso establece el art. 28.2 de la LPAC «*la Administración actuante podrá consultar o recabar dichos documentos salvo que el interesado se opusiera a ello*», oposición, que no cabe en procedimientos de carácter sancionador o de inspección. Según este sismo apartado deberá llevarse a cabo por medio de las plataformas de intermediación. Este tipo de plataformas están previstas en el ENI y de manera específica están reguladas por la Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Protocolos de intermediación de datos.

consonancia con el principio de cooperación, este artículo permite a las AA.PP. facilitar el acceso a los datos personales de los interesados en su poder a las demás AA.PP., siempre que se especifiquen las condiciones, los protocolos funcionales o técnicos para que la administración pública cesionaria pueda acceder a los datos con «*las máximas garantías de seguridad, integridad y disponibilidad*»[766]. Precisando que, bajo ningún caso la cesión podrá tener lugar si se pretendiera realizar un tratamiento posterior incompatible con los fines para los cuales fueron recogidos los datos personales inicialmente. Así lo entendió en su momento en aplicación con la normativa anterior en la materia el TC en su sentencia 17/2013 de 31 de enero, la que a la letra dice que «*es claro que la Ley Orgánica de protección de datos no permite la comunicación indiscriminada de datos personales entre Administraciones públicas dado que, además, estos datos están, en principio, afectos a finalidades concretas y predeterminadas que son las que motivaron su recogida y tratamiento*»[767]. Sin embargo, no se consideran incompatibles los tratamientos ulteriores con fines de archivo en interés público, estadísticos o fines de investigación sea científica o histórica[768]. A este respecto el Profesor VALERO TORRIJOS determina que bajo este nuevo marco jurídico en la materia (RGPD y LOPDGDD) estos tratamientos de datos tienen como «*premisa inexcusable*» la adopción de «*medidas técnicas y organizativas*

Hay cuatro agentes intervinientes: el cedente, el emisor, el cesionario y el requirente, normalmente estas dos funciones las asumen dos personas, una las primeras dos y la otra las restantes cuando son aceptadas las transmisiones. Funciona de la siguiente manera, el cedente es el responsable de los datos personales, con lo cual puede ser cualquier organización que posea datos relativos a los ciudadanos, pudiendo ser personales o no y cuando facilite datos a otras organizaciones actúa también como emisor. El cedente facilita información un catálogo o registro de sus servicios de intercambio, este es quién determina los protocolos y condiciones de acceso a los servicios de intercambio de datos, métodos de consulta y la información que necesite el requirente. En el caso de rechazar o denegar una solicitud realizada por el requirente tiene el deber de justificar dicha decisión. Si realiza también las funciones de emisor también establece las condiciones técnicas, define clo controles y criterio de acceso para garantizar la confidencialidad, proporciona los datos estrictamente necesarios de manera confidencial, informa sobre la disponibilidad del servicio de intercambio y llevará un registro de las peticiones recibidas con sus respectivas respuestas (Apartado II. Agentes en los intercambios intermediados de datos, de la «Norma Técnica de Interoperabilidad de Protocolos de Intermediación de Datos»). Lo cual es acorde con el control *ex ante* del art. 155 de la LRJSP, ya que no hay un acceso automatizado de interconexión. En relación con lo anterior el Profesor VALERO TORRIJOS califica a ese tipo de accesos como «*tratamientos pueden incurrir en graves contradicciones con los principios generales vigentes en la materia*», *vid.* VALERO TORRIJOS, J., «Implicaciones …» *op. cit.,* pp. 195-196.

[766] Art. 155.1 de la LRJSP.

[767] F.J. 4 de la STC (Pleno) 17/2013, de 31 de enero (RTC 2013\17; ECLI:ES:TC:2013:17).

[768] Apartado 2 del art. 155 de la LRJSP.

que garanticen que el acceso a la información tiene lugar con las máximas garantías de seguridad, integridad y disponibilidad»[769].

Una excepción al principio de limitación de la finalidad se incorpora en el apartado 3 del art. 155 de la LRJSP, por el cual se establece que en tanto una norma especial aplicable al caso concreto no prohíba expresamente su tratamiento posterior para finalidades distintas, se iniciará un procedimiento por el cual la Administración pública cesionaria que pretenda tratar los datos para fines distintos tendrá que comunicárselo previamente a la Administración cedente para que se pronuncie sobre la compatibilidad ulterior del tratamiento en relación los fines para los cuales fueron recabados los datos, esta podrá oponerse motivadamente en un plazo de diez días. En tanto, no se comunique la decisión la Administración cesionaria no podrá utilizar los datos.

Este procedimiento se exceptúa en los casos en que una norma con rango de Ley prevea tratamientos ulteriores con finalidades distintas para los cuales fueron recogidos inicialmente[770]. Ya la sentencia citada anteriormente en el mismo F.J. 4 determinaba que: «*los límites al derecho a consentir la cesión de los datos a fines distintos para los que fueron recabados están sometidos a reserva de Ley*»[771].

En relación con el contenido del art. 155 del RJSP, es importante señalar que el contenido de los apartados 1 y 2 se ajustan a la existente correspondencia entre finalidad del tratamiento y las competencias de las Administraciones. En una ley que permita el tratamiento de datos personales, se determinan las finalidades del

[769] VALERO TORRIJOS, J., «Protección de datos…» *op. cit.,* p. 433.
[770] Apartado 3 *in fine* del art. 155 de la LRJSP.
[771] F.J. 4 de la STC 17/2013, de 31 de enero (RTC 2013\17; ECLI:ES:TC:2013:17). En relación con esto el considerando 31 del RGPD establece que no deben considerarse no deben considerarse destinatarios de datos si reciben datos personales que: «*Las autoridades públicas a las que se comunican datos personales en virtud de una obligación legal para el ejercicio de su misión oficial, como las autoridades fiscales y aduaneras, las unidades de investigación financiera, las autoridades administrativas independientes o los organismos de supervisión de los mercados financieros encargados de la reglamentación y supervisión de los mercados de valores, no deben considerarse destinatarios de datos si reciben datos personales que son necesarios para llevar a cabo una investigación concreta de interés general, de conformidad con el Derecho de la Unión o de los Estados miembros. Las solicitudes de comunicación de las autoridades públicas siempre deben presentarse por escrito, de forma motivada y con carácter ocasional, y no deben referirse a la totalidad de un fichero ni dar lugar a la interconexión de varios ficheros. El tratamiento de datos personales por dichas autoridades públicas debe ser conforme con la normativa en materia de protección de datos que sea de aplicación en función de la finalidad del tratamiento*».

tratamiento relacionadas con las competencias de las AA.PP. El apartado 3 *in fine* se ajusta a la base de licitud por la que las AA.PP. podrán tratar datos con la finalidad de cumplir con una obligación legal.

El apartado 3 de este mismo precepto es quizás la razón por la cual el legislador ha abierto una nueva posibilidad para ajustar la única base del tratamiento que quedaría pendiente, la de cumplir con un interés público, es decir, una administración que tiene conferidas competencias distintas a las de la A.P. cedente puede requerirle su pronunciamiento acerca de la compatibilidad del nuevo tratamiento con los fines iniciales. Este apartado confiere entonces una facultad discrecional de decisión sobre la cesión de los datos otorgada a la A.P. cedente y por tanto esta decisión tendrá ese carácter. Para evitar el abuso de esta facultad discrecional se requerirá entonces una rigurosa justificación de la toma de decisión. Bajo este apartado cabrían también las solicitudes de transmisiones de datos a la AA.PP. que los tenga en su poder para tratamientos ulteriores con fines estadísticos o de investigación científica o histórica, de acuerdo con el art. 89. 1 del RGPD.

Con respecto a la comunicación de datos a particulares, de acuerdo con lo dispuesto en la D.A. 10ª de la LOPDGDD, esta podrá realizarse siempre que los datos hayan sido solicitados por sujetos privados, y cuenten con el consentimiento del interesado. También se prevé la entrega de datos personales si las autoridades públicas enumeradas en el art. 77.1 de la LOPDGDD estimasen que concurre un interés legítimo que prevalente sobre los derechos e intereses de las personas interesadas, de acuerdo con la base de licitud de tratamiento del art. 6.1.f) del RGPD. Al hilo de lo anterior el Profesor Simón Castellano determina que: «*Los órganos y entidades del sector público podrán comunicar los datos de los administrados sujetos de derecho privado que los soliciten cuando cuenten con el consentimiento de los administrados o cuando aprecien que concurre en el sujeto privado solicitante un interés legítimo que prevalezca sobre los derechos e intereses de los administrados concernidos*»[772]. En este último caso, bajo nuestra perspectiva la entrega de datos personales debe llevar aparejada una ponderación previa entre los intereses entre

[772] SIMÓN CASTELLANO, P., «La protección de datos en el sector público…» *op. cit.*

el solicitante y el interesado, de manera que las entregas de los datos sean proporcionales con las finalidades del tratamiento.

1.4.6 Conservación y destrucción de los datos personales.

Cuando los procedimientos administrativos que han dado lugar al tratamiento de datos personales han finalizado, se procede a su archivo. Cada Administración debe contar con un archivo electrónico único que permita que los documentos electrónicos sean conservados en «*un formato que permita garantizar la autenticidad, integridad y conservación, así como su consulta con independencia del tiempo transcurrido desde su emisión*»[773]. Los documentos podrán ser conservados en distintos formatos y soportes que permitan acceder a ellos desde distintas aplicaciones. En relación con los soportes o medios que contengan este tipo de documentos, deberán aplicárseles medidas de seguridad conformes al ENS a fin de que se garantice su «*integridad, autenticidad, confidencialidad, calidad, protección y conservación*»[774], con especial atención a los mecanismos de control de acceso y de identificación de los usuarios que pretendan acceder a tales informaciones. De acuerdo con la Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos se determina que la «*Destrucción o eliminación de los documentos, que atenderá a la normativa aplicable en materia de eliminación de Patrimonio Documental y contemplará la aplicación de las medidas de seguridad relacionadas definidas en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica: Borrado y destrucción del capítulo de "Protección de los soportes de información [mp.si]" y Limpieza de documentos del capítulo de "Protección de la información [mp.info]"*»[775]. En este sentido Guía de aplicación de la Norma Técnica de Interoperabilidad establece que «*El proceso de eliminación de documentos constituye un proceso clave en la gestión de documentos y tiene como objetivo impedir su restauración y posterior reutilización. Para ello, es*

[773] Cfr. Art. 17.2 de la LPAC.
[774] Cfr. Art. 17.3 de la LPAC.
[775] Apartado VI. Procesos de gestión de documentos electrónicos de la Norma Técnica de Interoperabilidad de Política de Gestión de Documentos Electrónicos.

necesario aplicar un proceso que incluya tanto el borrado de la información (el propio documento y sus metadatos) como la destrucción física del soporte, en función de las características del formato y las del propio soporte»[776].

Ahora bien, el art. 17 de la LPAC deja entrever que se deberá aplicar una normativa específica para la gestión documental de los archivos, en este caso debemos de acudir a la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (LPHE) y a la normativa de desarrollo. El art. 49.2 de la LPHE determina que son parte del patrimonio documental, todos los documentos de cualquier época que hayan sido «*generados, conservados y reunidos en el ejercicio de su función por cualquier organismo o entidad de carácter público*». En esta ley se determinan plazos de acceso a los mismos en el artículo 57, a los que haremos referencia en un próximo epígrafe de este trabajo y que pueden servir en determinados casos como parámetros para determinar el plazo de conservación.

Respecto a la eliminación de bienes del patrimonio documental español, el art. 55 establece que deberá ser autorizada por la Administración competente, que sería en el ámbito estatal la AGE o sus organismos públicos. Se entiende como eliminación de acuerdo con su normativa de desarrollo como «*la destrucción física de unidades o series documentales por el órgano responsable del archivo u oficina pública en que se encuentren, empleando cualquier método que garantice la imposibilidad de reconstrucción de los mismos y su posterior utilización*»[777]. La LPHE también restringe la destrucción de documentos si de su existencia se derivase valor probatorio de derechos y obligaciones, tanto de interesados como de la propia Administración. En el ámbito estatal será la Comisión Superior Calificadora de Documentos Administrativos (CSCDA), la que realice el estudio y dictamen de las cuestiones concernientes a la calificación y utilización de documentos, su

[776] Dirección de Tecnologías de la Información y las Comunicaciones (DTIC), «Guía de aplicación de la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos (2ª edición electrónica)», p. 31. Disponible esta publicación en el Portal de Administración Electrónica (PAe): http://administracionelectronica.gob.es/ (consulta 8 de enero de 2021).

[777] *Vid.* art. 2.1 del Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original.

integración en archivos y en materia de accesos e inutilidad administrativa de estos[778].

El procedimiento para determinar si se debe eliminar o conservar la información en otro soporte diferente al original se encuentra regulado en los artículos del cuatro al ocho del Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus organismos públicos y la conservación de documentos administrativos en soporte distinto al original. Ambos procedimientos, tanto el de eliminación como el de conservación se inician por iniciativa propia de la «Comisión Calificadora de Documentos Administrativos» o por los organismos responsables de los documentos, lo anterior está regulado de los artículos cuatro al ocho del referido Real Decreto. Esta comisión es la encargada de acordar en todo caso su iniciación.

En los procedimientos de eliminación deberá constar en el acuerdo que los documentos no tienen valor histórico ni utilidad para le gestión administrativa y que carecen de valor probatorio «para los derechos y obligaciones de las personas físicas o jurídicas»[779]. Respecto a los procedimientos llevados a cabo para la conservación en un formato diferente, el acuerdo debe señalar que el soporte original carece de valor histórico, artístico o que por su carácter relevante se aconseje su conservación y protección, además se hará constar que en el soporte no figuran firmas, expresiones manuscritas que le confieran un valor especial y que su contenido en todo caso carece de valor probatorio. En ambos casos deberán acompañar al acuerdo de iniciación: 1) el informe del órgano proponente que justifique la necesidad de su eliminación o en su caso que se traslade a un soporte distinto, por el cual se analizan «las características históricas, administrativas, jurídicas fiscales

[778] De acuerdo con el art. 58 de la LPHE y con el art. 1 del Real Decreto 1401/2007, de 29 de octubre, por el que se regula la composición, funcionamiento y competencias de la Comisión Superior Calificadora de Documentos Administrativos. De manera específica se encarga de determinar: los plazos de permanencia de los documentos administrativos; las transferencias, una vez cumplido los plazos de permanencia de cada tipo de archivo; la accesibilidad y utilización de los documentos; examinar las propuestas de eliminación de documentos y de conservación en un soporte distinto al de origen; vigilar la correcta aplicación de sus dictámenes y demás cuestiones relacionadas en materia archivística relacionadas con sus competencias, Cfr. Art. 1 del RD 1164/2002, de 8 de noviembre.

[779] Cfr. 4.2 del RD 1164/2002, de 8 de noviembre.

e informativas», además se debe realizar una valoración sobre «los plazos de transferencia, la posible eliminación o expurgo y el régimen de accesibilidad de los documentos» [780], en la que debe indicarse si la documentación incluye datos relativos a la intimidad de las personas, datos personales de carácter sanitario, si su contenido afecta o podría afectar la defensa de la seguridad del Estado y otras características que se consideren específicas como datos personales; 2) una memoria acerca de la documentación en la que se señale su origen, tipo documental, legislación que la origina y su ubicación.

Posteriormente este acuerdo junto con la documentación se remite al Presidente de la Comisión Superior Calificadora de Documentos Administrativos (CSCDA) con la propuesta de eliminación o conservación [781], para que realice un dictamen de carácter preceptivo en el plazo de un año, contado desde que se disponga de la documentación completa, salvo que se aleguen razones de urgencia para la eliminación o cambio de soporte, en cuyo caso se emitirá el dictamen en un plazo inferior al citado.

Cuando el dictamen de la CSCDA resultase contrario a la propuesta de eliminación, tendrá carácter vinculante y no podrá presentarse una nueva propuesta dentro de los dos años siguientes contados desde la comunicación del misma al organismo proponente, a menos que se cambiaran los criterios archivísticos, en cuyo caso la Dirección General del Libro, Archivos y Bibliotecas [782], proponga la realización de una nueva una nueva propuesta. Una vez que se cuente con el dictamen del CSCDA y este fuese favorable, el órgano que tenga bajo su custodia los documentos dictará resolución motivada que deberá ser publicada en el B.O.E. [783]. Su eficacia de acuerdo con el art. 39.2 de la LPAC quedará demorada tres meses desde su publicación en el B.O.E. y, siempre que no se haya interpuesto un recurso administrativo en contra de la resolución, en cuyo caso, se procederá a su

[780] Cfr. Art. 2.2 del RD 1164/2002, de 8 de noviembre.
[781] Lo descrito anteriormente está regulado en el art. 4 del RD 1164/2002, de 8 de noviembre.
[782] Actualmente, Dirección de General de Archivos Estatales, según lo establecido en el inciso e) del aparado 2 y en los incisos x) y y) del apartado 2 del art. 5 del Real Decreto 509/2020, de 5 de mayo, por el que se desarrolla la estructura orgánica básica del Ministerio de Cultura y Deporte.
[783] Cfr. Apartados 1 y 2 del Art. 6 del RD 1164/2002, de 8 de noviembre.

eliminación o al cambio de soporte, hasta que haya adquirido firmeza el acto[784]. En todo caso, cuando se determine la eliminación de la información se deben adoptarán las medidas de protección específicas del ENS[785].

1.5 El equilibrio entre la transparencia y el derecho a la protección de datos.

Antes de profundizar sobre el equilibrio entre el principio de transparencia y el derecho a la protección de datos, conviene señalar el contenido del principio de transparencia, cuál es su encaje legal en nuestro ordenamiento, y su clasificación. En todas las democracias avanzadas este principio resulta fundamental ya que permite conocer a los ciudadanos sobre los asuntos públicos, controlar la toma de decisiones de las autoridades públicas e incentiva y permite la participación ciudadana, sin embargo, como bien señala el Profesor VILLAVERDE MENÉNDEZ «*Resulta paradójico que en casi la totalidad de los sistemas constitucionales contemporáneos de tradición occidental no exista la mención expresa ni a un principio ni a un derecho constitucional a la transparencia, a pesar de ser el instituto jurídico más esgrimido, exigido y manido en el derecho público actual*» [786], ya que en España como en muchas otras constituciones no hay una referencia directa a la transparencia. De cualquier forma, es innegable que la transparencia sea «*una dimensión irrenunciable de la legitimación democrática*» [787]. En este mismo contexto, el Profesor CERRILLO I MARTÍNEZ «*la transparencia consiste en la difusión proactiva de la información relativa a los ámbitos de actuación y las obligaciones de la Administración, con carácter permanente y actualizado, para facilitar su conocimiento así como la participación y*

[784] Apartado 2 del art. 6 del RD 1164/2002, de 8 de noviembre. En cuyo caso se seguirá el procedimiento del art. 7 del mismo R.D.
[785] Concretamente lo establecido en el epígrafe 5.5.5 del anexo II del ENS.
[786] VILLAVERDE MENÉNDEZ, I., «El marco constitucional de la transparencia», *Revista Española de Derecho Constitucional*, núm. 116, 2019, p. 169. El autor considera que la transparencia «*adopta la forma de valor constitucional latente en el principio constitucional "de publicidad"*», continua diciendo que « entre los ensamblajes de la transparencia en el sistema constitucional están el derecho fundamental a recibir libremente información veraz por cualquier medio de difusión [art. 20.1 d) CE], el derecho fundamental a la participación en los asuntos públicos (art. 23.1 CE), el derecho fundamental a la tutela judicial efectiva en su manifestación del derecho a un proceso con todas las garantías en relación con la publicidad de las actuaciones judiciales (art. 24.2 CE y 120.1 CE), el derecho constitucional de acceso a los registros y archivos públicos [art. 105 b) CE], los principios constitucionales de publicidad de las normas (art. 9.3 CE), de las sesiones parlamentarias (art. 80 CE), y los principios democrático y de Estado de derecho (art. 1.1 CE)», Cfr. *Ib.*, p. 170.
[787] *Íd.*

colaboración en los asuntos públicos»[788]. En palabras del CTBG la transparencia «*posibilita el escrutinio público y la fiscalización de la actividad pública, debe constituirse en eje fundamental de la acción política para garantizar la regeneración democrática, la eficacia y eficiencia del Estado y el crecimiento económico*»[789]. En este apartado se tratará la transparencia en relación con el sector público: publicidad activa, acceso a la información y reutilización de datos, y su relación con el derecho a la protección de datos personales.

Primeramente, se tiene que señalar que la transparencia, en específico el acceso a la información pública, se encuentra regulado de forma diferenciada en el ámbito internacional, europeo, comunitario y nacional. El acceso a la información ha tenido un desarrollo más antiguo y profundo en el plano internacional. El artículo 19 tanto de la DUDH como del PIDCP regulan el derecho de las personas a buscar o investigar y a difundir informaciones[790]. El Comité de Derechos Humanos en su «Observación general Nº34» sobre el art. 19 Libertad de opinión y libertad de expresión determina que «*El párrafo 2 del artículo 19 enuncia un derecho de acceso a la información en poder de los organismos públicos. Esta información comprende los registros de que disponga el organismo público, independientemente de la forma en que esté almacenada la información, su fuente y la fecha de producción*»[791]. Este derecho les ha sido reconocido especialmente a los medios de comunicación, debido a la labor que llevan a cabo, pues dan a conocer y difunden informaciones resultado de esa labor de investigación con base en información en poder de las autoridades públicas[792].

El TEDH interpretando el contenido del art. 10 del CEDH ha determinado que no puede leerse como un derecho general de acceso a la información, ni

---

[788] CERRILLO I MARTÍNEZ, A., «Transparencia y buen gobierno en las Administraciones locales de Cataluña: Una aproximación a la Ley 19/2014, de 29 de diciembre», VILLORIA MENDIETA, M. (Dir.). *Buen gobierno, transparencia e integridad institucional en el Gobierno Local.* Ed. Tecnos, Barcelona, 2015, p. 61.
[789] CTBG, Criterio interpretativo 2/2019, de 20 de diciembre, p.7.
[790] En la DUDH literalmente señala que se tiene derecho a «investigar y difundir informaciones», en el PIDCP se señala que se tiene la libertad de «*buscar, recibir y difundir informaciones de toda índole*».
[791] Apartado 18 de la Observación general Nº34, Ginebra 11 a 29 de julio de 2011. Disponible en: http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsrdB0H1l5979OVGGB%2BWPAXiks7ivEzdmLQdosDnCG8FaqoW3y%2FrwBqQ1hhVz2z2lpRr6MpU%2B%2FxEikw9fDbYE4QPFdIFW1VlMIVkoM%2B312r7R.
[792] *Íd.*

correlativamente como una obligación de los Gobiernos a facilitarla[793]. No obstante, el acceso a la información está vinculado al derecho a la libertad de expresión contenido en el art. 10 del CEDH cuando periodistas, defensores de derechos humanos e incluso asociaciones traten de acceder a información de interés público, siempre que la información para su entrega no suponga su reelaboración. Pues estos sujetos hacen de "perros guardianes" de la democracia frente abusos del poder[794]. Como establece el Profesor COTINO HUESO «*para el TEDH, sólo si se dan unos requisitos, el acceso a la información pública forma parte la libertad de expresión e información que reconoce el artículo 10 CEDH*»[795].

La previsión de este derecho a buscar o a investigar y difundir el resultado de esas actividades en estos tratados internacionales obliga a la luz del art. 10.2 de la CE a aplicarlos en ese sentido de manera indirecta en nuestro ordenamiento jurídico. Las sentencias que interpreten su contenido se constituyen como «*criterios interpretativos que determinan el contenido constitucional y perfil exacto*»[796].

En el plano comunitario, el art. 42 de la CDFUE establece el derecho a todo ciudadano de la Unión y a toda persona física o jurídica que resida en el territorio de la UE a «acceder a los documentos de las instituciones, órganos y organismos de la Unión, cualquiera que sea su soporte». Este derecho de acceso ha sido reconocido como un derecho autónomo por el TJUE[797] y aunque pueda pensarse que solamente es aplicable a las instituciones comunitarias, no obstante, debe considerarse el contenido del art. 51 de la propia CDFUE, de manera que su aplicación correspondería también a los Estados miembros siempre y cuando apliquen el Derecho de la Unión[798]. En la actualidad el art.42 de la CDFUE está desarrollado por el Reglamento (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de

[793] Apartado 36 de la STEDH de 17 de febrero de 2015, caso Guseva contra Bulgaria (TEDH 2015\52590) y apartado 74 de la STEDH de 26 de marzo de 1987, caso Leander contra Suecia (TEDH 1987\4).
[794] *Vid.* Apartados 37 y 38 de la STEDH de 17 de febrero de 2015, caso Guseva contra Bulgaria (TEDH 2015\52590) y del apartado 160 al 164 de la STEDH de 8 de noviembre de 2016, caso Magyar Helsinki Bizottság contra Hungría (JUR\2016\260055).
[795] COTINO HUESO, L., «El reconocimiento y contenido internacional del acceso a la información pública como derecho fundamental», *Teoría y realidad constitucional*. Núm. 40, 2017, p. 315.
[796] *Ib.,* p. 316.
[797] Apartado 52 de la STJUE de 18 de julio de 2017 (JUR\2017\199987; ECLI:EU:C:2017:563):
[798] *Vid.* COTINO HUESO, L., *op. cit.,* pp. 289-294.

mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión, por el cual se regulan las situaciones excepcionales por las que se deniega el acceso, el procedimiento de acceso a los documentos, medidas de aplicación, el acceso por medios electrónicos, etc.

Medio año antes, el 12 de enero del año 2001, se publicó en el DOCE (Diario Europeo de las Comunidades Europeas) un reglamento que vendría a compatibilizar a nivel comunitario al derecho de acceso a la información con el derecho a la protección de datos personales. El Reglamento 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, 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, instrumento de aplicabilidad directa, preveía la convergencia entre estos derechos y concretaba qué información debía proporcionarse a los interesados cuando la información hubiera sido o no recabada de los mismos, así como sus limitaciones: la investigación de delitos, seguridad nacional de los Estados miembros, la salvaguardia del interés económico[799]. También se establecía un derecho de acceso en su art. 13 específico en la materia, de manera que el interesado podía conocer de los sujetos responsables, en este caso de las instituciones comunitarias si llevaban a cabo tratamientos con sus datos personales y qué datos eran objeto del tratamiento, las finalidades, las categorías, si se preveían comunicaciones de datos y los criterios que regían el tratamiento automatizado de los mismos. Incluso se crea la figura del Supervisor Europeo de Protección de Datos, autoridad de control independiente encargada de velar por los derechos y libertades fundamentales de las personas físicas frente a los tratamientos llevados a cabo por las instituciones y organismos comunitarios[800].

El Reglamento 45/2001 estuvo vigente durante casi dieciocho años, hasta que fue desplazado por el contenido del Reglamento 2018/1725 del Parlamento Europeo y del Consejo de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las

[799] Cfr. Arts. 11, 12, 13 y 20 del Reglamento 45/2001.
[800] *Vid.* art. 41 del Reglamento 45/2001.

instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) 45/2001 y la Decisión 1247/2002/CE. Este reglamento es aplicable cuando se traten datos por instituciones y organismos de la UE, es decir, excluye de aplicación al RGPD. El mismos no afectaba los derechos y obligaciones de los Estados miembros contenidos en la entonces vigente Directiva 95/46/CE[801].

A nivel nacional, el principio de transparencia se encuentra bajo el amparo del art. 105.b) de la CE, principio rector de las Administraciones públicas. Su ubicación dentro de la Constitución hace que se le niegue de forma sistemática su carácter de fundamental, por no estar incluido en la Sección 1ª del Capítulo II del Título I de la CE, y, por tanto, no goza de las garantías previstas en el art. 53.2 CE[802]. En este sentido la STS de 30 de marzo de 1999 establece que: «*Este precepto constitucional remite expresamente a la configuración legal el ejercicio del derecho de acceso a los archivos y registros administrativos, como derecho no fundamental, aunque relacionado con el derecho de participación política, con el de libertad de información y con el de tutela judicial efectiva. Refleja una concepción de la información que obra en manos del poder público acorde con los principios inherentes al Estado democrático (en cuanto el acceso a los archivos y registros públicos implica una potestad de participación del ciudadano y facilita el ejercicio de la crítica del poder) y al Estado de derecho (en cuanto dicho acceso constituye un procedimiento indirecto de fiscalizar la sumisión de la Administración a la ley y de permitir con más eficacia el control de su actuación por la jurisdicción contencioso-administrativa)*[803]. Por tanto, al estar vinculado al control y a la participación del ciudadano, puede ser considerado como un medio de vigilancia que le permita conocer si las administraciones públicas realizan su función tal y como ordena el art. 103 de la CE.

[801] Considerando 18 del Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, 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

[802] ROLLNERT LIERN, G., «El derecho de acceso a la información pública como derecho fundamental: una valoración del debate doctrinal a propósito de la Ley de Transparencia», *Teoría y realidad constitucional,* núm. 34, 2014, pp. 350-351.

[803] F.D. 3º de la STS de 30 de marzo de 1999 (RJ\1999\3246; ECLI:ES:TS: 1999:2206).

Este Alto Tribunal ya ha tenido ocasión anteriormente de vincular el contenido de este derecho de configuración legal con otros derechos de corte fundamental, por ejemplo, en el caso que se pretenda comprobar la veracidad de informaciones en manos de la Administración: «*Este derecho a comprobar la veracidad de una información es un derecho derivado del artículo 20.1.d), pero que es imprescindible conectar en el caso examinado con el derecho establecido por el artículo 105.b), que concierne al acceso a los ciudadanos a los archivos y registros administrativos*», continua diciendo que «*La interpretación de las normas del ordenamiento jurídico, incluyendo las de la Constitución, no puede verificarse aisladamente, pensando que cada precepto constituye una unidad propia, que no se relaciona con los demás aplicables al caso. En el supuesto enjuiciado, ejercitándose estrictamente el derecho a tener acceso a los archivos y registros administrativos, no es posible negar la conexión del artículo 20.1.d) con el artículo 105.b)*»[804].

El derecho de acceso a archivos y registros fue desarrollado por el art. 37 de la hoy derogada LRJPAC, de forma bastante limitada, ya que genéricamente las personas interesadas solo podían tener acceso a los registros y documentos en procedimientos ya concluidos a fecha de la solicitud. Si se pretendía acceder a documentos que tuvieran solo datos de carácter nominativo, con exclusión de aquellos de carácter sancionador o disciplinario, solo podían acceder a ellos los interesados y aquellas personas que acreditaran un interés legítimo y directo.

El artículo antes referido limitaba el acceso cuando la autoridad competente alegara razones de interés público, intereses de terceros más dignos de protección o por disposición legal. Además, excluía el acceso si los documentos contenían: información sobre las actuaciones del Gobierno del Estado de las CCAA no sujetas al Derecho administrativo, informaciones relacionadas con la defensa o seguridad nacional, informaciones sobre la investigación de delitos siempre que supusieran peligro a la protección de derechos y libertades de terceros, informaciones protegidas por el secreto comercial o industrial, las relacionadas con la política monetaria y, todas aquellas informaciones que afectasen la eficacia del funcionamiento de los servicios públicos. Igualmente, en este artículo tampoco se

[804] F.D. 4º de la STS de 19 de mayo de 2003 (RJ 2003\3834; ECLI: ES:TS: 2003:3359).

establecía un procedimiento para la tramitación de dichas solicitudes, lo que ocasionó fácticamente problemas en la forma de acceder a la misma.

Posteriormente y después de poco más de veinte años de vigencia de la LRJPAC, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIBG), vio la luz. Tal y como establece el Profesor RAZQUIN LIZARRAGA «*Esta Ley alcanza tanto a la transparencia "activa" o publicidad, como al derecho de acceso de los ciudadanos a la información pública o transparencia "pasiva"*»[805]. Estable una diferenciación entre una y otra, tanto de su contenido como de sus límites. Esta norma tiene carácter básico de acuerdo con su Disposición Final Octava, salvo lo relativo a la Administración General del Estado y al Consejo de Transparencia y Buen Gobierno. En buena parte casi todas las CCAA han realizado un desarrollo normativo en la materia[806].

De manera genérica, y a grandes rasgos, la transparencia activa consiste en que determinados sujetos obligados publiquen datos sobre su funcionamiento, organización, normativa aplicable e información económica, presupuestaria y estadística[807]. La transparencia pasiva es traducida en el derecho que tienen los ciudadanos a acceder a la información pública que posean las autoridades sujetas al

[805] RAZQUIN LIZARRAGA, M. M., *op. cit.,* p. 141.
[806] Salvo el País Vasco, todas las CCAA cuentan con una ley en la materia: Ley 10/2019, de 10 de abril, de Transparencia y de Participación de la Comunidad de Madrid; Ley 8/2018, de 14 de septiembre, de Transparencia, Buen Gobierno y Grupos de Interés. Comunidad Autónoma del Principado de Asturias; Ley 1/2018, de 21 de marzo, de Transparencia de la Actividad Pública. Comunidad Autónoma de Cantabria; Ley Foral 5/2018, de 17 de mayo, de Transparencia, acceso a la información pública y buen gobierno; Ley 4/2016, de 15 de diciembre, de Transparencia y Buen Gobierno de Castilla-La Mancha; Ley 1/2016, de 18 de enero, de transparencia y buen gobierno. Comunidad Autónoma de Galicia; Ley 3/2015, de 4 de marzo, de Transparencia y Participación Ciudadana de Castilla y León; Ley 8/2015, de 25 de marzo, de Transparencia de la Actividad Pública y Participación Ciudadana de Aragón; Ley 2/2015, de 2 de abril, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana; Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía; Ley 3/2014, de 11 de septiembre, de Transparencia y Buen Gobierno de La Rioja; Ley 12/2014, de 16 de diciembre, de Transparencia y Participación Ciudadana de la Comunidad Autónoma de la Región de Murcia; Ley 12/2014, de 26 de diciembre, de transparencia y de acceso a la información pública. Comunidad Autónoma de Canarias; Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno. Comunidad Autónoma de Cataluña; Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura; Ley 4/2011, de 31 de marzo, de la buena administración y del buen gobierno de las Illes Balears. Desde 2015 se está gestando Ley de Transparencia, Participación ciudadana y Buen Gobierno del Sector público vasco, sin que aún vea la luz. Sin embargo, esta Comunidad Autónoma cuenta con un órgano específico que se encarga de realizar el control de transparencia al amparo de la D.A. 4º de la Ley 19/2013 (art. 1 del Decreto 128/2016, de 13 de septiembre, de la Comisión Vasca de Acceso a la Información Pública).
[807] Aquellos enumerados en los arts. 2, 3 y 4 de la LTAIBG.

ámbito de aplicación de la ley. La Audiencia Nacional señala que «*la principal diferencia entre el acceso a la información y la publicidad activa radica en que la primera se realiza mediante solicitud individualizada (artículo 17 de la Ley 19/2013) mientras que la segunda permite el acceso generalizado a la información (artículo 5 de la misma Ley)*[808]*.* Esta doble fórmula sin duda robustece las herramientas hasta ahora existentes utilizadas en contra de la corrupción y la rendición de cuentas[809].

Los sujetos obligados al cumplimiento normativo con aquellos contemplados en el art. 2.1 de la LTAIBG[810]. A efectos de esta ley se consideran como Administraciones públicas a las administraciones territoriales, a las entidades gestoras y servicios comunes de la SS, a los organismos autónomos, Agencias y otras entidades investidas de independencia funcional o autonomía por ley y que tengas atribuidas funciones de supervisión o regulación y, a las entidades con personalidad jurídica propia que estén vinculadas o sean dependientes de cualquier Administración pública, «*incluidas las Universidades*», de acuerdo con el contenido del art. 2.2 de la LTAIBG.

Existen otros sujetos que la LTAIBG considera como «cooperadores» por no tener una obligación directa de publicar información ya que estos no son una Administración pública, no pertenecen al sector público institucional o demás

[808] F.D. 5º de la SAN de 26 de marzo 2019 (JUR\2019\201813; ECLI:ES:AN:2019:2386).

[809] MARTÍN DELGADO, I., «La configuración legal de las autoridades de transparencia», MARTÍN DELGADO, I., GUICHOT REINA, E. y CARRILLO I MARTÍNEZ, A., *Configuración legal, actuación y funciones de las autoridades de transparencia. Algunas propuestas de mejora,* Ed. MIC, Barcelona, 2019, p. 16

[810] Son sujetos obligados de acuerdo con este precepto: a) las Administraciones territoriales, el sector público institucional; b) las entidades gestoras y los servicios comunes de la Seguridad Social, mutuas de accidentes y enfermedades de trabajo colaboradoras de la Seguridad Social; c) los organismos autónomos, las Agencias Estatales, las entidades públicas empresariales y entidades de derecho público que tengan reconocida independencia funcional o con especial autonomía y tengan atribuidas funciones de regulación o supervisión; d) las entidades de derecho público con personalidad jurídica propia vinculas a cualquiera de las Administraciones públicas o dependientes de ellas, incluidas las Universidades; e) Las corporaciones de Derecho público; f) la Casa real, el Congreso de los Diputados, el Senado, el Tribunal Constitucional, el Consejo General del Poder Judicial, el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, en relación con sus actividades sujetas a Derecho Administrativo; g) las sociedades mercantiles con participación directa o indirecta superior al 50 por 100; h) las fundaciones sujetas a la legislación de esa materia, i) asociaciones constituidas por las Administraciones, organismos, entidades y órganos de cooperación. Igualmente tendrán condición de sujetos obligados de acuerdo con el art. 3 de la misma ley: los partidos políticos, sindicatos y organizaciones empresariales, sujetos que «*tienen constitucionalmente asignado un rol esencial en el funcionamiento de nuestro sistema democrático*» (Cfr. CTBG, Criterio interpretativo 3/2019, de 20 de diciembre, p.59) a pesar de ser organizaciones de carácter privado.

sujetos obligados de la misma, son personas físicas o jurídicas que prestan servicios públicos o ejercen potestades administrativas, incluidos los adjudicatarios de contratos, obligados a proveer información a la Administración, organismo o entidad al que estén vinculadas, para que estos a su vez puedan cumplir con las obligaciones legales que les impone la LTAIBG, previo requerimiento, de acuerdo con el art. 4 de la referida norma legal.

El derecho de transparencia en sus dos formas tanto la activa como la pasiva tiene los mismos límites [811]: la seguridad nacional, la defensa, las relaciones exteriores, la seguridad pública, la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios, la igualdad entre partes en procesos judiciales y de tutela judicial efectiva, funciones administrativas de vigilancia y control, intereses económicos y comerciales, la política económica y monetaria, el secreto profesional, intelectual e industrial, los secretos en la toma de decisiones, la confidencialidad, la protección del medio ambiente y la protección de datos personales casi todos establecidos en el art. 14 de la LTAIBG, a excepción del derecho a la protección de datos personales, contemplado en el art. 15. A este hay que sumarle otros derechos constitucionalmente protegidos como la intimidad de las personas, límite previsto en el propio art. 105.b) Constitucional.

El límite del derecho a la protección de datos se aplica de manera directa [812] en relación con las obligaciones de publicidad activa, la propia LTAIBG establece qué información están obligadas a publicar los sujetos del art. 2.1 de la LTAIBG, relacionada con su actividad. En el caso del acceso a la información se deberá llevar a cabo una la ponderación de estos dos derechos aplicado al caso concreto, conocido también como «test de daño», si finalidad es evaluar si la estimación de una petición de información «*supone un perjuicio concreto, definido y evaluable*» [813]. En palabras de CERRILLO I MARTÍNEZ el equilibrio de estos dos derechos se plantea complicado ya que «*Por un lado, la transparencia persigue facilitar el conocimiento público de la*

[811] Conforme al criterio interpretativo del CTBG y la AEPD 002/2015, de 24 de junio, aplicación de los límites al derecho de acceso a la información, p. 4.
[812] A contrario sensu de los establecido en el Criterio interpretativo del CTBG y la AEPD 002/2015, de 24 de junio, «Aplicación de los límites al derecho de acceso a la información», p. 5.
[813] *Íd*.

información. Por otro, la protección de datos personales impide o limita su difusión a la concurrencia de determinadas circunstancias»[814].

El artículo 15 de la LTAIBG legalmente modula la relación entre el derecho a la protección de datos y la transparencia, siendo el primero límite del segundo. En concreto este límite es aplicable a los dos mecanismos por los cuales se lleva a cabo la divulgación de la información, sin embargo, la modulación en ambos es distinta, dependiendo principalmente del tipo de datos que se tratan, los medios por los cuales se dé a conocer la información y si los sujetos responsables han aplicado a la información que tratan algún tipo de mecanismo que impida su identificación.

Las administraciones públicas, el sector público institucional y aquellas personas físicas o jurídicas que presten servicios públicos, incluidos los adjudicatarios de contratos del sector público tratan datos personales en cantidades ingentes. Las Administraciones públicas y el sector público, genéricamente encuentran su base de licitud en el contenido de los incisos c) y e) del art. 6.1 del RGPD[815]. En el caso de las personas físicas o jurídicas que presten servicios públicos, además de regirse por su por su normativa específica, encuentran la licitud del tratamiento de datos personales en el cumplimiento de una misión realizada en aras de un interés público, como la prestación de un servicio (finalidad del tratamiento), y, por tanto, sujetos a obligaciones específicas de servicio público, convirtiéndose en encargados del tratamiento[816].

Estos sujetos obligados en el cumplimiento de sus obligaciones legales establecidas en la LTBG tratan datos de carácter personal de distinta naturaleza. La protección de datos personales dentro de la ley LTAIBG según el Profesor GUICHOT REINA[817], confiere tres círculos de protección con una protección diferenciada en

---

[814] CERRILLO I MARTÍNEZ, A., «El difícil equilibrio entre transparencia pública y protección de datos personales», *Cuadernos de derecho local*, núm. 45, 2017, p. 136.

[815] De acuerdo con el apartado II del informe 175/2018 de la AEPD. Disponible en: https://www.aepd.es/es/documento/2018-0175.pdf

[816] Aunque actúa por cuenta de otro y se traten datos para el cumplimiento de un contrato, los datos que se van a tratar no son los del contratista sino de los usuarios del servicio que gestionan, por tanto, la base del tratamiento no puede ser el inciso b) del art. 6.1 del RGPD. A lo que se le debe sumar que los fines del tratamiento cuando se presta un servicio público vienen delimitados por una norma de rango legal, que autoriza este tipo de contratos y que conforme con lo establecido en el 33.2 la posición jurídica del prestador de servicios públicos sería el encargado del tratamiento.

[817] GUICHOT REINA, E., «Transparencia y protección de datos en las Universidades Públicas», *Revista Española de Derecho Administrativo,* nº 193, p. 91-92.

cada uno de ellos con base en el art. 15 de la misma norma. En el círculo más amplio se encuentran los datos personales que contienen datos meramente identificativos, también llamado «circulo externo». Después encontramos un «círculo medio» dónde encontramos datos personales genéricos, es una especie de círculo residual, en el que se hayan datos personales que no pertenecen al círculo anterior ni datos del «círculo interno» en el que se contienen los datos especialmente protegidos o también llamados de categorías especiales[818].

De acuerdo con el RGPD y la LOPDGDD los datos personales son clasificados en «datos personales» y «datos personales de categorías especiales»[819]. Los datos de categorías especiales (art. 9.1 RGPD) a la luz de la normativa de la LTAIBG pueden a su vez dividirse en dos grupos, en el primero se encuentran aquellos que puedan revelar la ideología, afiliación sindical, religión o creencias religiosas de las personas; en el segundo grupo, estarían los datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluidos los datos genéticos o biométricos, y también aquellos que contuvieran datos relacionados con la comisión de infracciones penales o administrativas que no conllevasen amonestación pública al infractor.

El contenido del circulo residual y del circulo externo a los que hace referencia el Profesor GUICHOT REINA, desde la perspectiva de la normativa de protección de datos serían datos personales genéricos (art. 3.1 RGPD), ya que el RGPD no habla de datos meramente identificativos y la LOPDGDD tampoco los regula de manera directa. La modulación de este tipo de datos a la luz de la LTAIBG es distinta y en buena medida depende del contenido de la información, es decir, si los datos son o no meramente identificativos. Con el nuevo marco normativo en protección de datos, estos datos genéricos tienden a minimizarse por defecto incluso antes de comenzar su tratamiento teniendo en cuenta siempre las finalidades y su base de licitud.

Los datos personales tanto de categorías especiales como genéricos pueden ser recabados directamente del interesado o no, y dependiendo del caso se le tendrá

[818] *Íd.*
[819] Art. 4.1 y 9.1 del RGPD

que proporcionar determinada información descrita en los arts. 13 y 14 del RGPD, respectivamente. De cualquier forma, cuando se vaya a realizar algún tratamiento de datos de cualquier tipo, se debe cumplir con el principio de transparencia regulado en el art. 12 del RGPD. Consecuentemente la información que se proporcione al interesado deberá ser de manera concisa, transparente, inteligible, de fácil acceso, con lenguaje claro y sencillo por escrito u otros medios, (preferentemente electrónicos) en relación con sus derechos contemplados del art. 15 al 22: acceso, rectificación, supresión, acerca de las limitaciones del tratamiento, portabilidad, oposición, a saber si se toman decisiones individuales automatizadas , sobre las violaciones o probables violaciones de la seguridad de los datos personales. Igualmente, se les deberá dar a conocer la identidad y los datos de contacto del responsable, los datos del contacto del DPD, los fines del tratamiento, plazo de conservación. En su caso, si la recogida de datos es una obligación o un requisito legal y las consecuencias de no facilitarlos.

De acuerdo con el Criterio interpretativo del CTBG y la AEPD 004/2015, de 23 de julio de 2015, «Publicidad activa de los datos del DNI y la firma manuscrita», son considerados datos meramente identificativos: el nombre, apellidos, dirección o teléfono, así como «*otros datos que identifican la posición del afectado dentro de la organización administrativa, como los relacionados con la identificación de rango o puesto de trabajo*»[820]. En este sentido el Profesor RAZQUIN LIZARRAGA dispone que aquellos otros datos «*que excedan de lo anterior ya no son datos meramente identificativos y se incardinan en el tipo anterior de datos personales no sensibles. Así, pues, los datos como el número de DNI de NIF o de pasaporte, el domicilio, el correo electrónico o el número de móvil no son datos meramente identificativos*»[821].

El límite del art.15 y los parámetros de ponderación no serán aplicables a los datos que son disociados[822] cuando deba ser entregada con motivo de una solicitud. El límite del art. 15 también es aplicable si ha de publicarse información en el portal de transparencia por un sujeto obligado en la LTAIBG y contenga datos de categorías

[820] Criterio interpretativo del CTBG y la AEPD 004/2015, de 23 de julio de 2015, «Publicidad activa de los datos del DNI y de la firma manuscrita», p. 5.
[821] RAZQUIN LIZARRAGA, M. M., *op. cit.,* p. 155.
[822] Cfr. Arts. 5.3, 15.4 y 24 de la LTAIBG.

especiales. En relación con el primero de los casos, se entiende por disociar el procedimiento por el cual se separan los datos personales de la información dónde se contenían, como consecuencia hace que los titulares de la información se vuelvan anónimos, a este procedimiento se denomina anonimización. Mediante este proceso «*se deberá producir la ruptura de la cadena de identificación de las personas*»[823] y su finalidad es «*eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales. Un análisis masivo de los datos o macrodatos que puedan derivar de los datos anonimizados no debería diferir del análisis que pudiera obtenerse si hubiera sido realizado con datos no anonimizados*»[824]. Si la anonimización pudiera garantizarse al cien por cien, solo en ese caso, implicaría la inaplicación de la normativa en materia de protección de datos, pues no sería posible ya identificar a las personas[825].

No obstante, suele ser habitual que no se rompa esa «cadena de anonimización», bien por microdatos que permiten la identificación directa o por aquellos que permiten indirectamente de manera cruzada la identificación. En ese caso le seguiría siendo de aplicación la normativa en materia de protección de datos. Como solución a esta problemática, bien podría no incorporar metadatos relacionados con la identidad de las personas, como medida de minimización establecida en el actual marco normativo vigente. Posteriormente, si se estimase necesario utilizar distintas técnicas de anonimización como el uso de algoritmos, sellos de tiempo o anonimización por capas, si es necesario de forma simultánea.

Se podría recurrir a la seudonimización como buena práctica antes de efectuar la anonimización de datos en caso de que sea posible, «*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*

[823] AEPD, Orientaciones y garantías en los procedimientos de anonimización de datos personales, p. 2.
[824] *Íd.*
[825] *Ib.,* p. 5.

y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable»[826]. No olvidemos que los sujetos responsables del tratamiento de datos son autoridades públicas y muchas veces para el ejercicio de sus competencias y la emisión de actos jurídicos requieren que la información sea atribuible a un sujeto determinado, si estos seudonimizaran la totalidad de los datos personales que tuvieran en su poder, tendrían que acudir constantemente a la información localizada de manera separada para atribuirla de manera plena a determinado sujeto. Sin embargo, este acceso no puede ser indiscriminado por todos los funcionarios, en este caso solo deberían tener acceso aquellos que realicen determinadas funciones como la de inspección y de instrucción en materia de sanciones, o, cuando sea necesario para dejar constancia de la prestación de un servicio como es el caso del ámbito sanitario, por ejemplo, solo determinado personal podrá tener acceso a la historia clínica del paciente. Lo anterior nos hace pensar que esta medida puede ser complementaria y compatible con las ya contenidas en el Sistema Nacional de Seguridad, de acuerdo con la D.A. 1ª de la LOPDGDD.

1.5.1 La publicidad activa en relación con el derecho a la protección de datos personales.

La transparencia activa o «publicidad activa» no está definida por la LTAIBG, sin embargo, de su regulación legal se puede inferir su contenido, es una «*obligación de los sujetos que determina la Ley de publicar, de forma proactiva y en las condiciones establecidas, los datos o informaciones que sean relevantes para garantizar la transparencia de su actividad y, en todo caso, los designados expresamente en la norma, con vistas a posibilitar el ejercicio por la ciudadanía de su derecho a la participación y al control de los asuntos públicos*»[827]. A nivel estatal está regulada por la LTAIBG, concretamente por el contenido de su Capítulo II (arts. 5 al 11). Como bien señala GARCÍA MORALES es la primera norma de aplicación estatal en regular

[826] Art. 4.5 del RGPD.
[827] CTBG, Criterio interpretativo 2/2019, de 20 de diciembre de 2019, p. 11. En este mismo sentido Cfr. VILLORIA MENDIETA, M. y CRUZ-RUBIO, C.N., «Gobierno abierto, transparencia y rendición de cuentas: marco conceptual», VILLORIA MENDIETA, M. (Dir.), *Buen gobierno, transparencia e integridad institucional en el Gobierno Local.* Ed. Tecnos, Barcelona, 2015, p. 91.

aquellas obligaciones mínimas del lado más visible de la transparencia[828]. Los sujetos obligados a observar la aplicación de la LTAIBG genéricamente deben publicar de forma proactiva información referente a su actividad. Desde la perspectiva del derecho a la protección de datos, este tratamiento encuentra su base de licitud en el cumplimiento de las obligaciones legales establecidas en la LTAIBG, de acuerdo con el art. 6.1.c) del RGPD.

La LTAIBG también contiene obligaciones concretas de publicar determinada información que puede ser dividida en cuatro bloques[829]: 1) información institucional, organizativa y de planificación, 2) información de relevancia jurídica, 3) información económica y, 4) la información relativa al inventario de actividades de tratamiento de datos personales.

Son sujetos obligados en el primero de los bloques las Administraciones públicas, el sector público institucional, la Casa Real, el Congreso de los Diputados, el Senado, el Tribunal Constitucional, el Consejo General del Poder Judicial, el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, en relación con sus actividades sujetas a Derecho Administrativo[830], así como partidos políticos, organizaciones sindicales, organizaciones empresariales, entidades privadas[831] y, personas físicas y jurídicas que presten servicios públicos o ejerzan potestades administrativas[832]. De acuerdo con el art. 6 de la LTAIBG la información que deben publicar los sujetos antes descritos comprenderá aquella información sobre sus funciones y su normativa de aplicación, incluido un organigrama en el cual se

---

[828] GARCÍA MORALES, M.J., *Transparencia y rendición de cuentas de las relaciones de cooperación intergubernamental en el Estado autónomico,* Generalitat de Catalunya. Institut d´Estudis de l´Autogovern Palau Centelles, Barcelona, 2017, p. 80. Sin embargo, cabe destacar previa publicación de la LTAIBG ya existían dos leyes autonómicas, la de las Islas Baleares («BOIB» núm. 53, de 09/04/2011, «BOE» núm. 103, de 30/04/2011) y la de la Comunidad Autónoma de Extremadura («DOE» núm. 99, de 24/05/2013, «BOE» núm. 136, de 07/06/2013) que regulaban la transparencia activa en su ámbito competencial.

[829] Del art. 6 al 8 de la LTAIBG.

[830] Art. 2 de la LTAIBG en relación con el art. 6.1 de la referida ley.

[831] De conformidad con lo establecido en el art. 3 de la LTAIBG. En el caso de las entidades privadas que perciban ayudas o subvenciones de una cuantía superior a los 100.000 euros o si al menos el 40% de sus ingresos provienen de ayudas o subvenciones que tengan una cuantía mínima de 5.000 euros.

[832] En este caso la publicidad activa se llevará a cabo por la Administración, administración o entidad a la que se encuentren vinculadas, previo requerimiento. Se incluyen dentro de este apartado los adjudicatarios de contratos del sector público, de acuerdo con el art. 4 de la LTAIBG.

identifique a los responsables, su correspondiente perfil y trayectoria. Las Administraciones bajo este apartado deberán incluir en este tipo de información sus planes, programas anuales y plurianuales, objetivos, sus actividades, los medios y el tiempo estimado para su realización.

El segundo de los bloques contiene información referente a todos aquellos instrumentos jurídicos que supongan una interpretación del derecho o tengan efectos jurídicos, incluidas las memorias e informes que integren los expedientes de elaboración de estos, además de los anteproyectos de leyes, proyectos de decretos legislativos o reglamentos, y aquellos documentos que de acuerdo con las leyes sectoriales deban ser sometidos a información pública durante su tramitación[833]. Esta obligación solamente les será aplicable a las Administraciones públicas, entendidas como tal en la LTAIBG, es decir, aquellas comprendidas entre el inciso a) al d) del art. 2.1, con base en el art. 2.2 y al art. 7 de la referida ley.

Los sujetos obligados en el tercer bloque de información son los mismos que los del bloque primero, sin embargo, la información que deberán hacer pública será la relacionada con sus actos de gestión administrativa que tengan repercusión económica o presupuestaria como contratos, convenios, subvenciones, ayudas públicas, presupuestos, cuentas anuales, retribuciones percibidas por los altos cargos, indemnizaciones, resoluciones de autorización o reconocimiento de compatibilidad de sus empleados públicos, las autorizaciones del ejercicio de la actividad privada e información estadística que hagan saber el grado de cumplimiento y la calidad de los servicios públicos. Los representantes locales además deberán hacer públicas sus declaraciones anuales de bienes y actividades. También las Administraciones públicas tendrán que publicar la relación de sus bienes en propiedad o sobre los cuales ostenten algún derecho real[834].

El último bloque ha sido recientemente introducido como consecuencia de la aplicación del RGPD y de la LOPDGDD[835], como hemos mencionado anteriormente, los responsables del tratamiento de datos enumerados en el art. 77.1 de la

[833] Cfr. Art. 7 LTAIBG.
[834] Con base en el art. 8 de la LTAIBG.
[835] Cfr. art. 30 del RGPD y en el art. 31.2 de la LOPDGDD.

LOPDGDD[836] están obligados a llevar a cabo un registro de los tratamientos de datos personales que efectúan. El art. 6 bis de la LTAIBG además los obliga a publicar su inventario de actividades de tratamiento, el cual debe contener el nombre y datos del responsable, el nombre del delegado en protección de datos, los fines del tratamiento, las categorías de interesados y de los datos personales, las categorías de destinatarios a quienes se comunicarán o se comunicaron datos personales, si es posible el plazo de supresión por categorías de datos personales, y las medidas técnicas y organizativas, que en el caso del sector público deberán ajustarse al ENS. De acuerdo con el Criterio interpretativo 3/2019 de 20 de noviembre del CTBG, quedan excluidos del ámbito de aplicación del Título I de la LTAIBG, los Órganos Jurisdiccionales y Grupos Parlamentarios de las Cortes Generales y de las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales, incluidos en los incisos b) y k) del art. 77.1, de manera que no están incorporados en el listado de sujetos obligados a la LTAIBG en su art. 2.1, y por tanto, «*únicamente están vinculados al cumplimiento de una obligación en la materia: la específicamente prevista en el nuevo art. 6 bis de la Ley de publicar proactivamente sus inventarios de actividades de tratamiento de datos de carácter personal*».[837]

Parece idóneo y casi evidente que los ciudadanos puedan tener acceso a este tipo de informaciones por medios electrónicos, a través de un «Portal de transparencia», entendiéndose como tal, al sitio web creado con la finalidad de cumplir con las obligaciones de transparencia activa derivadas de la legislación en la materia[838]. Como bien señala la Profesora GARCÍA MORALES «*La transparencia*

[836] Las autoridades enumeradas en el art. 77.1 de la LOPDGDD son las siguientes: «*a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos, b) Los órganos jurisdiccionales, c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local, d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas, e) Las autoridades administrativas independientes, f) El Banco de España, g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público, h) Las fundaciones del sector público, i) Las Universidades Públicas, j) Los consorcios y, k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales*».

[837] CTBG, Criterio interpretativo 003/2019, de 20 de diciembre, p. 89.

[838] El portal de transparencia solo es obligatorio para la AGE, de acuerdo con el art. 10 de la LTAIBG. Los Profesores MESEGUER YEBRA, J. y IBÁÑEZ PASCUAL, A. haciendo referencia al Portal de transparencia determinan que «*Esta cuestión, sin embargo, puede tener una importancia secundaria o relativa, limitada únicamente a la denominación del instrumento que garantiza el cumplimiento de las*

entendida como forma de hacer pública información mediante medios electrónicos pretende empoderar al ciudadano y darle competencias para examinar la acción de sus gobiernos y participar en asuntos públicos»[839]. Resulta adecuado, por no decir necesario, que se creen este tipo de sitios web a fin de tener concentrada en un mismo lugar toda la información que los sujetos enumerados en los arts. 2 y 3 de la LTAIBG, así como los del art. 77.1 de la LOPDGDD (en relación con el registro de actividades del tratamiento de datos personales) estén obligados a publicar. Se debe procurar además que su estructura sea intuitiva, de fácil localización y que preferentemente dispongan de un buscador propio «*para facilitar el acceso rápido y comprensible a la información. Así mismo, deben organizar la información de manera que sea fácilmente accesible y ordenada temáticamente y cronológicamente*»[840]. También sería válida la opción de publicar la información en el portal web o sede electrónica del sujeto obligado en un apartado específico y visible, sin embargo, no lo considero adecuado para aquellos sujetos obligados que no sean considerados como Administraciones públicas dada su organización administrativa[841]. No

obligaciones de publicidad activa, ya el art. 5.4 de la LTAIP sí obliga a todos los sujetos a que la información sea publicada en las correspondientes sedes electrónicas o páginas web. Recordemos que esta conjunción "o", vino a sustituir a "y", que aparecía en las dos primeras versiones del texto normativo, una vez preciadas dos cuestiones: la falta de justificación para que un mismo contenido apareciera publicado en dos espacios diferentes y, aún más importante, la imposibilidad de que algunos de los sujetos obligados por ley poseyeran sede electrónica dada su naturaleza», cfr. MESEGUER YEBRA, J. y IBÁÑEZ PASCUAL, A., «Capítulo I. Transparencia y acceso a la información pública en el nuevo contexto de la administración electrónica», PINTOS SANTIAGO, J. (Dir.), *La implantación de la Administración electrónica y de la e-factura,* Wolters Kluwer, Madrid, 2017, p. 38.

[839] GARCÍA MORALES, M.J., *op. cit*., p. 316.

[840] CERRILLO I MARTÍNEZ, A., «Transparencia…» *op. cit*., p. 62.

[841] Es preciso recordar en este momento qué se entiende por «sede electrónica» y dónde está regulada. Está regulada en el art. 38.1 de la LRJSP en el que se establece que: «*es aquella dirección electrónica, disponible para los ciudadanos a través de redes de telecomunicaciones, cuya titularidad corresponde a una Administración Pública, o bien a una o varios organismos públicos o entidades de Derecho Público en el ejercicio de sus competencias*». El Profesor VALERO TORRIJOS ha determinado al respecto que «*la sede electrónica no es más que una prolongación virtual de las oficinas administrativas tradicionales, servidas por personal administrativo y a las cuales pueden dirigirse presencialmente -o incluso a través de otros medios como el teléfono- los ciudadanos para obtener información o realizar actuaciones administrativas*», cfr. VALERO TORRIJOS, J., «Acceso a los servicios y a la información por medios electrónicos», VALERO TORRIJOS, J. y GAMERO CASADO, J. (Coords.), *La ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos,* Thomson Reuters Aranzadi, Madrid, 2008, p. 273. En este contexto cabe señalar que, la mayoría de las CCAA han optado por el modelo de sede electrónica y así se prevé en las distintas leyes autonómicas en la materia: art. 29 de la Ley 10/2019, de 10 de abril, de Transparencia y de Participación de la Comunidad de Madrid; art. 39 de la Ley 1/2018, de 21 de marzo, de Transparencia de la Actividad Pública, de la Comunidad Autónoma de Cantabria; art. 11 de la Ley 8/2018, de 14 de septiembre, de Transparencia, Buen Gobierno y Grupos de Interés, del

obstante *«la experiencia empírica acredita que los órganos de cooperación que tienen un espacio web propio ofrecen una información monográfica y más completa que aquellos que no lo tienen»*[842].

Debido a la accesibilidad de los datos, la publicidad y el alcance del medio hace necesaria una modulación más restrictiva en relación con los datos personales que se publican en los portales de transparencia en cumplimiento de las obligaciones legales descritas anteriormente. Como bien señala el Profesor ROMEO RUÍZ «*En los casos de publicidad activa el límite debe aplicarse de manera más estricta, es decir, con mayor garantía del derecho a la protección de datos, puesto que la información se difunde públicamente y, a partir de esa difusión, es de conocimiento general. Por lo que la afectación a la protección de datos de los afectados, así como a*

Principado de Asturias; art. 29 de la Ley 1/2016, de 18 de enero, de transparencia y buen gobierno, de la Comunidad Autónoma de Galicia; art. 8 de la Ley 4/2016, de 15 de diciembre, de Transparencia y Buen Gobierno de Castilla-La Mancha; art. 10 de la Ley 2/2015, de 2 de abril, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunidad Valenciana; art. 2 de la Ley 3/2015, de 4 de marzo, de Transparencia y Participación Ciudadana de Castilla y León (Portal de Gobierno Abierto); art. 39 de la Ley 8/2015, de 25 de marzo, de Transparencia de la Actividad Pública y Participación Ciudadana de Aragón; art. 18 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía (Portal de la Junta de Andalucía); art. 7 de la Ley 3/2014, de 11 de septiembre, de Transparencia y Buen Gobierno de La Rioja; art. 11 de la Ley 12/2014, de 16 de diciembre, de Transparencia y Participación Ciudadana de la Comunidad Autónoma de la Región de Murcia; art.34 de la Ley 12/2014, de 26 de diciembre, de transparencia y de acceso a la información pública de la Comunidad Autónoma de Canarias; apartados 5 y 6 del art. 5 de la Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno de la Comunidad Autónoma de Cataluña; D.A. Segunda de la Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura. En cambio, otras CCAA han optado por la formula dada por el art. 38 de la LPAC al hacer pública la información por medio de las Sedes electrónicas de los sujetos obligados en su normativa autonómica en la materia, tal es el caso de la Comunidad Foral de Navarra (art. 7 de la Ley Foral 5/2018, de 17 de mayo, de Transparencia, acceso a la información pública y buen gobierno) e Islas Baleares (art. 7.4 de la Ley 4/2011, de 31 de marzo, de la buena administración y del buen gobierno de las Illes Balears). Sin embargo, actualmente las dos CCAA cuentan con un portal de transparencia. En la Comunidad Autónoma de las Islas Baleares es competencia de la Consejería de Administraciones Públicas y Modernización, a través de la Dirección General de Transparencia y Buen Gobierno, encargada de la «*planificación, impulso y coordinación interdepartamental de la transparencia del Gobierno, de la Administración autonómica y del sector público instrumental, tanto en la vertiente de la publicidad activa como del derecho de acceso; coordinación interdepartamental de medidas para impulsar el buen gobierno; calidad de las organizaciones y de los servicios públicos, y evaluación de políticas públicas*» (art. 2.11.e) del Decreto 21/2019, de 2 de agosto, de la presidenta de las Illes Balears, por el que se establecen las competencias y la estructura orgánica básica de las consejerías de la Administración de la Comunidad Autónoma de las Illes Balears.

842 GARCÍA MORALES, M.J., *op. cit.*, p. 318.

otros derechos de protección constitucional que pudieran afectarles, como puede ser el derecho al honor o el derecho a la intimidad, es mayor»[843].

Como se ha mencionado anteriormente en este trabajo, el límite del derecho a la protección de datos está regulado por el art. 15 de la LTAIBG, además los responsables de datos personales que sean Administraciones públicas, sector público institucional u otros obligados por la LTAIBG están obligados a cumplir con lo dispuesto en el RGPD y en la LOPDGDD[844]. El primer bloque de información institucional, organizativa y de planificación (art. 6) y el tercero de información económica, presupuestaria y estadística (art. 8) suelen entrar en conflicto con la normativa de protección de datos pues la publicidad activa requiere identificar a determinados sujetos como: empleados públicos, altos cargos, beneficiaros de subvenciones o de ayudas públicas, adjudicatarios de contratos, subcontratistas y aquellos responsables de los diferentes órganos. En este caso se publicarán sus datos personales como su nombre y apellidos relacionándolos con las obligaciones en materia de publicidad activa con carácter general, pues son considerados a efectos de la LTAIBG como «meramente identificativos» siempre que estén relacionados con las finalidades de la norma. No podrán publicarse datos de categorías especiales contenidos en la información que deba ser publicada, salvo que se haya efectuado previamente la respectiva disociación de estos[845].

El Criterio interpretativo 004/2015 del CTBG y la AEPD, de 23 de julio de 2015, determina que al art. 15 de la LTAIBG también de aplicación a las obligaciones de publicidad activa, específicamente a la publicación de los datos identificativos de los adjudicatarios de contratos[846] y de las partes firmantes de los convenios suscritos con los sujetos obligados de la LTAIBG si estos correspondiesen a personas físicas[847]. La publicación de estos datos supone la publicación de la identidad del adjudicatario o del firmante, por tanto, cabría «*considerar que la publicación del*

[843] ROMEO RUIZ, A., «Conflictos entre protección de datos personales y publicidad activa sobre retribuciones de empleados públicos. A propósito de la Sentencia de la Audiencia Nacional 2386/2019, de 26 de marzo de 2019», *Revista Vasca de Administración Pública*, núm. 116, enero-abril, 2020, p. 198-199.
[844] D.A. 2ª de la LOPDGDD.
[845] Art. 5.3 *in fine* de la LTAIBG.
[846] Art. 8.1. a) de la LTAIBG.
[847] Art. 8.1.b) de la LTAIBG.

nombre, apellidos y cargo de los firmantes cumpliría con la obligación contenida en dicho precepto»[848]. En este mismo supuesto el Criterio interpretativo determina que tanto la publicación del DNI como la firma manuscrita no contribuyen a alcanzar los objetivos de los incisos a) y b) del art. 8.1 de la LTBG, situación que se materializa con el nombre y apellidos de los firmantes. En referencia a las firmas manuscritas, establece como buena práctica la supresión de la totalidad de las firmas de este tipo de documentos siempre que «*ponga de manifiesto que el original ha sido efectivamente firmado*»[849]. En relación con las autorizaciones de compatibilidad a empleados públicos, el CTBG ha determinado por Resolución 0075/2016 del CTBG, de 17 de mayo de 2016, que, para alcanzar la finalidad perseguida por la LTAIBG, resulta idónea la publicación de la identidad de la persona titular de la autorización y en este caso «*no puede presuponerse una limitación absoluta de la información por causa de protección de datos*»[850].

Así pues, los órganos jurisdiccionales en el ámbito contencioso-administrativo, así como el CTBG y la AEPD, a través de sus criterios interpretativos y resoluciones, han ido perfilando este limite a la publicidad activa. Aunque es menester señalar que los criterios interpretativos de estas dos autoridades se refieren únicamente al sector público estatal, pues es su ámbito de actuación[851].

1.5.2 El acceso a la información y el derecho a la protección de datos personales.

El derecho de acceso a la información es la cara pasiva de la transparencia, permite el escrutinio del quehacer de las autoridades públicas por parte de los ciudadanos, y su participación en los asuntos públicos. Este acceso requiere que los ciudadanos formulen una solicitud para tener acceso a aquellos documentos que estén en poder de los sujetos obligados, bien sea por haber sido elaborados por estos o adquiridos en el ejercicio de sus funciones. La información deberá entregarse a los solicitantes preferentemente por vía electrónica a menos de que el solicitante haya

[848] Criterio interpretativo 004/2015 del CTBG y la AEPD, de 23 de julio de 2015, p.6.
[849] *Ib.,* p.8.
[850] Resolución 0075/2016 del CTBG, de 17 de mayo de 2016, p. 9-10.
[851] D.A. 5ª de la LTAIBG.

señalado de manera expresa otro medio o formato[852]. El acceso a la información pública está regulado por el Capítulo III del Título I de la LTAIBG, sin embargo, existen otras leyes que regulan de manera específica el acceso a archivos o registros, principalmente: la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (LPHE), la Ley 14/2007, de 3 de julio, de investigación biomédica (LIB), Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica y, la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública (LFEP). Normalmente el tratamiento de datos efectuado por los responsables es necesario para el cumplimiento del interés público[853] o como consecuencia de las competencias que les han sido atribuidas legalmente [art.6.1. e) RGPD]. El contenido del art. 86 del RGPD también prevé la conciliación entre el tratamiento de datos personales y el acceso público a los documentos oficiales.

La tramitación de la solicitud estará sujeta al contenido de la Sección 2ª del Capítulo III de la LTAIBG. De acuerdo con el contenido del art. 17.3 de la LTAIBG el solicitante no estará obligado a motivar su solicitud, sin embargo, dicha motivación es conveniente a efectos de una adecuada ponderación, sobre todos si la información solicitada pudiera estar afectada por algún límite legal contenido en los art. 14 y 15 de la misma ley. El Consejo de Transparencia y Buen Gobierno (CTBG) y la AEPD[854] han determinado que los límites establecidos en el art. 14, «*a diferencia de los relativos a la protección de datos de carácter personal* «*no operan ni automáticamente a favor de la denegación ni absolutamente en relación con los contenidos. La invocación de motivos de interés público para limitar el acceso a la información deberá de estar ligada con la protección concreta de un interés racional y legítimo*»[855]. En este apartado estudiaremos específicamente el límite contemplado en el art. 15 relativo a la protección de datos personales.

[852] *Vid.* art. 22.1 de la LTAIBG.
[853] Cfr. Considerando 154 del RGPD.
[854] De acuerdo con el contenido del art. 38.2.a) y la D.A. 5ª de la LTAIBG, el CTBG tiene entre otras funciones la de «adoptar criterios de interpretación», y a su vez este organismo deberá adoptar criterios conjuntos con la AEPD cuando se necesite una ponderación del interés público de acceso a la información y el derecho a la protección de datos personales.
[855] Criterio interpretativo del CTBG y la AEPD 002/2015, de 24 de junio, aplicación de los límites al derecho de acceso a la información, p.5.

Para que se realice la ponderación entre estos dos derechos es necesario que los datos personales no sean de categorías especiales contenidos en el art. 9.1 del RGPD y 15.1 de la LTAIBG. En ese caso se aplicarán los criterios de ponderación del apartado 3 del art. 15 de la LTAIBG: «*a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español; b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos; c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos; d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad».* De acuerdo con el CTBG y la AEPD estos criterios «*se refieren exclusivamente al acceso a la información pública*» y, por tanto, «*en ningún caso estos criterios son de aplicación a la publicación de dicha información en el régimen de publicidad activa previsto en los artículos 5 y siguientes de la LTAIBG*[856]*.*

El derecho a la protección de datos personales cede en mayor o menor medida, dependiendo del tipo de los datos personales se contengan en la información a la que se pretende acceder, es decir, «*la intensidad en la aplicación del límite es menor*»[857], de manera contraria a lo que ocurre con la publicidad activa, en atención a los medios y el grado de difusión, pues el acceso a la información solo le será entregada al solicitante. Este derecho también puede ceder en función del titular de los datos personales «*Así, para los puestos de mayor nivel de responsabilidad, autonomía en la toma de decisiones, provisión con cierto margen de discrecionalidad o con base en una relación de confianza, prevalece, por regla general, el interés derivado de la finalidad de la transparencia; entre ellos menciona varias categorías de empleados públicos, como los titulares de órganos directivos, personal eventual y de libre designación; frente a ellos se encuentra la información referente a los restantes empleados públicos que han accedido a sus puestos mediante los sistemas de provisión establecidos en las leyes reguladoras de la función pública, con*

[856] Criterio interpretativo del CTBG y la AEPD, CI/001/2015 de 24 de junio de 2015.
[857] ROMEO RUIZ, A., *op. cit*., p. 198.

independencia de la persona de quien dependan, en cuyo caso el objetivo de transparencia resulta insuficiente para limitar su derecho a la protección de sus datos personales, que prevalecerían sobre aquél objetivo»[858]. A este respecto el Profesor ROMEO RUÍZ determina que en este caso: «*la incidencia de la difusión de la información es limitada»*[859].

El apartado 2 del art. 15 hace una matización relacionada con el acceso a información que contenga datos meramente identificativos, de manera general, se podrá acceder a los mismo siempre que los datos estén relacionados con la organización funcionamiento o actividad pública del órgano, salvo que prevalezca el derecho a la protección de datos personales u otros constitucionalmente protegidos sobre la divulgación pública de la información. Hecha la ponderación de daño, resultase que una parte de la información está afectada por este límite, podrá darse acceso de manera parcial a la información al solicitante con indicación de qué la parte ha sido omitida, y siempre que no suponga distorsión o carezca de sentido, de acuerdo con el contenido del art. 16 de la LTAIBG.

Como mencionamos anteriormente, los datos de categorías especiales según la propia LTAIBG se divide en dos tipos y dependiendo que pertenezcan a uno u otro, deberán cumplirse determinados requisitos específicos para su acceso. Solo se podrá autorizar el acceso a la información que revele ideología, afiliación sindical, religión o creencias, si se cuenta con el consentimiento expreso y por escrito de la persona afectada, salvo que el afectado «*hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso*» [860]. En el caso de que la información haga referencia al origen racial, a la salud, a la vida sexual, incluya datos genéticos o biométricos, datos relacionados con la comisión de infracciones penales o administrativas que no conlleven amonestación pública, solo podrá darse acceso si se cuenta con el consentimiento expreso del afectado o su acceso esté amparado en una norma de rango de ley[861].

[858] F.D. 5º de la SAN de 26 de marzo 2019 (JUR\2019\201813; ECLI:ES:AN: 2019:2386).
[859] ROMEO RUÍZ, A., *op. cit.,* p. 198.
[860] Art. 15.1 de la LTAIBG.
[861] *Íd.*

La información que se entregue al solicitante que contenga datos personales y que su nuevo uso suponga, de alguna forma, tratamiento datos de acuerdo con el contenido del art. 4.2 del RGPD, seguirá estando sujeta a la normativa de protección de datos personales, siempre que no se utilice con fines exclusivamente personales o domésticos, motivo de exclusión de su ámbito material. Así también lo determina el apartado 5 del art. 15 de la LTAIBG. Este tipo de comunicaciones de datos se realizan con respaldo en una norma con rango de ley, lo cual las inviste de licitud según el art. 8 de la LOPDGDD. Es decir, la persona a la que se le da acceso se convertiría en responsable, pues fijaría nuevos fines y medios del tratamiento y, por tanto, se le aplicaría el contenido del Capítulo IV del RGPD y, cambiaría su base de licitud de tratamiento. Para concluir, es importante enfatizar que, el límite al derecho a la protección de datos personales con motivo de una solicitud de acceso no se aplicará si la información a la que se da acceso está disociada, por no contener datos que identifiquen a las personas o las hagan identificables.

1.5.3 La reutilización de datos

La llamada «transparencia colaborativa» es otro de los mecanismos que permiten a los ciudadanos tener conocimiento de las informaciones que tienen en su poder las AA.PP., de acuerdo con el Profesor CERRILLO I MARTÍNEZ «*se basa en la reutilización de la información pública, consistente en el uso de la información que está en poder de las Administraciones públicas, por parte de la ciudadanía, con finalidades comerciales o no comerciales, siempre que este uso no constituya una actividad administrativa pública*»[862]. Una de las ventajas que supone la reutilización de datos es la posibilidad que ofrece a las empresas «*desarrollar productos más atractivos y competitivos*»[863].

Tal y como lo establece el considerando 154 del RGPD, el derecho de acceso a documentos oficiales y el derecho a la protección de datos personales «*deben conciliar el acceso público del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de datos personales»*

[862] CERRILLO I MARTÍNEZ, A., «El difícil…» *op. cit*., p. 129.
[863] Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones. El papel de la administración electrónica en el futuro de Europa, COM (2003) 567 final, p. 7.

La reutilización de datos hasta ahora a nivel comunitario estaba regulada por el contenido de la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público. Ha sido transpuesta a nuestro ordenamiento jurídico por la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. En esta ley se define a reutilización como «*el uso de documentos que obran en poder de las Administraciones y organismos del sector público, por personas físicas o jurídicas, con fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública. Queda excluido de este concepto el intercambio de documentos entre Administraciones y organismos del sector público en el ejercicio de las funciones públicas que tengan atribuidas*»[864]. Su ámbito de aplicación atañe a los documentos que han sido elaborados o custodiados por organismos del sector público.

La reutilización de la información que está en poder de las AA.PP. está estrechamente relacionada con las obligaciones de transparencia activa reguladas en la LTAIBG. Pues la información se hace pública de manera habitual por medio de las sedes electrónicas y páginas web de las AA.PP.[865]. El formato reutilizable de las informaciones en tenencia de las AA.PP. constituye una de las prescripciones técnicas que debe cumplir la información para su publicación[866].

El art. 3.3.a) establece que la Ley 37/2007 no se aplicará a los documentos que se encuentren limitados por el contenido de la LTAIBG, es decir, aquellos que encuentren su límite en el contenido del art. 14 y 15 de esta última norma, entre los que se encuentran los datos personales especialmente protegidos y demás intereses como la seguridad nacional, defensa, relaciones exteriores, seguridad pública, etc. En el mismo artículo, pero en su inciso j) también se prevé la falta de aplicación a la normativa y, por tanto, a su reutilización, si los documentos o el acceso a los mismos se encuentran limitados por motivos de protección de datos personales e incluso las partes de documentos que aun siendo accesibles, contengan datos personales que supongan su incompatibilidad y esté establecido así por ley.

[864] Art. 3.1 de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.
[865] Cfr. Art. 5.4 de la LTAIBG.
[866] Cfr. Art. 11 de la LTAIBG.

Tampoco será objeto de reutilización aquella información que contenga datos personales y haya sido objeto de ponderación conforme al contenido del art. 5.3 y 15 de la LTBG, cuya conclusión estime la prevalencia del derecho a la protección de los datos personales, salvo que se haya procedido a la disociación de los datos, de modo que se impida la identificación de las personas afectadas[867]. En caso de que esa ponderación arroje un resultado distinto o cuando no hayan sido disociados los datos, la publicación de la información que contenga datos de esta naturaleza seguirá estando sujeta a la normativa en materia de protección de datos vigente, siempre que se determinen las finalidades concretas para las que sea posible su reutilización[868].

Lo anterior es plenamente compatible con el contenido del considerando 154 del RGPD, el cual establece que la Directiva de reutilización de los datos, no altera ni el nivel de protección de los datos de carácter de las personas físicas, ni las obligaciones a cumplir por los responsables y demás agentes que intervienen en el tratamiento contenidas en el RGPD[869].

Ahora bien, es necesario señalar que debido a los cambios sufridos en la Directiva 2003/98[870] se ha realizado una refundición de la Directiva, dando paso a la nueva Directiva 2019/1024, del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público, la cual atiende a la necesidad de «*disponer de un marco general para las condiciones de reutilización de los documentos del sector público con el fin de garantizar que dichas condiciones sean equitativas, proporcionadas y no discriminatorias*»[871], esta ha derogado la Directiva 2003/98 CE, entrando en vigor desde el 16 de julio de 2019, pero con efectos a partir del 17 de julio de 2021.

[867] *Vid.* art. 3.4 de la Ley 37/2007, de 16 de noviembre.
[868] *Vid.* art. 8.e) de la Ley 37/2007, de 16 de noviembre.
[869] A su vez compatible con el contenido del art. 1.4 de la Directiva 2003/98/CE.
[870] Por la Directiva 2013/37/UE, del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público.
[871] Considerando 20 de la Directiva 2019/1024, del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público.

Directiva que requiere ser transpuesta a nuestro ordenamiento jurídico a más tardar el día 17 de julio de 2021[872].

Esta nueva Directiva mantiene el contenido de los artículos que regulaban la relación de la reutilización con la normativa de protección de datos casi en los mismos términos. Su aplicación se entiende sin perjuicio al contenido del RGPD[873]. Esta Directiva tampoco se aplica a los documentos a los que no se pueda tener acceso o el mismo esté limitado en «virtud de regímenes de acceso por motivos de protección de los datos personales», tampoco se aplicará la Directiva a las partes de documentos personales, si una ley ha determinado que es incompatible con el régimen de reutilización[874] o si una ley haya determinado su incompatibilidad por suponer «un menoscabo de la protección de la intimidad y la integridad física». Esta última causa de inaplicación ha sido introducida por la nueva Directiva.

Con esta Directiva ahora los datos deberán ser abiertos por diseño y por defecto, sin perjuicio de la consideración del derecho a la protección de datos como un límite para la reutilización de la información. En el caso de que documentos o parte de documentos puedan ser objeto de reutilización, esta quedará limitada al principio de finalidad, es decir, que solo la información podrá ser reutilizable si tiene las mismas finalidades para los cuales fueron recogidos[875]. También contempla a la anonimización como fórmula que hace compatible plenamente el derecho a la protección de datos personales y la reutilización de datos, su aplicación permite que los interesados no sean o puedan ser identificados[876]. Como novedad también se prevé el principio de tarificación, para recuperar los costes de la anonimización[877]. Finalmente, se establece que debe tomarse en cuenta la protección de los datos personales como límite a la apertura de los datos de las investigaciones financiadas

[872] De acuerdo con el contenido de los art. 17, 19 y 20 de la Directiva 2019/1024.
[873] Antes y ahora regulado por el contenido del art. 1.4 de ambas directivas.
[874] Antes contenido en el art. 1.2.c *quater* (modificación introducida por la Directiva 2013/37/UE, del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público) y ahora contemplado en el contenido del art. 1.2 h) de la Directiva 2019/1024.
[875] De acuerdo con el considerando 52 de la Directiva 2019/1024.
[876] De acuerdo con el contenido del art. 2.7 de la Directiva 2019/1024.
[877] Cfr. Art. 6.1 de la Directiva 2019/1024.

con fondos públicos, bajo el principio «*tan abiertos como sea posible, tan cerrados como sea necesario*»[878].

1.6 El tratamiento de datos con fines de archivo, investigación científica o histórica y estadísticos.

Es ampliamente conocido que la investigación y la actividad estadística son herramientas de especial envergadura en cada Estado, pues ayudan a la consecución de sus fines, al crecimiento económico, en algunos casos forman parte de la resolución de determinados problemas, además, son sustento del desarrollo de políticas públicas[879]. Por su parte, el acceso a los archivos y a documentos permite a los ciudadanos realizar un escrutinio con bases sólidas sobre el desempeño de la actividad pública y a su vez, puede generar la participación de estos en los asuntos de naturaleza pública. Sin duda todas estas actividades permiten un mayor crecimiento económico, el desarrollo de nuevos bienes y servicios y la mejora de estos últimos. De manera que permite a las Administraciones públicas poder conseguir sus fines con mayor eficacia y eficiencia.

El RGPD establece garantías excepcionales a los tratamientos de datos con estos fines, de acuerdo con el contenido del art. 89. Este tipo de tratamientos deben llevarse a cabo con la implementación de medidas técnicas y organizativas que garanticen el principio de minimización de datos, es decir, siempre que se pueda se podrá implementar la seudonimización para este tipo de tratamientos, lo cual supondría separar los datos personales del resto de la información de manera que durante el tratamiento no se pueda relacionar con el interesado a menos de que se utilice la información adicional que permita su identificación. Este tipo de medidas solo podrán ser utilizadas si estas finalidades permiten ser alcanzadas con su implementación.

---

[878] De acuerdo con el considerando 28 y el contenido del art. 10.1 de la Directiva 2019/1024.

[879] En relación con lo anterior y realzando la importancia de la función estadística pública el Profesor DE LA FUENTE MIGUÉLEZ, determina que «*se erige en una poderosa herramienta que, por decirlo de algún modo, transforma los datos relativos al complejísimo entramado de los diversos ámbitos de la actividad humana en información cuantitativa que constituya una descripción sintética de la sociedad. Es decir, la operatividad de los poderes públicos, su eficacia y eficiencia, exige que sus decisiones se basen no directamente en la sociedad (lo cual es humanamente imposible en la actualidad), sino en información acerca de esa sociedad*», *vid.* FUENTE MIGUÉLEZ, A. DE LA, *El secreto estadístico. Factor clave en la Administración pública,* Mc Graw Hill INAP, Madrid, 2018, p. 7.

Como sabemos, los datos personales solo pueden ser tratados para las finalidades por las cuales han sido recogidos y su tratamiento se limita a determinado periodo de tiempo para alcanzar estas. El RGPD permite la posibilidad de llevar a cabo tratamientos ulteriores por las AA.PP. competentes para ello con fines de investigación científica o histórica, de archivo y para realizar la actividad estadística, pues todas estas finalidades están relacionadas con intereses generales. Entonces la base de licitud para realizar estos tratamientos por las AA.PP. deberá ser por obvias razones las contempladas en los incisos c) y e) del art. 6.1 del RGPD, es decir, en cumplimiento de un deber legal. De ser necesario para el cumplimiento de un interés público o con motivo del ejercicio de las competencias que le han sido atribuidas. En relación con los principios establecidos en el art. 5 del RGPD, también es necesario señalar que la conservación de la información por periodos más largos al estrictamente necesario para el tratamiento inicial está autorizada por el propio reglamento (art. 5.1.e RGPD), es decir, que se podrán conservar datos por periodos más largos si son tratados con fines archivísticos, estadísticos o de investigación científica o histórica, siempre que se tomen medidas técnicas y organizativas que aseguren el respeto a los derechos y libertades de los interesados.

El RGPD puntualiza en el apartado 1 del art. 89 que, en la medida que puedan alcanzarse estos fines, el tratamiento de los datos personales deberá ser llevado a cabo de modo que no se permita o ya no se permita la identificación de los interesados y aun así se puedan cumplir con las estas finalidades, lo anterior se hace eco de la necesidad de la minimización de datos aun cuando se pretenda cumplir con intereses públicos, en la medida de lo posible.

En relación con lo anterior, en nuestro ordenamiento jurídico el art. 155 de la LRJSP prevé la transmisión de datos de carácter personal por AA.PP., en los mismos términos que lo establecido en el RGPD, ya que estima que: «*no se considerará incompatible con los fines iniciales el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos*».

Para cumplir con las finalidades de investigación científica, histórica o estadística se pueden excepcionar y limitar los derechos de acceso, rectificación

limitación y oposición[880] por el Derecho de la Unión o el de los Estados miembros, siempre que sea necesario para el cumplimiento de estas finalidades, en tanto que estos derechos obstaculicen o imposibiliten su logro. Ocurre de la misma manera con los tratamientos que se realicen con fines de archivo en interés público y limitándose los mismos derechos para el caso anterior, a los que han de sumarse, el derecho de portabilidad y la obligación de comunicar en su caso la rectificación, supresión o limitación del tratamiento a los interesados. En cualquier caso, las excepciones antes descritas solo son aplicables a estas finalidades[881].

El tratamiento de datos personales de categorías especiales como mencionamos anteriormente está prohibido de manera genérica, a menos que le sea aplicable una excepción del apartado 2 del art. 9 del RGPD. En el caso que nos ocupa, el tratamiento con fines de archivo en interés público, de investigación científica o histórica y estadísticos, puede llevarse a cabo siempre y cuando el tratamiento sea proporcional al objetivo que se persiga, se guarde respeto en lo esencial al derecho a la protección de datos personales y se establezcan medidas adecuadas y específicas que protejan los derechos fundamentales de los interesados[882].

Antes de realizar un análisis específico relacionado con cada finalidad, es importante saber cuáles son las normas de carácter legal en nuestro sistema jurídico que pueden limitar derechos del art. 15 al 22, según sea el caso. Es menester señalar que en la actualidad se ha limitado mayoritariamente el derecho de acceso a los datos que son tratados con estas finalidades. Igualmente, es importante aclarar en este punto que el análisis posterior solamente se realizará a la luz de las competencias que tiene asumidas el Estado, sin perjuicio de que el tratamiento de datos personales con esos fines también se realice por las CC.AA. como consecuencia de las competencias asumidas en sus respectivos Estatutos de Autonomía.

1.6.1 El tratamiento de datos con fines estadísticos.

Primeramente, es necesario determinar cuál es el objeto de la función estadística llevada a cabo por las AA.PP., en este sentido el Profesor SOUVIRÓN

[880] Derechos contemplados en los arts. 15,16, 18 y 21 del RGPD.
[881] *Vid.* Apartados 2, 3 y 4 del art. 89 del RGPD.
[882] Art. 9.2. j) del RGPD.

MORENILLA determina que se es aquella encargada de describir «*los fenómenos colectivos y de la realidad social mediante la recopilación, elaboración y ordenación sistemática de datos así como la obtención, presentación, publicación y difusión de resultados, a través de las correspondientes acciones de planificación y ejecución estadísticas*», de tal manera que «*no se trata de una tarea puramente matemática, sino vinculada al análisis de la vida colectiva y que integra en la tarea matemática la toma de datos de los fenómenos empíricos, su elaboración tratamiento e interpretación*»[883]. De acuerdo con el Profesor DE LA FUENTE MIGUÉLEZ la función estadística debe entenderse como «*la capacidad de acción o la actividad humana propia de los cargos y oficios que se ejercen mediando potestad, jurisdicción o autoridad específica propia de los poderes públicos de una sociedad, que consiste en la realización de censos o recuentos de la población, de los recursos naturales e industriales y demás manifestaciones de un Estado, provincia, pueblo o clase, o en el estudio de los hechos morales o físicos que se presten a numeración, recuento y la comparación de las cifras a ellos referentes, y que a tal fin se sirve de la ciencia que, partiendo de conjuntos de datos numéricos, obtiene inferencias basadas en el cálculo de probabilidades*»[884]. Sin duda la función estadística pública es un pilar en la elaboración de políticas públicas, pus sistematiza información que refleja distintos aspectos de nuestra sociedad, en este sentido, permite a las Administraciones públicas contar con información y datos en los que pueden fundamentar la toma de decisiones en aras de conseguir los diversos intereses de carácter general conforme a los principios de eficacia y eficiencia[885].

En nuestro sistema jurídico la actividad estadística a nivel estatal está regulada por el contenido de la Ley 12/1989, de 9 de mayo, de la Función Estadística

[883] SOUVIRÓN MORENILLA, J.M., «Consideraciones sobre la función estadística pública», *Revista de Administración Pública,* núm. 134, mayo-agosto, 1994, pp. 426-427.
[884] FUENTE MIGUÉLEZ, A. DE LA, *El secreto estadístico…op. cit.,* p. 3.
[885] En este sentido, es necesario señalar la diferenciación de estos dos principios, por un lado «*la eficacia conlleva que la Administración lleve a cabo todas aquellas actuaciones necesarias para cumplir con sus fines, que no son otros que los intereses generales, y la eficiencia conlleva que la satisfacción de dichos intereses se lleve a cabo evitando todas aquellas demoras y molestias que resulten innecesarias, especialmente para los ciudadanos*», *Vid.* TRAYTER JIMÉNEZ, J. M., *op. cit.,* p. 211.

Pública (LFEP)[886], concordancia con lo establecido en el art. 149.1.31 de la CE. En esta Ley se regula el Plan Estadístico Nacional el cual supone «*el instrumento central de ordenación de la función estadística, en cuanto se contienen en todos los programas estadísticos a desarrollar y se referencian los medios e inversiones que van a ser necesarias*»[887]. Este Plan tiene una vigencia de cuatro años y deberá ser aprobado por medio de una norma reglamentaria con rango de Real Decreto[888]. Los responsables del tratamiento de datos personales con carácter estatal que utilizan datos personales con la finalidad de realizar la función estadística pública son: 1) el Instituto Nacional de Estadística, 2) el Consejo Superior de Estadística, 3) las unidades de los diferentes departamentos ministeriales y, 4) otras entidades públicas dependientes de los departamentos ministeriales a las que se haya encomendado aquella función, de acuerdo con el contenido del art. 23 de la LFEP.

El contenido del art. 25 de la LOPDGDD regula en términos generales los tratamientos de datos llevados a cabo con fines estadísticos. Los cuales están sujetos la normativa específica, es decir, a la Ley 12/1989, de 9 de mayo, de la Función Estadística Pública (LFEP) y a su vez al contenido en la normativa de protección de datos personales. Los datos personales podrán ser comunicados a órganos que tengan atribuidas competencias en materia estadística, la base de licitud de esa comunicación está amparada por el contenido del art. 6.1.e) del RGPD, pues la

[886] De acuerdo con el contenido del art. 149.1.31, es competencia exclusiva del Estado la función estadística para fines estatales. Sin perjuicio de las competencias asumidas por las CC.AA. en sus respectivos Estatutos de Autonomía, para realizar esta función en su ámbito competencial. Las CC.AA. que han regulado la función en sus determinados territorios, las leyes autonómicas que la regulan son: la Ley 4/1986, de 23 de abril, de Estadística de la Comunidad Autónoma de Euskadi; la Ley 9/1988, de 19 de julio, de Estadística de Galicia; la Ley 4/1989, de 12 de diciembre, de Estadística de la Comunidad Autónoma de Andalucía; la Ley 5/1990, de 7 de junio, de estadística de la Comunidad Valenciana; Ley 1/1991, de 28 de enero, de Estadística de la Comunidad Autónoma de Canarias; la Ley 12/1995, de 21 de abril, de Estadística de la Comunidad de Madrid; la Ley Foral 11/1997, de 27 de junio, de Estadística de Navarra; la Ley 23/1998, de 30 de diciembre, de Estadística de Cataluña; la Ley 7/2000, de 11 de julio, de Estadística de Castilla y León; la Ley 3/2002 de 17 de mayo, de Estadística de las Illes Balears; la Ley 10/2002, de 21 de junio, de Estadística de Castilla-La Mancha; la Ley 6/2002, de 25 de junio, de Estadística de la Región de Murcia; la Ley 4/2003, de 20 de marzo, de Estadística de la Comunidad Autónoma de Extremadura; la Ley 2/2005, de 1 de marzo, de Estadística de La Rioja; la Ley 4/2005, de 5 de octubre, de estadística de Cantabria; y la Ley del Principado de Asturias 7/2006, de 3 de noviembre, de Estadística. No debemos olvidarnos de las competencias de las Administraciones Locales de elaboración del Padrón municipal, del Censo de población y vivienda, así como la realización del Censo electoral, con base en el contenido de los artículos 16 y 17 de la LBRL.

[887] Apartado II de la Exposición de motivos de la LFEP.

[888] En la actualidad el Plan Estadístico vigente ha sido aprobado por el Real Decreto 410/2016, de 31 de octubre, por el que se aprueba el Plan Estadístico Nacional 2017-2020.

función estadística pública es considerada tradicionalmente como un instrumento que ayuda a la consecución de los intereses públicos y su realización se les atribuye a determinados sujetos, sin perjuicio de que esas transmisiones se encuentren en los instrumentos de programación estadística «legalmente previstos», de acuerdo con el art. 25.2 de la LOPDGDD. Dicha planificación se lleva a cabo a través de los diversos planes de estadísticos, a nivel por medio del Plan Estadístico Nacional[889], que precisamente no son creados a través de una norma con rango legal. Este tipo de tratamiento de datos también puede encontrar su base jurídica de licitud en el art. 6.1.c), es decir, siempre que tengan como finalidad el cumplimiento de un deber legal que sea aplicable al responsable del tratamiento[890]. En relación con los datos especialmente protegidos y con los datos relativos a condenas e infracciones penales (arts. 9.1 y 10 del RGPD), serán destinados a la función estadística de manera voluntaria y con previo consentimiento de carácter expreso de los interesados, tal y como se establece en el RGPD, por tanto, deberá ser explícito e informado, en este contexto GUASP MARTÍNEZ señala «*que el consentimiento sea explícito no significa que deba recabarse por escrito, si bien lo cierto es que como corresponde al responsable del tratamiento la carga de acreditar que tal consentimiento se prestó por el interesado, la experiencia nos demuestra que será la forma habitual de recabar el consentimiento por las Administraciones Públicas»*[891]. En este sentido el Profesor VALERO TORRIJOS determina que el nuevo marco jurídico refuerza la posición jurídica de los interesados «*al requerir el consentimiento sea necesariamente expreso para la recogida de los datos más sensibles a que se refieren los artículos 9 y 10 del RGPD*»[892].

Los tratamientos ulteriores de datos están permitidos de acuerdo con los arts. 5.1.b) y 89.1 del RGPD, siempre que se lleven a cabo por el responsable del

[889] El Plan Estadístico Nacional es aprobado por medio de un Real Decreto con vigencia de cuatro años. Cfr. art 8 de la LFE. El último fue aprobado por el Real Decreto 1110/2020, de 15 de diciembre, por el que se aprueba el Plan Estadístico Nacional 2021-2024.

[890] Por ejemplo, el Instituto de las Mujeres estas obligado por ley a la realización de análisis estadísticos (y al mantenimiento de las bases de datos) que afecten «*a la igualdad de trato y de oportunidades entre mujeres y hombres*», cfr. art. Tercero inciso e) de la Ley 16/1983, de 24 de octubre, de creación del Organismo Autónomo Instituto de la Mujer.

[891] GUASP MARTÍNEZ, V., «Tratamientos concretos de datos personales en la LOPDGDD (Arts. 19-27 LOPDGDD)», LÓPEZ CALVO, J. (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, p. 207.

[892] VALERO TORRIJOS, J., «Protección de datos…» *op. cit.,* pp. 435-436.

tratamiento medidas técnicas y organizativas que garanticen el respeto a los derechos y libertades de los interesados, especialmente se deberá observar el principio de minimización de los datos, en este sentido los datos tendrán que ser seudonimizados siempre la aplicación de esta técnica de minimización permita cumplir con los fines estadísticos. Incluso el RGPD permite el tratamiento ulterior de los datos de categorías especiales establecidos en el art. 9.2.j) siempre que el tratamiento sea proporcional con los fines estadísticos perseguidos, aunque como señalamos anteriormente el legislador orgánico ha optado por el consentimiento como base legitimadora para su tratamiento[893].

En consonancia con el art. 89.2 del RGPD, el artículo 25.3 de la LOPDGDD establece que las autoridades encargadas de llevar a cabo el tratamiento de datos con esas finalidades, podrán denegar solicitudes relativas al ejercicio de derechos, específicamente las relacionadas con los derechos de acceso, rectificación, supresión, portabilidad, oposición , a no ser objeto de decisiones individuales automatizadas, a la limitación del tratamiento, y a comunicar al interesado cualquier rectificación o supresión o limitación, portabilidad, oposición[894]; siempre que los datos estén bajo el amparo del secreto estadístico, en la legislación estatal o autonómica, en consecuencia como lo establece FERNÁNDEZ ACEVEDO el secreto estadístico «*está obligado a consolidar unas garantías de tal calibre, que las mismas pueden llegar a fundamentar la necesidad de tener que negar el ejercicio de cualquiera de los derechos*»[895] contemplados en el RGPD. En relación con lo anterior, el art. 13 de la LFEP establece que el objeto de protección del secreto estadístico son los datos personales de los interesados sin importar si estos han sido recabados directamente de los mismos o si han sido obtenidos como parte de una transmisión de datos con otras Administraciones públicas para esos efectos. Por lo que obliga a los servicios estadísticos a no difundir este tipo de datos. Las transferencias con fines estadísticos entre Administraciones públicas y por tanto bajo el secreto estadístico, de acuerdo con el contenido del art. 15 de la LFEP solo podrán realizarse si la administración

[893] Art. 25.2 de la LOPD en relación con el art. 11.2 de la LFE y con el art. 9.2 .a) del RGPD.
[894] Contemplados de los artículos 15 al 22 del RGPD, no por ese orden.
[895] FERNÁNDEZ ACEVEDO, J., «Disposiciones relativas a situaciones específicas de tratamiento (Arts. 85-91 RGPD. Disposición adicional segunda y vigésimo segunda LOPDGDD), LÓPEZ CALVO, J. (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, p. 746.

receptora desarrolla funciones estadísticas, que el destino de los datos sea la elaboración de estadísticas como consecuencia de sus competencias, y que cuente con los medios necesarios para preservar el secreto estadístico.

El secreto estadístico deberá ser preservado por el personal al servicio de las autoridades públicas que traten datos personales como consecuencia del ejercicio de sus funciones. De igual manera están obligados a guardarlo aquellas personas físicas o jurídicas que hayan conocidos los datos personales durante el proceso estadístico [896]. El secreto estadístico se inicia desde que se conozcan los datos personales [897] y se mantendrá durante el proceso estadístico e incluso si el personal que realizaba funciones de este tipo ya no está vinculado laboral o materialmente a esta actividad.

Parece idóneo señalar que con la entrada en vigor del RGPD en este caso obliga a las AA.PP a adoptar medidas técnicas y organizativas que minimicen el uso de los datos como la seudonimización para estas finalidades, especialmente cuando los datos son recabados directamente de los interesados por autoridades públicas que lleven a cabo funciones en materia estadística, siempre que de esta manera pueda ser conseguida esa la finalidad del tratamiento, sin la necesidad de determinar la identidad de los sujetos.

En relación con lo anterior, incluso el apartado 2 del art. 14 de la LFEP prohíbe la utilización de datos para finalidades distintas obtenidas directamente por los servicios estadísticos, con lo cual este artículo limita el acceso a los mismos para una utilización distinta. En el caso de que la información que sirva como muestra para elaborar estadísticas, provenga de otras Administraciones y no esté seudonimizada, con el nuevo marco jurídico en materia de protección de datos, habrá que proceder a esta desde su recepción, ya que genéricamente no obstaculizaría las funciones de esta autoridad y se cumpliría con la limitación de la finalidad establecida por la norma estatal. En relación con lo anterior ya la LFEP, ya preveía incluso antes de la publicación del RGPD en su art. 18, como medida técnica, la eliminación de los datos que sirvieran para identificar a las personas de forma

[896] Cfr. Apartados 1 y 2 del art. 17 de la LFEP.
[897] *Vid.* Art. 19.1 de la LFEP.

inmediata cuando su conservación resultase innecesaria. En cuanto a este artículo también se preveía una suerte de seudonimización, ya que por mandato legal se establece que los datos que identifiquen de forma directa a los interesados deben estar bajo claves, precintos o depósitos especiales y no así el resto de la información.

Es importante señalar que a menudo el desarrollo de una investigación científica o histórica requiere datos de naturaleza estadística sin la necesidad de determinar la identidad de los interesados, en este caso la información deberá ser entregada sin que consten los datos de identificación de los interesados u otros datos que permitan su identificación por el cruce de datos, de esta forma la entrega será respetuosa del secreto estadístico y será útil para la consecución de esa nueva finalidad.

La LFEP limita el derecho de acceso a la información que contenga datos personales y por ende bajo el secreto estadístico, por tanto, la información no podrá ser consultada a menos de que se cuente con el consentimiento expreso del interesado (persona titular de los datos personales) contenidos en la documentación a cuál se pretende acceder. Sin embargo, en la misma ley se prevé que la información podrá ser consultada si han transcurrido veinticinco años desde la muerte de titular de los datos y en caso de que la fecha de su fallecimiento fuese desconocida se podrá acceder a la información siempre que haya pasado el plazo de cincuenta desde que la información haya sido obtenida[898]. Se podrá permitir la consulta de la información al solicitante que acredite interés legítimo, siempre que haya transcurrido un plazo de veinticinco años desde que se haya obtenido la información.

1.6.2 El tratamiento de datos con fines de investigación.

Constitucionalmente se prevé la competencia concurrente en materia de investigación, por un lado, el art. 148.1.17 establece que las Comunidades Autónomas podrán asumir competencias en materia de fomento de investigación[899],

[898] Cfr. Art. 19.2 de la LFEP.
[899] Art. 10.16 de la Ley Orgánica 3/1979, de 18 de diciembre, de Estatuto de Autonomía para el País Vasco; arts. 44.4 y 158.1 de la Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de Autonomía de Cataluña; art. 27.19 de la Ley Orgánica 1/1981, de 6 de abril, de Estatuto de Autonomía

por otro lado, el Estado tiene competencia exclusiva para coordinar de la investigación científica y técnica [900], sin embargo, también es el encargado de fomentar la investigación a nivel nacional. En relación con lo anterior, la Profesora CUETO PÉREZ haciendo una comparación entre el contenido de dos artículos anteriores determina que «*lo primero que salta a la vista es que ambos recogen competencias similares, por no decir idénticas, en lo que se refiere al fomento de la investigación, en lo que se refiere a fomento de la investigación, y que además dentro de estas competencias no se han delimitado las funciones que corresponden a cada Administración territorial, por lo que tenemos que entender que tanto la función normativa (sin distinguir entre bases y desarrollo) como la función ejecutiva, corresponden tanto al Estado como a las Comunidades Autónomas, y que por ello, es necesario diferenciar una política científica de carácter estatal (nacional) y una política científica propia de cada Comunidad Autónoma. En investigación científica se produce una concurrencia total o paralelismo pleno en el reparto de competencias que la Constitución ha diseñado. Esta realidad exige que el Estado tenga un plus de competencia, plus que viene dado por el hecho de que la coordinación sobre la materia le corresponde exclusiva a el, lo que lleva que los instrumentos de coordinación deban ser establecidos por el Estado y asumidos por las Comunidades Autónomas, de forma*

para Galicia; art. 54.1 Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía; arts. 10.1.19 y 18.3 de la Ley Orgánica 7/1981, de 30 de diciembre, de Estatuto de Autonomía para Asturias; art. 24.19 de la Ley Orgánica 8/1981, de 30 de diciembre, de Estatuto de Autonomía para Cantabria; art. 8.1.24 de la Ley Orgánica 3/1982, de 9 de junio, de Estatuto de Autonomía de La Rioja; art. 10.1.15 de la Ley Orgánica 4/1982, de 9 de junio, de Estatuto de Autonomía para la Región de Murcia; art. 49.1.7ª de la Ley Orgánica 5/1982, de 1 de julio, de Estatuto de Autonomía de la Comunidad Valenciana; art. 71. 41ª de la Ley Orgánica 5/2007, de 20 de abril, de reforma del Estatuto de Autonomía de Aragón; art. 31.1. 17ª de la Ley Orgánica 9/1982, de 10 de agosto, de Estatuto de Autonomía de Castilla-La Mancha; arts. 135 y art. 141.2.c) de la Ley Orgánica 1/2018, de 5 de noviembre, de reforma del Estatuto de Autonomía de Canarias; art. 44.7 de la Ley Orgánica 13/1982, de 10 de agosto, de reintegración y amejoramiento del Régimen Foral de Navarra; apartados 22 y 24 del art. 9 .1 de la Ley Orgánica 1/2011, de 28 de enero, de reforma del Estatuto de Autonomía de la Comunidad Autónoma de Extremadura; art. 30. 44 de la Ley Orgánica 1/2007, de 28 de febrero, de reforma del Estatuto de Autonomía de las Illes Balears; apartado 1.20 del art. 26.1 de la Ley Orgánica 3/1983, de 25 de febrero, de Estatuto de Autonomía de la Comunidad de Madrid; arts. 70.1.23º y 74.4 de la Ley Orgánica 14/2007, de 30 de noviembre, de reforma del Estatuto de Autonomía de Castilla y León.

[900] Art. 149.1.15ª de la CE.

que la política científica estatal y la política científica de las Comunidades Autónomas no se interfiera ni se contradiga o entorpezca»[901].

Ahora bien, de acuerdo con el considerando 159 del RGPD «*el tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia*». Sin embargo, el GT29 ha matizado los alcances de este considerando y ha establecido que «*no debe ampliarse más allá de su significado común y entiende que "investigación científica" en este contexto se refiere a un proyecto de investigación establecido con arreglo a las correspondientes normas metodológicas y éticas relacionadas con el sector, de conformidad con prácticas adecuadas*»[902].

En la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación, se señalan determinados agentes que desde la perspectiva del derecho a la protección de datos son considerados como responsables del tratamiento: los agentes públicos de financiación y aquellos que realicen la actividad investigadora, como el personal investigador de las Universidades Públicas y de organismos públicos de investigación tanto estatales[903] como autonómicos[904]. Entre los

---

[901] CUETO PÉREZ, M., *Régimen jurídico de la investigación científica: la labor investigadora en la Universidad,* Centro de Estudios de Derecho, Economía y Ciencias Sociales Cedecs, Barcelona, 2002, p. 106.

[902] GT29, Directrices sobre el consentimiento en el sentido del Reglamento (UE)2016/679, 2017, p. 31.

[903] De acuerdo con el art. 47 de la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación, tienen condición de órganos públicos de investigación de la AGE: «la Agencia Estatal Consejo Superior de Investigaciones Científica (CSIC), el Instituto Nacional de Técnica Aeroespacial (INTA), el Instituto de Salud Carlos III (ISCIII), el Instituto Geológico y Minero de España (IGME), el Instituto Español de Oceanografía (IEO), el Centro de Investigaciones Energéticas Medioambientales y Tecnológicas (CIEMAT), el Instituto Nacional de Investigación y Tecnología Agraria y Alimentaria (INIA), y el Instituto de Astrofísica de Canarias (IAC)».Para un estudio más profundo sobre estas cuestiones, *vid.* CUETO PÉREZ, M., «La organización de los Organismos Públicos de Investigación Estatales», DÍEZ BUESO, L., *La organización de la ciencia a revisión: Administración General del Estado, Cataluña, Madrid y País Vasco,* Huygens, 2020, pp. 11-52.

[904] De acuerdo con el contenido del art. 149.1.15 de la CE, el Estado tiene la competencia exclusiva en fomentar y coordinar de forma general la investigación científica y técnica. Sin perjuicio de la asunción de estas competencias por las CC.AA. en sus respectivos Estatutos de Autonomía en base al art. 148.1.17 de la CE, como competencia propia el fomento de la investigación en su ámbito competencial: Asturias (arts. 10.1.19 y art. 18.3 de su E.A), Cantabria (art. 24.19 de su E.A.), la Rioja (art. 8.1.24 de su E.A.), Murcia (art. 10.1.15 de su E.A.), Valencia (arts. 49.1.7ª y 52.2 de su E.A.), Aragón (arts. 28.1 y 71.41ªde su E.A.), Catilla-La Mancha (arts. 31.1.17ªy 37.3 de su E.A.), Canarias (art. 135 de su E.A), Navarra (art. 44.7 de su E.A.), Extremadura (apartados 22 y 24 del art. 9.1 de su E.A.), Islas Baleares (art. 30.44 de su E.A.), Madrid (art. 26.1.20 de su E.A.), Castilla y León (arts. 70.1.23º y 79.4 de su E.A.), Cataluña (art. 158 y 44.4 de su E.A.), País Vasco (art. 10.16 de su E.A.),

deberes del personal investigador [de acuerdo con el inciso h) del art. 15.1 de esta misma ley] y del personal técnico [art. 28.3.g) de la referida norma] se encuentra la adopción de medidas para cumplir con la normativa en materia de protección de datos, con especial atención a la confidencialidad. En tanto, sus D.A. novena determina que se le aplicará la normativa de protección de datos al tratamiento y cesión de los datos obtenidos a partir de la investigación y, además, se determina que tanto los agentes públicos de financiación[905] como los de ejecución[906] deberán adoptar medidas técnicas y organizativas encaminadas a preservar la seguridad y evitar su alteración, tratamiento o acceso no autorizado.

En este caso, la actividad constituye un interés público por lo que la base genérica de licitud es el art. 6.2.e) del RGPD. Sin embargo, la realización de esta actividad no siempre tiene el mismo objeto, depende de las líneas de investigación de los grupos que realicen esta actividad, de proyectos específicos o trabajos individuales[907]. En algunos casos puede implicar tratamientos de datos personales, sobre todo cuando en la investigación científica e histórica, en cuyo caso los sujetos responsables estarán obligados a implementar las medidas técnicas y organizativas con la finalidad de cumplir lo establecido en el RGPD y en la LOPDGDD, específicamente deberán evitar la alteración de los datos, tratamientos y accesos que no estén autorizados[908]. Por lo que, las Administraciones públicas deberán adoptar las determinadas en el ENS. Este último prevé la limitación y el control de accesos en su art. 16. Las medidas a adoptar en este caso serían aquellas previstas bajo el marco operacional «control de acceso "op. acc"» y, las medidas de protección relacionadas de: la protección de las comunicaciones «mp.com», de los soportes de

Galicia (art. 27.19 de su E.A.), y Andalucía (art. 54 y 55.2 de su E.A.). En relación con materias que afecten a la Administración Local será el Instituto de Estudios de Administración Local adscrito al Ministerio de Administración territorial, quien llevará a cabo investigaciones de estas materias (art. 120.1 de la LBRL).

[905] Son agentes públicos de financiación a efectos de esta ley los contemplados en el apartado 3 del art. 3: «*Son agentes de financiación las Administraciones Públicas, las entidades vinculadas o dependientes de éstas y las entidades privadas, cuando sufraguen los gastos o costes de las actividades de investigación científica y técnica o de innovación realizadas por otros agentes, o aporten los recursos económicos necesarios para la realización de dichas actividades*».

[906] Art. 3.4 de la Ley 14/2011: «*Son agentes de ejecución las entidades públicas y privadas que realicen o den soporte a la investigación científica y técnica o a la innovación*».

[907] En este sentido, los Planes de ordenación en investigación científica incluyen actividades de «promoción, fomento y coordinación en materia de investigación», Cfr. «Plan Estatal de Investigación Científica y Técnica y de Innovación 2017-2020», p. 12.

[908] D.A. 9ª de la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación.

la información «mp.si», de los equipos « mp.eq» y de la protección de la información « mp.info». El ENS no es aplicable a los agentes de ejecución por no ser administraciones públicas, sin embargo, como buena práctica tomarán medidas análogas a las descritas contenidas en el ENS[909].

En la actualidad, otras leyes de carácter sectorial son las encargadas de regular de forma específica, en algunos casos el tratamiento de datos en la investigación científica y en otros su regulación solo se limita al acceso a la información que contienen datos de carácter personal. Por ejemplo, el artículo 28 del Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, regula el acceso a archivos que contienen datos personales. Específicamente el apartado 3 del referid artículo considera que los investigadores cuentan con interés legítimo para acceder a archivos que contengan datos personales meramente identificativos, siempre que acrediten que el acceso se produce con fines de investigación o estadísticos.

Ley 14/2007, de 3 de julio, de investigación biomédica (LIB), es una norma que regula la investigación en un sector concreto. Buena parte del contenido de esta ley se dedica a determinar qué datos personales se tratan y cómo, las limitaciones en relación con el acceso a este tipo de datos, las medidas técnicas y organizativas aplicables a los datos personales durante su tratamiento, concretamente la anonimización. En relación con la investigación biomédica, se tienen que destacar las siguientes cuestiones a partir de la renovación del marco jurídico en materia de protección de datos. Por una parte, ahora el RGPD proporciona una definición de los datos genéticos en su art. 4.13. Al tratarse de datos que se refieren a la naturaleza más intrínseca del ser humano son considerados como datos de una categoría especial de acuerdo con el art. 9.1 del RGPD, es decir que no podrán ser tratados a menos de que se cumplan una de las circunstancias previstas en el apartado dos del mismo precepto entre las que se encuentra la investigación científica [inciso j)], en cuyo caso se requiere que el tratamiento sea proporcional en relación con el objeto

[909] En su caso, se podría determinar la adopción de estas medidas técnicas como un requisito a cumplir por los beneficiarios en las bases reguladoras de las subvenciones (art. 17 de la Ley 38/2003, de 17 de noviembre, General de Subvenciones).

de la investigación, que el tratamiento se efectúe con arreglo a la normativa nacional (LIB) y, se adopten medidas técnicas y organizativas que aseguren el respeto a los derechos y libertades de los interesados. Sobre esta cuestión el Profesor MEDINA GUERRERO establece que se trata de una condición especifica que pretende salvaguardar los intereses de los particulares[910]. De manera que, de acuerdo con el art. 89.1 del RGPD, se debe prestar especial atención al cumplimiento del principio de minimización de datos, procurando aplicar la seudonimización para el tratamiento aplicable a la investigación siempre que no obstaculice sus finalidades. Y de ser posible en tratamientos ulteriores con esta finalidad que se realice sin la identificación de los interesados. En este contexto como bien señala JOVE VILLARES esta «*pone de manifiesto la importancia que la investigación cobra en el RGPD y abre nuevas posibilidades para el desarrollo de la biomedicina*»[911]. A partir de este nuevo contexto la LOPDGDD ha establecido un nuevo marco aplicable a la investigación biomédica en el apartado segundo de la D.A. vigesimoséptima. En donde se introduce como novedad la creación de un Comité Ético para la investigación que determinará la idoneidad de la reutilización de datos[912] y la utilización de la técnica

---

[910] MEDINA GUERRERO, M., «Capítulo VII. Categorías especiales de datos», RALLO LOMBARTE, A. (Dir.), *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, Tirant lo blanch, Valencia, 2019, p. 256.

[911] *Vid.* JOVE VILLARES, D., «Consecuencias en la ley de investigación biomédica del RGPD», *Revista General de Derecho Constitucional,* núm. 28, 2018, p. 13.

[912] Lo anterior tiene relación con la reutilización de información obtenida a partir de investigaciones financiadas con fondos públicos. Como mencionamos anteriormente, la Directiva 2019/1024 de 20 de junio, relativa a los datos abiertos y la reutilización de la información del sector público es aplicable a los datos obtenidos a partir de la investigación. De acuerdo con lo establecido en el art. 10 de la referida Directiva, los Estados deberán adoptar «Políticas de acceso abierto» de tal manera que se pueda reutilizar los datos con respeto a los «*derechos de propiedad intelectual e industrial, la protección de datos personales y la confidencialidad, la seguridad y los intereses comerciales legítimos de conformidad con el principio "tan abiertos como sea posible, tan cerrados como sea necesario"*», cfr. art. 10 de la referida Directiva. En este contexto las AA.PP. deberán cumplir con los principios de protección de datos del art. 5 del RGPD y procurar que el tratamiento de datos se efectúe minimizando los datos por diseño y por defecto, recurriendo especialmente a la seudonimización de manera que los datos puedan ser reutilizados sin ser anonimizados, pues como recuerda la Profesora ÁLVAREZ RIGAUDIAS, C., «*la completa anonimización no es posible conforme a las reglas de la buena práctica clínica antes citada (ya que no podría proteger la salud del paciente) y no es deseable, ya que esta destruye el valor científico del dato*», *vid.* ÁLVAREZ RIGAUDIAS, C., «Capítulo XXI. Tratamiento de datos con fines de investigación científica y/o médica», RALLO LOMBARTE, A. (Dir.), *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, Tirant lo blanch, Valencia, 2019, p. 731. Aunque como bien apunta el CEPD «*La anonimización permite utilizar los datos sin ninguna restricción, mientras que los datos seudonimizados siguen entrando en el ámbito de aplicación del RGPD*», cfr. CEPD, Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia, 21 de abril de 2020, p. 7.

de seudonimización en la investigación biomédica. Lo cual amplia las funciones del Comité de Bioética de España, previstas en el art. 78 de la LIB. Otra novedad que se prevé en la referida D.A es la incorporación de un delegado de protección de datos a los Comités de ética de la investigación en los ámbitos de investigación de la salud, biomédica y del medicamento[913].

1.6.3 El tratamiento de datos con fines de archivo.

El tratamiento de datos personales con fines de archivo llevado a cabo por las AA.PP. en interés público requiere también que se adopten medidas técnicas y organizativas, pues esta actividad puede suponer el tratamiento de datos, de tal modo que, en la medida de lo posible no permita que el individuo titular de los datos no pueda o sea identificado sin que suponga un perjuicio a esta finalidad. Como establece el art. 26 de la LOPDGDD el tratamiento de datos personales llevado a cabo por las Administraciones públicas «en interés público» estará sujeto a lo previsto en el RGPD y en la LOPDGDD[914]. Especialmente se deberá cumplir con las previsiones especificas contenidas en la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español (LPHE), en el Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, así como la legislación autonómica que resulte de aplicación[915].

---

[913] Es decir que se deberá de integrar también por mandato legal de acuerdo con esta D.A. un delegado de protección de datos al Comité de ética en la investigación del art. 10 de la Ley 14/2011, de 1 de junio, de la Ciencia, la Tecnología y la Innovación, al Comité de Bioética de España del art. 78 de la LIB y a los comités de ética de la investigación con medicamentos (art. 15 del El Real Decreto 1090/2015, de 4 de diciembre, por el que se regulan los ensayos clínicos con medicamentos, los Comités de Ética de la Investigación con medicamentos y el Registro Español de Estudios Clínicos).

[914] En este sentido, como bien apunta el Profesor VALERO TORRIJOS «*debe tenerse en cuenta que el artículo 5.1.e RGPD, aun cuando impide que los datos se conserven por más tiempo del necesario para los fines que justificaron su tratamiento, también autoriza periodos más largos por razones de archivo en interés público*», *Vid.* VALERO TORRIJOS, J., «Protección de datos…», *op. cit.*, p. 436.

[915] En la actualidad estas son las leyes autonómicas que regulan la gestión de los archivos en cada una de ellas: Ley 6/1986, de 28 de noviembre, de Archivos de Aragón; Ley 6/1990, de 11 de abril, de Archivos y Patrimonio Documental de la Región de Murcia; Ley 3/1990, de 22 de febrero, de Patrimonio Documental y Archivos de Canarias; Ley 6/1991, de 19 de abril, de Archivos y del Patrimonio Documental de Castilla y León; Ley 4/1993, de 21 de abril, de Archivos y Patrimonio Documental de la Comunidad de Madrid; Ley 4/1994, de 24 de mayo, de Archivos y Patrimonio Documental de La Rioja; Ley del Principado de Asturias 1/2001, de 6 de marzo, de Patrimonio Cultural (arts. 93 y 94); Ley 10/2001, de archivos y gestión de documentos de Cataluña; Ley 3/2002, de 28 de junio, de Archivos de Cantabria; Ley 19/2002, de 24 de octubre, de Archivos Públicos de

En este caso, son numerosos los responsables del tratamiento de datos personales. Uno de ellos puede ser el Estado, en relación con sus competencias establecidas en los art. 149.1.1 y en el art. 149.1.28 de la CE. Otro de los posibles responsables del tratamiento de los datos personales en virtud de las competencias ejecutivas que le confiere la LPHE en sus respetivos territorios son las CCAA. En algunos esta competencia ha sido asumida en los Estatutos de Autonomía de las CCAA [916]. Las CC.AA. también podrán ser responsables del tratamiento por las competencias propias asumidas en sus Estatutos de Autonomía y en los términos que establezcan en estos, siempre que el patrimonio sea de interés para cada Comunidad Autónoma [917]. Sin perjuicio de la competencia atribuida a los Municipios de proteger y gestionar el patrimonio histórico, de acuerdo con el contenido del art. 25.2 de la LBRL.

Los archivos conglomeran en gran medida el patrimonio documental de un pueblo, los documentos que lo integran normalmente tienen gran valor histórico y forman parte del Patrimonio Documental y Bibliográfico. La LPHE entiende como documentos a efectos de esta a: «*toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos. Se excluyen los ejemplares no originales de ediciones*». Forman parte del mismo: 1) los documentos de cualquier época generados, conservado o reunidos por organismos y entidades de naturaleza

Castilla-La Mancha; Ley 3/2005, de 15 de junio, de Archivos de Valencia; Ley 15/2006, de 17 de octubre, de archivos y patrimonio documental de las Illes Balears; Ley Foral 12/2007, de 4 de abril, de Archivos y Documentos; Ley 2/2007, de 12 de abril, de Archivos y Patrimonio Documental de Extremadura; Ley 7/2014, de 26 de septiembre, de archivos y documentos de Galicia.

[916] Como es el caso de Galicia (Real Decreto 2434/1982, de 24 de julio, sobre traspaso de funciones y servicios del Estado a la Comunidad Autónoma de Galicia en materia de cultura), el País Vasco (Real Decreto 897/2011, de 24 de junio, sobre ampliación de las funciones y servicios de la Administración General del Estado traspasados a la Comunidad Autónoma del País Vasco por el Real Decreto 3069/1980, de 28 de septiembre, en materia de gestión de archivos de titularidad estatal.), la Rioja (Real Decreto 3023/1983, de 13 de octubre, sobre traspaso de funciones y servicios del Estado a la Comunidad Autónoma de La Rioja en materia de cultura) y Madrid (Real Decreto 680/1985, de 19 de abril, sobre traspaso de funciones y servicios de la Administración del Estado a la Comunidad de Madrid en materia de cultura).

[917] Como es el caso de Cantabria (art. 24.6 de su Estatuto de Autonomía), Navarra (art. 44 de la Ley Orgánica 13/1982, de 10 de agosto, de reintegración y amejoramiento del Régimen Foral de Navarra), Aragón (art. 36.1.16 de su Estatuto de Autonomía), Castilla y León (art. 26 de su Estatuto de Autonomía), Castilla-La Mancha (art. 31.1.16.a de su Estatuto), Extremadura (art. 49.1 de su Estatuto), Andalucía (art. 68 de su Estatuto), Murcia (art. 10.1 I y II de su Estatuto), Valencia (art. 31.6 de su Estatuto), Cataluña (art. 33.2 de sus Estatuto), Baleares (art. 10.20 y 21 de su Estatuto) y Canarias (art. 70.2 p).

pública, por personas jurídicas que tengan participación mayoritaria del Estado u otro tipo de entidades públicas o por personas privadas físicas o jurídicas que gestionen servicios públicos; 2) los documentos que tengan un antigüedad mayor a los cuarenta años siempre que estos hayan sido generados, conservados o reunidos en como parte del ejercicio de sus actividades por entidades y asociaciones de naturaleza política, sindical, religiosa, así como por las entidades, fundaciones y asociaciones educativas y culturales de naturaleza privada; 3) aquellos documentos que tengan una antigüedad superior a cien años siempre que hayan sido entidades particulares o personas físicas las que los hayan generado, conservado o reunido; 4) residualmente, todos aquellos que merezcan esa consideración y hayan sido declarados así por la Administración del Estado, sin que se les requiera alcanzar los umbrales de antigüedad detallados con anterioridad.

A su vez, la LPHE entiende como archivo a efectos de esta a «*los conjuntos orgánicos de documentos, o a la reunión de varios de ellos, reunidos en personas jurídicas públicas y privadas en el ejercicio de sus actividades al servicio de su utilización para la investigación, la cultura, la información y la gestión administrativa. Asimismo, se entienden por Archivos las instituciones culturales donde se reúnen, conservan, ordenan y difunden para los fines anteriormente mencionados dichos conjuntos orgánicos*»[918].

El inciso c) del apartado 1 del artículo 57 de la LPHE limita el acceso a determinados documentos en relación con el derecho a la protección de datos personales debido a su contenido. Este límite afecta a la consulta de documentos que son parte del Patrimonio Documental Español. La limitación al acceso a estos documentos tiene que ver con su contenido y riesgos, es por ello que aquellos que contengan datos personales de carácter policial, procesal o clínico no podrán ser consultados si esta pudiera afectar a la seguridad de las personas titulares de los datos que se contienen en los documentos, sus derechos relacionados con la personalidad, tales como el honor, la imagen y la intimidad personal y familiar, a menos de que se haya dado consentimiento expreso de los titulares de los datos o hayan transcurrido veinticinco años de la fecha de la muerte del titular o en caso de

[918] Cfr. Art. 59 de la LPHE.

desconocerse hayan pasado cincuenta años contados a partir de la fecha que contengan los documentos.

El art. 28 del Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso, limita la finalidad del tratamiento en los siguientes términos: «*La información que contenga datos de carácter personal únicamente podrá ser utilizada para las finalidades que justificaron el acceso a la misma y siempre de conformidad con la normativa de protección de datos*». Este mismo artículo se limita a los documentos que contuviesen datos personales, y contempla tres supuestos específicos de acceso, detallando en cada uno de ellos las condiciones o requisitos para el mismo. En el primero de los casos se prevé el acceso a documentos que contengan datos de carácter personal que puedan afectar la intimidad o seguridad de las personas titulares de los mismos, que contuviera datos especialmente protegidos y aquellos que pudieran contenerse en expedientes sancionadores, siempre y cuando se cuente con el consentimiento expreso de las personas afectadas. Es necesario señalar que la limitación al derecho de acceso es plenamente compatible con el contenido del art. 89.2 del RGPD, siempre que sean adoptadas medidas técnicas y organizativas encaminadas al respeto de los derechos y libertades de los interesados, como las previstas en el ENS y en el ENI.

En el segundo de los casos, el acceso a estos documentos se relaciona con determinados plazos temporales y si se cumplen determinadas circunstancias. Se podrá acceder a documentos que contengan datos personales si ha transcurrido el plazo de veinticinco años desde la fecha de fallecimiento de la persona afectada (titular de los datos). Si no fuera posible saber la fecha de su fallecimiento y el documento tuviera una antigüedad superior a cincuenta años, se podrá conceder el acceso siempre y cuando se entienda razonadamente excluida la posibilidad de lesión a la intimidad personal o familiar del fallecido, y de acuerdo con la normativa en protección de datos vigente[919].

[919] Cfr. Art. 28.2 del Real Decreto 1708/2011, de 18 de noviembre.

El tercer supuesto de acceso se prevé en relación con documentos que contengan solo datos nominativos o meramente identificativos siempre que no afecte a la intimidad o seguridad de la persona titular de los datos en los casos que se acredite un interés legítimo o cuando la persona titular haya fallecido [920].

Sin perjuicio de lo anterior, se podrán entregar informaciones si los datos han sido disociados, de modo que, se impida la identificación de las personas titulares de los datos que se contuviesen tales documentos. [921]

2. LAS AUTORIDADES Y ORGANISMOS DE DERECHO PÚBLICO, QUE UTILIZAN O SOLICITAN UN SERVICIO RELACIONADO CON EL TRATAMIENTO DE DATOS.

En este apartado se analizarán las figuras contractuales que pueden utilizarse para cumplir adecuadamente con el contenido del RGPD. Es decir, cuando el tratamiento de datos no pueda llevarse a cabo por la Administración pública directamente y tiene la posibilidad de contratar a un tercero para que este por cuenta de la primera lleve a cabo ese tratamiento como encargado. O, en su caso, si la figura del DPD puede externalizarse al no incorporarlo dentro de la estructura organizativa de la Administración. También en este apartado veremos si un contratista puede a su vez contratar a un tercero para que este desempeñe las funciones de DPD o de responsable del tratamiento y, si en estos casos deben aplicarse determinadas medidas técnicas y organizativas específicas.

2.1 Contrato entre el responsable y el encargado.

El tratamiento de datos personales realizado por cualquier ente del sector público en su calidad de responsable puede encomendarse a otra persona denominada «encargado». Este último tratará datos personales por cuenta del responsable siguiendo sus instrucciones en todo momento. Esta figura es una ficción jurídica heredada por la Directiva 95/46/CE con la que se pretendía según la propuesta de la Comisión de dicha directiva «*evitar una disminución del grado de protección del interesado como consecuencia del tratamiento efectuado por un tercero*

[920] Cfr. Art. 28.3 del Real Decreto 1708/2011, de 18 de noviembre.
[921] Cfr. Art. 28.4 del Real Decreto 1708/2011, de 18 de noviembre.

por cuenta del responsable del fichero»[922]. De acuerdo con lo establecido por el GT29 «*actuar en nombre de alguien significa servir a los intereses de otro y remite al concepto legal de "delegación"*»[923]. Lo cual no implica cambios en las finalidades del tratamiento, ya que siguen siendo las mismas, finalidades que han sido determinadas por en el caso que nos atañe por alguna norma con rango legal que la Administración tenga la obligación de cumplir, motivo suficiente para no considerarse una cesión de datos. Esta figura se traspuso a nuestro ordenamiento jurídico por medio del art. 12 de la hoy derogara LO 15/1999, de 13 de diciembre. Incluso el GT29 determinó que «los encargados» debían cumplir esencialmente dos situaciones básicas para ser considerados como tales: «*ser una entidad jurídica independiente del responsable del tratamiento*» y, «*realizar el tratamiento por cuenta de este*»[924]. Esto permitiría al responsable trasladar los datos al encargado sin que constituyera una cesión de datos[925] y, por tanto, no ser necesario el consentimiento del interesado. Incluso en el régimen de responsabilidades que prevé la LOPDGDD no se traslada al encargado pues de acuerdo con el art. 33.2 establece literalmente lo siguiente: «*Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público*»[926].

---

[922] Comisión de las Comunidades Europeas. COM (90) 314 final, de 24 de septiembre de 1990. «Propuesta de Directiva del Consejo, relativa a la protección de las personas en lo referente al tratamiento de datos personales», p.30. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:1990:0314:FIN (consulta: 15 de abril de 2020).

[923] GT29, Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", adoptado el 16 de febrero de 2010, 28.

[924] *Ib.,* p. 27.

[925] En este sentido el F.D. 4 de la SAN (Sala de lo Contencioso), de 20 de mayo de 2005 (JUR\2005\249468; ECLI:ES:AN:2005:2635), y F.D. 2 de la STS (Sala de lo Contencioso), de 4 de mayo de 2009 (RJ\2009\5165; ECLI:ES:TS:2009:2651).

[926] Régimen aplicable cuando el contratista lleve a cabo incluso contratos de servicios que conlleven prestaciones directas a favor de la ciudadanía, regulado en el art. 312 de la LCSP. En relación con los contratos celebrados entre el contratista-encargado y el subcontratista-encargado no tendrán naturaleza de contratos del sector público, ya que la parte contratante es decir el contratista encargado del tratamiento de los datos personales ni una Administración pública ni un poder adjudicador, aunque el objeto del contrato sea el de una prestación de servicios, por tanto, no le será aplicable el régimen que se establece en la LCSP en sus distintas fases aunque deberán contener

Actualmente la figura del encargado se contempla respectivamente en el art. 28 del RGPD y en el art. 33 de la LOPDGDD. Analizaremos primero el contenido del Reglamento debido a su aplicabilidad directa y al hecho de que en reiteradas ocasiones la LOPDGDD hace referencia al mismo con determinadas matizaciones. A primera vista este precepto solo admite que asuman esta posición aquellas personas que ofrezcan garantías que permitan aplicar medidas técnicas y organizativas conformes al contenido del propio RGPD[927]. Podría pensarse que el apartado 1 del art. 28 restringe el número de personas con las que debe contar el responsable como encargado, sin embargo, en realidad habla de las cualidades que deben reunir aquellas personas que pretendan llevar a cabo la labor de encargado. Lo anterior queda confirmado con el contenido del apartado 2, que supedita la existencia de otro encargado a la autorización previa del responsable. Por las características antes descritas el acto jurídico que rige los derechos y obligaciones del responsable y del encargado del tratamiento sea un contrato. Sin embargo, el apartado 3 abre la posibilidad de que este encargo se lleve a cabo por medio de cualquier otro medio válido en derecho, lo cual habría que ver si es posible compatibilizar con lo establecido para los contratos del sector público en nuestro ordenamiento jurídico. De acuerdo con el considerando 81 del RGPD debe vincular al responsable con el encargado en los siguientes extremos, fijar el objeto, la duración la naturaleza, los fines el tipo de datos personales, las categorías de los interesados, funciones y responsabilidades específicas «*en el contexto del tratamiento que ha de llevarse a*

cláusulas y requisitos que el RGPD y la LOPDGDD establezcan para estas dos figuras (tanto el de representante subcontratista como el de DPD). Esta autorización para tratar los datos por cuenta del responsable puede hacerse para una parte específica de los datos que trata «encargado principal» o bien de manera genérica, en cualquiera de los casos esta autorización deberá constar por escrito. Lo cual no interfiere en la obligación a cargo del encargado «principal» de informar al responsable en el caso que se prevea algún cambio por sustitución o incorporación de un nuevo encargado, para que el responsable a su vez pueda pronunciarse ante alguna de estas dos circunstancias. En cuanto a la responsabilidad del encargado-contratista, parece que tal y como lo menciona NÚÑEZ GARCÍA, J. L. sería «*una suerte de responsabilidad solidaria cuyo fundamento podríamos hallar en la culpa in eligendo, a la que tanto recurre la nueva norma*», NÚÑEZ GARCÍA, J. L., «El encargado del tratamiento», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad*, Reus, Madrid, 2011, p. 327. Parece razonable pensar además que el contratista subencargado del tratamiento de datos personales a su vez deberá contar con un DPD a efectos de que el primero cumpla con sus obligaciones relacionadas con el tratamiento y en general, en relación con el marco jurídico en la materia.

[927] Las garantías para poder implantar medidas técnicas y organizativas a las que hace referencia el reglamento se traducen en: «conocimientos especializados, fiabilidad y recursos», de acuerdo con el Considerando 81 del RGP.

cabo y del riesgo para los derechos y las libertades del interesado». La Sentencia de 16 de febrero de 2005 determinó la necesidad de realizar un contrato entre el responsable del tratamiento y el encargado en los siguientes términos, debe: «*estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido y deberá incluir las especificaciones que el propio precepto legal determina»* [928]. También determina que este tipo de contratos no puede equipararse al contenido de las facturas comprobantes y cartas[929].

El Tribunal Supremo también por sentencia de 4 de mayo de 2009 se pronunció igualmente sobre la necesidad de un contrato y además estableció unos criterios de contenido mínimo que tienen que regular la relación entre el responsable y el encargado del tratamiento de datos, a tenor literal establece que: «*el responsable del fichero debe haber encomendado el tratamiento de los datos mediante un contrato, pactado de forma que permita comprobar su existencia, así como su contenido. En segundo término, dicha convención ha de contener las instrucciones que el responsable del tratamiento impone para el uso de los datos y de las que el encargado no puede separarse. Finalmente, tiene que constar también el fin que legitima la comunicación, que no pueden obviar las partes, quienes, además, han de abstenerse de comunicar los datos a otras personas*»[930]. Por tanto, la falta de un contrato entre ambos agentes intervinientes y la transmisión de datos personales del responsable al encargado se consideraría una transmisión de datos quedando sometido al régimen general previsto para este tipo de acciones en la normativa de protección de datos[931].

---

[928] Haciendo referencia a art. 12.1 de la entonces vigente LO 15/1999, en su F.J. 2 de la SAN (Sala de lo Contencioso), de 16 de febrero de 2005 (JUR\2005\222020; ECLI:ES:AN:2005:901).

[929] Literalmente esto se establece en los siguientes términos del F.D. 4º de la SAN (Sala de lo Contencioso), de 20 de mayo de 2005 (JUR\2005\249468; ECLI:ES:AN:2005:2635): «*contrato al que tampoco pueden ser equiparadas las facturas y comprobantes a que alude la entidad actora en la demanda ni tampoco, en cuanto a la relación jurídica entre la misma y Valoración Corporal, el documento que figura en el folio 216 de la demanda, ya que el mismo es una carta, tal y como incluso se denomina en la demanda y un contrato es, por definición, un negocio jurídico bilateral (con obligaciones recíprocas para ambas partes) al que por tanto no es posible equiparar ningún negocio jurídico unilateral, lo que, como máximo constituiría tal carta*».

[930] F.D. 2 de la STS (Sala de lo Contencioso-administrativo), de 4 de mayo de 2009 (RJ\2009\5165; ECLI:ES:TS:2009:2651).

[931] *Íd.*

En este orden de ideas, cuando un ente del sector público actúe como responsable del tratamiento de acuerdo con los incisos c) y e) del art. 6 del RGPD y necesite contratar el servicio de una persona para hacer frente a sus obligaciones en la materia, a estos contratos cuyo objeto principal o accesorio sea el tratamiento de datos personales les será de aplicación la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público por la que se transponen al ordena miento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (LCSP). Como es el caso de los contratos llevados a cabo entre responsable y «encargado-contratista» y los llevados a cabo entre el «encargado-contratista» y «el encargado-subcontratista».

Debemos recordar que los contratos del sector público pueden estar sometidos al derecho administrativo o al derecho privado, para saber qué régimen le es aplicable debemos ver el objeto del contrato y a la entidad pública que lo celebra como parte, para lo que debemos de acudir a lo establecido por los artículos 25 y 26 de la LCSP[932]. De acuerdo con el apartado 2 del art. 25, a estos contratos les será aplicable la LCSP en lo relativo a su preparación, adjudicación, efectos, modificación y extinción. En cuanto al régimen supletorio de aplicación de la ley, a estos contratos se les aplicarán las leyes administrativas en lo que no esté contemplado en esta ley y, en última instancia las leyes de derecho privado. En el caso de los contratos que estén vinculados a un giro especial de la administración, primero les será aplicable su normativa específica, después la LCSC y

[932] Son contratos sometidos al derecho administrativo, los celebrados por una Administración pública considerada así por el apartado 2 del art. 3 de la misma ley, entre las que se encuentran: a) las administraciones territoriales, incluidas las Ciudades Autónomas de Ceuta y Melilla; b) entidades gestoras y servicios comunes de la Seguridad Social; c) los organismos autónomos, las Universidades y autoridades Administrativas independientes (Como la AEPD); d) las Diputaciones Forales y las Juntas Generales de Territorios Históricos del País Vasco; e)los consorcios y otras entidades del sector público siempre que una o varias Administraciones públicas, Fundaciones públicas o Mutuas colaboradoras con la Seguridad Social financien mayoritariamente su actividad, controlen su gestión o nombren a más de la mitad de los miembros de su órganos de administración, dirección o gestión, teniendo en cuenta además que hayan sido creadas de manera específica para satisfacer necesidades de interés general y carezcan de carácter industrial o mercantil. Ahora bien, el objeto de estos contratos será la realización de una obra, la concesión de una obra, la concesión de servicios, la prestación de un servicio, el suministro o aquellos declarados así por ley que «*tengan una naturaleza administrativa especial por estar vinculados al giro y tráfico específico de la administración contratante o por satisfacer de forma directa o inmediata una finalidad pública*» [Art. 25.1.b) LCSP] comprendida de entre sus competencias.

posteriormente el régimen supletorio en las leyes de derecho privado[933]. En el caso concreto objeto de este epígrafe, la contratación del responsable de protección de datos deberá ajustarse al caso específico según las normas antes descritas.

El encargo de la labor del tratamiento de datos por cuenta del responsable a una persona ajena a la Administración o ente del sector público, se efectué bajo el tipo contractual de servicios. La LCSP ofrece una definición residual en relación con el contenido de los demás contratos previstos en esa ley en su artículo 17, son «*contratos de servicios aquellos cuyo objeto son prestaciones de hacer consistentes en el desarrollo de una actividad o dirigidas a la obtención de un resultado distinto de una obra o suministro, incluyendo aquellos en que el adjudicatario se obligue a ejecutar el servicio de forma sucesiva y por precio unitario. No podrán ser objeto de estos contratos los servicios que impliquen ejercicio de la autoridad inherente a los poderes públicos*»[934]. De acuerdo con la Profesora MENÉNDEZ SEBASTIÁN este tipo de

[933] De manera residual, los contratos a los que se les aplica el régimen de derecho privado deberán tener un objeto distinto a los contratos sometidos al régimen de derecho administrativo pese a estar celebrados por Administraciones públicas. Tienen la misma consideración aquellos contratos que sean celebrados por entidades del sector público que de acuerdo con el contenido del art. 3 y no reúnan las condiciones para considerarle poder adjudicador o siendo poder adjudicador no la parte contratante no sea considerada a efectos de la LCSP como una Administración Pública(art. 26 de la LCSP). Al primer tipo de estos contratos, es decir aquellos que celebren las AA.PP. pero con objeto distinto a una obra, una concesión de obra, una concesión de servicios, un suministro o un servicio, estarán sujetos a lo establecido por la LCSP en relación con su preparación y adjudicación (Se les aplicará el contenido de la Sección 1.ª y 2.ª del Capítulo I del Título I del Libro Segundo de la LCSP. Su régimen supletorio está integrado por las normas de derecho administrativo y en su defecto por las normas de derecho privado en razón de la entidad contratante, de acuerdo con el contenido del apartado 2 del art. 26.2 de la LCSP), en cambio, les serán aplicables normas de derechos privado a cuestiones relativas a sus efectos, modificación y extinción, conforme al art. 26.2 de la ley referida anteriormente. A los contratos celebrados por entes del sector público, pero sin que sean considerados AA.PP. también se le aplicará en cuanto a su preparación y adjudicación lo establecido en Título I de la LCSP. Sin embargo, les será de aplicación a sus efectos y extinción, las normas de derecho privado. Finalmente, el régimen normativo aplicable a los contratos celebrados por entes del sector público que no sean considerados por la LCSP como poder adjudicador, les será aplicable el contenido del Título II del Libro II de la referida ley. Es menester señalar en este punto que la calificación de uno u otro tipo de contrato depende en buena de quién actúe como contratista y del objeto de contrato.

[934] De acuerdo con la Profesora MENÉNDEZ SEBASTIÁN hasta la entrada en vigor de la LCSP con este tipo de contrato «*se pretendía cubrir aquellas carencias especialmente de tipo personal que impiden a la Administración llevar a cabo sus obligaciones, por tratarse, en muchos casos, de actividades que por su alto componente intelectual, así como el grado de conocimiento y especialidad y la titulación que se exige del contratista, deriva de la ausencia de personal funcionarial o laboral que disponga de tales características, pero también físico o material en el resto de supuestos de servicios, y siempre que sea de carácter excepcional u ocasional, en el sentido de no tratarse de una necesidad constante que llevaría a la obligación de dotar de una plaza en la plantilla. En efecto, otra nota relevante de estos contratos es la falta de generalidad, homogeneidad y habitualidad suficientes para incrementar la plantilla existente*

contratos en principio dan respuesta a carencias de tipo personal o de conocimientos [935]. Esta opción puede tener una especial aplicación en aquellas Entidades Locales que con motivo de su actividad traten datos de carácter personal y que por su tamaño o motivos presupuestarios no puedan permitirse incorporar a un encargado de tratamiento de datos.

Ahora bien, ya que hemos determinado el tipo de contrato -de servicios-que se debe llevar a cabo por la Administración pública o ente del sector público responsable del tratamiento datos. Habrá que analizar el contenido de este. Los contratos del sector público como bien sabemos contienen en sus pliegos cláusulas administrativas, es decir, «*documentos que expresan un conjunto de pactos y condiciones definidores de los derechos y obligaciones de las partes del contrato. La normativa sobre contratos públicos distingue los pliegos de cláusulas administrativas "generales" (art. 121LCSP/2017) de los "particulares" (art. 122LCSP/2017)*» [936].

Las condiciones del contrato deben contenerse en los pliegos de cláusulas administrativas particulares, de acuerdo con el contenido del apartado 2 del art. 122 de la LCSP, recientemente modificado por el Real Decreto-ley 14/2019, de 31 de octubre por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Con anterioridad a este cambio solo se hacía referencia al régimen de protección de los datos personales en la D.A. 25ª de la LCSP. En esta última D.A. aún se hace referencia a la LO 15/1999, de 13 de diciembre [937], cuestión

---

en aras de dar respuesta a las mismas, y por lo cual estima más conveniente acudir a la vía externa de la contratación administrativa para cada caso en que sea necesario». En este sentido la autora considera que el art. 17 de la LCSP debió de haberse excluido en la primera parte del artículo 17 lo referente a la concesión de servicios, «*pues no es cierto que toda prestación de hacer consistente en el desarrollo de una actividad o a la obtención de un resultado distinto de una obra o suministro sea un contrato de servicios, sino que podrá ser también una concesión de servicios*», Cfr. MENÉNDEZ SEBASTIÁN, E. Mª, «El contrato de servicios», GIMENO FELIU, J. M. (Dir), *Estudio sistemático de la Ley de Contratos del Sector Público* (en línea), Thomson Reuters Aranzadi, 2018. Disponible en: https://proview.thomsonreuters.com (consulta: 30 de octubre de 2020).

[935] *Íd.*

[936] BERNAL BLAY, M.Á., «Las "leyes del contrato" (los pliegos): Contenido esencial y formas de control», GIMENO FELIU, J. M. (Dir), *Estudio sistemático de la Ley de Contratos del Sector Público* (en línea). Thomson Reuters Aranzadi, 2018. Disponible en: https://proview.thomsonreuters.com (consulta: 30 de octubre de 2020).

[937] En la D.A. 25ª de la LCSP además de referirse a la normativa anterior aplicable a los tratamientos que impliquen el tratamiento de datos, también se hace referencia a la posición que adoptaría el

que pasa por alto el RDL que modifica esta ley para adaptarla al nuevo marco jurídico (RGPD y LOPDGDD).

Pues bien, en el apartado segundo del art. 122 de la LCSP se establece que en aquellos casos que requiera en la ejecución del contrato tratar datos personales por cuenta del responsable deberá contenerse en los pliegos de cláusulas administrativas particulares: 1) la o las finalidades del tratamiento, 2) la obligación del contratista de someterse a lo establecido en la normativa de protección de datos, tanto nacional como europea, 3)la obligación de presentar una declaración sobre la ubicación de los servidores y la ubicación de dónde se pretende realizar tal operación, 4)la obligación de comunicar cambios relacionada con la ubicación de los servidores y el lugar dónde se va a realizar el tratamiento de datos y, 5) si se tiene contemplada la subcontratación de servidores o de los servicios asociados a los mismos, así como el nombre o perfil empresarial y la solvencia técnica o profesional de los subcontratistas. Estas obligaciones son calificadas por la ley como esenciales y su falta de previsión y, por tanto, su incumplimiento sería una causa de resolución del contrato[938].

Adicionalmente también se pueden contener en los pliegos aspectos más concretos sobre el tratamiento de datos personales según la normativa de protección de datos[939], sobre todo si el servicio tiene que ver con el objeto principal del contrato, pues estos serán ley para ambas partes[940]. En concordancia con lo establecido en el apartado 3 del art. 28 del RGPD, el Profesor NÚÑEZ GARCÍA considera que se deberán contener mínimamente ocho obligaciones en el contrato de servicios

contratista, la de encargado del tratamiento de datos, solo que ahora el marco vigente contempla las obligaciones en el RGPD (arts. 28 y 29). También se establece la obligación del contratista de devolver o destruir los datos personales una vez finalizada la prestación contractual al responsable o encargado del tratamiento; en este caso solo conservará los datos debidamente bloqueados con la finalidad de dilucidad responsabilidades de su relación contractual. Finalmente, se contempla la posibilidad de que un tercero trate datos personales por cuenta del contratista debiéndose de cumplir con tres requisitos para su validez: 1) que se haya especificado en el contrato principal entre el contratista y el contratante, 2) que el tratamiento sea llevado a cabo bajo las instrucciones del contratante y 3) que la subcontratación sea formalizada en un contrato. Finalmente, a este tercero subcontratista también se le considerará como encargado del tratamiento a efetos de la normativa de protección de datos.

[938] De acuerdo con el contenido del apartado 2 *in fine* del art. 122, en relación con el art. 211.1.f) de la LCSP.

[939] Relacionados con el contenido de los art.

[940] En este sentido el F.D. 4 de la STS de 27 de mayo de 2009 (RJ\2009\4517; ECLI:ES:TS:2009:3589).

celebrado entre el contratante y contratista para cumplir con lo establecido en materia de protección de datos: a) que el tratamiento de datos se lleve a cabo únicamente siguiendo instrucciones «documentadas del responsable», b) se establezcan obligaciones de confidencialidad, c) se adopten medidas de seguridad apropiadas, d) no recurrir a subencargados sin contar con la debida autorización del responsable, e) asistir al responsable, en la medida de lo posible, en el cumplimiento de la obligación del responsable de responder a las solicitudes relacionadas con el ejercicio de derechos de los interesados, f)ayudar al responsable a cumplir con sus obligaciones en materia de seguridad y de evaluación de impacto, g) a elección del responsable, suprimir o devolver la totalidad de los datos objeto del tratamiento una vez finalice la prestación del servicio, eliminando todas las copias, h) poner a disposición del responsable cuanta información sea precisa para poder demostrar el cumplimiento de estas obligaciones [941]. La AEPD suma a estos requisitos, la determinación de la duración del contrato, la naturaleza del tratamiento, la determinación de los tipos de datos personales, las finalidades de los tratamientos, y las categorías de los afectados, así como las obligaciones y derechos del responsable [942].

El contratante puede solicitarle si lo estima conveniente al contratista como requisito «*la adhesión del encargado a un código de conducta o un mecanismo de certificación aprobado*» con la finalidad de demostrar el correcto cumplimiento de su encargo [943]. Lo anterior podría contenerse en el pliego de prescripciones técnicas del contrato. Por ejemplo, tener una certificación de la norma UNE-ISO 27001 en «Tecnología de la información-Técnicas de seguridad-Sistemas de gestión de la seguridad de la información. Requisitos». En relación con lo anterior, el Tribunal Administrativo de Recursos Contractuales de Castilla y León, han tenido oportunidad de pronunciarse al respecto en el sentido de que «*el contrato debe ajustarse a los objetivos que la Administración contratante persigue para la consecución de los fines que le son propios; y es precisamente a esta a la que*

941 NÚÑEZ GARCÍA, J. L., *op. cit.*, pp. 328-329.
942 AEPD, «*Guía Protección de datos y Administración Local*», p. 30. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf (consulta: 22 de septiembre de 2020).
943 En consonancia con el contenido del art. 28.1 y con lo establecido en el Considerando 81 del RGPD.

corresponde apreciar las necesidades a satisfacer con el contrato y la forma de hacerlo»[944]. Además, no debe perderse de vista que los contratistas que traten información deberán también respetar el contenido en el ENS durante el tratamiento de los datos a fin de cumplir con el principio de integridad y confidencialidad (art. 5.1.f del RGPD). En este sentido el Profesor VALERO TORRIJOS nos recuerda que la D.A. primera de la LOPDGDD «*incorpora l obligación de los contratistas del sector público de respetar el ENS, de manera que una eventual adjudicación a favor de una entidad que no cumpla con dicha exigencia sería inválida y, muy posiblemente, nula de pleno derecho, puesto no se estaría respetando el contenido esencial del derecho fundamental en términos del art. 47.1.a LPAC por remisión del art. 39.1 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público*»[945].

2.2 Contrato entre el responsable y el delegado de protección de datos.

Como hemos visto a lo largo de este trabajo de investigación[946], los responsables y encargados del tratamiento deben contar de manera obligatoria con la figura del DPD, bien en el seno de su organización o externalizar dicho servicio, como consecuencia de su tamaño y de capacidad presupuestaria[947], como forma de satisfacer esa carencia de personal con conocimientos especializados, en este caso en materia de protección de datos. En el caso del encargado sería una obligación accesoria, ya que este tratará datos personales por cuenta del responsable. En este caso concreto, serán datos que el proporciona una Administración pública o un ente del sector público. El apartado 2 del art. 37 del RGPD establece que se puede

[944] F.D. 4 de la resolución 118/2019, de 1 de agosto, del Tribunal Administrativo de Recursos Contractuales de Castilla y León, por la que se estima parcialmente el recurso especial en materia de contratación interpuesto por la Empresa ASPY Prevención S.L., contra los pliegos que han de regir el procedimiento de contratación de los Servicios de Prevención de Riesgos Laborales para la Administración de la Comunidad de Castilla y León.

[945] VALERO TORRIJOS, J., «Protección de datos…*op. cit.,* P. 426.

[946] Específicamente en el epígrafe 2.1 de este Capítulo. En este sentido, es necesario mencionar que el mismo régimen aplicable establecido en la LCSP en relación con el tipo y objeto del contrato analizado en el epígrafe anterior, le será aplicable al contrato que deba celebrar el responsable con un DPD, sin perjuicio de las especificidades que deban incluirse en el mismo debido al tipo de servicio que se requiere.

[947] De acuerdo con lo establecido en GT29. Directrices sobre los delegados de protección de datos. Adoptadas el 13 de diciembre de 2016, revisadas por última vez y adoptadas el 5 de abril de 2017, p. 7 (pp. 28).

designar un solo DPD para «*varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño*». Lo que deja abierta la posibilidad de contar con un solo DPD para una sola Administración, organismo, ente, agencia, consejo, gerencia, comisión, autoridad independiente, etc. Para que la labor de asesoramiento desempeñada por el DPD en protección de datos sea eficiente debe corresponder al tamaño del ente público, al contenido, al tipo de los datos y los medios utilizados en el tratamiento. Al hilo de lo anterior, POVEDANO ALONSO enumera una serie de beneficios que supone la externalización de esta figura entre las que destacan: el acceso a una persona mejor formada de manera inmediata, la reducción del coste para las AA.PP. especialmente se trata de entes locales y evitar cualquier tipo de conflicto de intereses en el desempeño de sus funciones[948]. Otra cuestión añadida a la complejidad de asesoramiento a este tipo de responsables o encargados deviene de los tipos de finalidades que desarrolle un solo ente. Cuanto más grande sea el ente y más finalidades de tratamiento de datos la labor se tornará más compleja.

El GT29 ha determinado que la función de DPD puede realizarse bajo la modalidad de un contrato de servicios, pero es imprescindible que el contratista DPD «*cumpla todos los requisitos pertinentes de la sección 4 de la RGPD (por ejemplo, es esencial que nadie tenga un conflicto de intereses)*»[949]. Es decir, que se deberá seguir con las previsiones generales que contempla el RGPD para su designación, funciones, deberes, derechos y obligaciones. Entre las que destaca su posición de independencia, respecto del responsable del tratamiento de datos personales.

En cuanto a la designación de DPD en Administraciones de menor tamaño, como alternativa al contrato de servicios llevado por cada una de ellas para su

[948] Otros beneficios serían: «*Mayor flexibilidad a la hora de modificar o sustituir al DPD por motivos que no vulneren su independencia. Mejor especialización a la hora de afrontar tareas complejas como evaluaciones de impacto, inspecciones y recomendaciones. Mayor independencia respecto del responsable y del encargado del tratamiento. Permite aportar recursos en otras tareas estructurales y más estratégicas. En el supuesto de puestos de trabajo distantes, algo muy común facilita la designación de un único DPD*», Cfr. POVEDANO ALONSO, D., «Capítulo 11. Especialidades del DPO en el ámbito local: un enfoque práctico», CAMPOS ACUÑA, C. (Dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, Segunda edición, Wolters Kluwer, 2019, p. 435.

[949] GT29, «Directrices sobre el delegado de protección de datos», de 13 de diciembre de 2016, p. 12. Disponible en: https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A (consulta: 20 de mayo de 2020).

designación, se podría recurrir a un convenio de colaboración entre varias AA.PP. o EE.LL. para que un solo DPD examine el cumplimiento del RGPD y de la LOPDGDD. Tal y como lo prevé el Profesor GAMERO CASADO en los siguientes términos: «*así, las Diputaciones provinciales podrían contemplar la dotación de DPDs a disposición de los municipios que lo precisen, en especial cuando sean de pequeño tamaño y les resulte ineficiente (en términos presupuestarios) la dotación de un puesto de plantilla*»[950].Lo cual les permitiría a los EE.LL. cumplir de una mejor forma todas las obligaciones relacionadas con la responsabilidad proactiva, así como atender las reclamaciones de los interesados incluso antes de que estos últimos acudiesen a la autoridad de control competente y en su caso tomar las medidas que estimasen necesarias para reconducir su actuar a lo establecido en la normativa vigente.

[950] GAMERO CASADO, E., «El Delegado de Protección de Datos en las Administraciones públicas: ombudsperson de los datos», JIMÉNEZ DE CISNEROS CID, F.J. *Homenaje al Profesor Ángel Menéndez Rexach*. Thomson Reuters-Aranzadi, Navarra, 2018, p. 280.

CONCLUSIONES

Primera. — La configuración de la web tal y como hoy la conocemos es producto de la incorporación de muchas herramientas tecnológicas que la hacen cada vez más intuitiva y fácil de utilizar por los usuarios. Sin embargo, algunas de estas herramientas solo tienen como finalidad la satisfacción de los intereses de los prestadores de servicios de la sociedad de la información, lo que hace necesario que esta configuración deba realizarse partiendo del respeto a los derechos y libertades de las personas, lo que aún en la actualidad supone una necesidad imperiosa y no es incompatible con la satisfacción de los intereses legítimos de naturaleza económica de los prestadores de este tipo de servicios. Debido a que, actualmente, Internet es el principal medio de comunicación utilizado y la web una herramienta de suma importancia, este binomio supone uno de los mayores retos para el derecho sobre todo por su capacidad de cambio.

Segunda. — Al margen de que la web sea también una herramienta de trabajo imprescindible para muchas personas, mayoritariamente es utilizada para desarrollar la personalidad de sus usuarios, expresarse y mantenerse informado de lo que ocurre en su entorno, esto implica que a través de muchas de las acciones realizadas por las personas mediante la web se puedan producir colisiones de derechos de carácter fundamental, lo que hace necesaria la ponderación de un órgano jurisdiccional para determinar la prevalencia de uno u otro derecho. En este sentido, los órganos jurisdiccionales han trasladado los criterios de ponderación que venían utilizando para resolver las controversias en el «mundo analógico», pues la existencia de este tipo de servicios no cambia el contenido de los derechos fundamentales, aunque en este caso se deberán tomar en cuenta las peculiaridades que presenta el entorno digital y su efecto multiplicador. Lo mismo ocurre si los servicios prestados a través de la web son los que transgreden algún derecho fundamental, en este caso la responsabilidad será de los prestadores de estos servicios siempre y cuando tengan conocimiento efectivo sobre dicha transgresión. La manera de entender el conocimiento efectivo se ha ido perfilando por la jurisprudencia, entendiéndose como tal no solo a las determinaciones de órganos jurisdiccionales competentes sobre la ilicitud de los datos retirándolos o

imposibilitando su acceso, sino también a aquellos otros medios que pudieran hacer efectivo el conocimiento de los prestadores de servicios. En este contexto, se consideran como «otros medios de conocimiento efectivo» a aquellos encargados de moderar el contenido o al sistema de denuncias implementado por los servicios de almacenamiento de datos y por los servicios de motor de búsqueda.

Tercera.— En relación con esta cuestión se debe señalar que, el legislador ha perdido la oportunidad de regular de manera explícita este tipo de mecanismos o de incorporar, por lo menos, criterios de ponderación utilizados para dirimir estos conflictos en la Ley de Servicios de la Sociedad de la Información (LSSI) como podría ser la inclusión de un cuestionario por el que el prestador de servicios en vista de las respuestas dadas por el usuario pueda determinar previo análisis del contenido si considera necesaria su retirada por estimar que el contenido es dañino e ilícito. De modo que con base a las respuestas se pueda resolver a primera vista la potencial existencia de la vulneración al derecho a la intimidad personal o familiar o en su caso al derecho a la protección de datos personales. Aunque generalmente los prestadores de estos servicios ya cuentan con este tipo de herramientas que les permiten conocer de manera efectiva si alguna publicación transgrede los derechos de los usuarios, los criterios para la retirada o no del contenido no son homogéneos pues dependen de cada prestador.

Cuarta. —Entre los derechos de la personalidad el que más resulta afectado por los servicios de la sociedad de la información es sin duda el derecho a la intimidad personal y familiar; pues la mayoría de los servicios prestados en la web introducen publicidad para hacer viable económicamente este modelo de negocio, un claro ejemplo de ello son las cookies, herramientas que recaban información de la navegación de los usuarios. Existen diversos tipos de cookies según su finalidad y temporalidad. Algunas veces son necesarias para mejorar la navegación en la web y en otras ocasiones son introducidas de manera permanente en nuestros dispositivos por agentes diferentes al editor de la página web en dónde se insertan. En relación con el marco jurídico regulador de estas, actualmente se está tramitando en el ámbito comunitario la propuesta de Reglamento denominado *e-Privacy* que complementará el contenido del Reglamento (UE) 2016/679 de Protección de Datos Personales que actualizará entre otras cosas, los términos para recabar el

consentimiento de los usuarios para que el prestador de servicios pueda hacer uso de las cookies, lo que resulta de gran importancia en caso de que el editor de la página web o terceros, utilizasen cookies u otras herramientas que puedan elaborar un perfil detallado de la navegación de las personas. Esta actualización del marco regulatorio de los servicios de la sociedad de la información ya resultaba necesaria desde hace años, pues su última modificación se realizó en el año 2009 (Directiva 2009/136/CE). En este sentido, el Reglamento *e-Privacy* constituye el instrumento jurídico idóneo, pues tendrá aplicabilidad directa y, por tanto, supondrá la aplicación homogénea en toda la UE. Ante este inminente cambio, los servicios de la sociedad de la información han ido adaptándose paulatinamente de manera que no tengan que hacer grandes modificaciones cuando se publique el texto definitivo. Sin embargo, aún se siguen realizando modificaciones a la propuesta, hasta ahora según el texto en proceso el consentimiento de las personas físicas y jurídicas debe otorgarse en los términos de lo establecido en el RGPD, es decir, de manera expresa, informada y para cada finalidad del tratamiento de los datos personales y si es técnicamente posible y factible se otorgará a través de medios electrónicos.

Quinta. — Los derechos a la libertad de expresión y comunicación son un pilar necesario para la democracia pues alientan la participación de los ciudadanos, y permiten el escrutinio de la actuación del gobierno y de la Administración pública. Esto implica que las personas que ejercen algún tipo de cargo o que tengan relevancia o notoriedad en la vida pública del país tienen un mayor deber de soportar críticas relacionadas con el desempeño de sus funciones o actividad. Lo anterior no es óbice para que esté todo permitido al amparo de estos dos derechos, incluso en determinados casos los prestadores de servicios de la sociedad de la información, y no sólo los usuarios, pueden llegar a ser responsables de la vulneración de los mismos por dar difusión a noticias que propicien la transgresión de derechos, tengan contenido ilícito o inciten a conductas violentas frente a determinados colectivos, que pueden derivar en el peor de los casos en conductas tipificadas como delitos. En este sentido es importante señalar que uno de los mayores problemas que presentan los servicios de la sociedad de la información es el alcance que tienen.

Sexta. — El RGPD ha supuesto un hito para el derecho a la protección de datos personales, por medio de este no solo se refuerzan los principios que ya se contenían en la Directiva 95/46/CE, sino que también se añaden nuevos derechos como por ejemplo el de portabilidad y el de limitación de datos. Otra incorporación de gran importancia al RGPD es la responsabilidad proactiva a cargo de los responsables del tratamiento de datos. Con este nuevo modelo no solo estos últimos estarán obligados a cumplir con lo establecido en el RGPD, sino que además deberán demostrar el cumplimiento de los principios del tratamiento. En este sentido, los responsables podrán adoptar aquellas medidas técnicas y organizativas que estimen pertinentes y que, de acuerdo con el contenido del art. 25 se deberán establecer cuando se determinen los medios del tratamiento e incluso durante el mismo procurando la minimización de los datos a través de técnicas como la seudonimización. El contenido de este último precepto supone un gran cambio en cuanto al diseño basado en el respeto al derecho a la protección de datos, lo que implica sin duda la adecuación de las nuevas tecnologías a este marco jurídico siempre que traten datos personales. En este contexto, existen algunas aplicaciones que se pueden considerar *data friendly* como son Snapchat, Wetransfer y Periscope debido al periodo de duración del contenido publicado y su visibilización por otros usuarios. De hecho, esta tendencia a limitar el periodo de duración del contenido publicado y su visibilización por otros usuarios está en alza, siendo algunas de las características implementadas en otras redes sociales como las «*stories*». Respecto al periodo de duración del contenido en la web, hay otras herramientas, como los motores de búsqueda, que pueden dar acceso a información que es obsoleta pero que permanece albergada en algún lugar de la web y que puede contener datos de carácter personal, de manera que también estos se deberán adaptar al nuevo marco jurídico.

Séptima. — En este contexto, la incorporación del derecho al olvido en el Reglamento poco tiene que ver con el contenido de la STJUE de 13 de mayo de 2014, ya que el derecho de supresión es más amplio y genérico, además puede ser ejercido frente a cualquier responsable del tratamiento y no solo frente a los motores de búsqueda, en relación con los enlaces obtenidos por una búsqueda realizada a partir del nombre del interesado. Por lo anterior, parece que el legislador nacional no

conforme con el contenido del art. 17, incorpora a la LOPDGDD (art. 93) el derecho al olvido frente a los buscadores de Internet, el cual es más próximo al contenido de la referida sentencia. Este posibilita a los ciudadanos solicitar la supresión del enlace de manera autónoma tanto a los motores de búsqueda como a los editores de la página web responsables del tratamiento de los datos personales. En relación con la aplicación territorial del derecho al olvido, de acuerdo con la reciente sentencia STJUE de 24 de septiembre de 2019, este solo tiene efectos dentro del territorio de la UE, lo que implica que no se le podrá solicitar a un motor de búsqueda que desindexe la información en un dominio diferente a los que corresponden a los países de la UE.

Octava. —En lo referente al papel de las Administraciones públicas en este contexto de protección y tratamiento de datos, estas tienen una doble acepción, por un lado, existen autoridades administrativas independientes que se encargan de velar y hacer cumplir los principios y derechos establecidos en el RGPD y en la LOPDGDD, y por otro lado, encontramos a las Administraciones públicas que se configuran como responsables del tratamiento de datos personales, pero también sometidas a la ley y al derecho. Esta última acepción no debe entenderse contrapuesta a la primera, pues deben colaborar entre ellas y cumplir con determinadas obligaciones, así como los demás responsables del tratamiento, pero con algunos matices.

Novena. —Todas las autoridades de control de los Estados miembros tienen las mismas funciones y poderes, al margen de que puedan actuar como autoridad de control interesada o principal, cuando se realice una reclamación por un interesado que inicie el sistema de ventanilla única aplicable a tratamientos transfronterizos, lo que es consecuencia del efecto unificador de la normativa y del principio de primacía del derecho de la Unión. De hecho, el RGPD establece un mecanismo de cooperación entre las autoridades de control, con el que se pretende obtener una única resolución aplicable que resuelva una reclamación realizada por el interesado si se tratan sus datos de manera transfronteriza. Este mecanismo es preceptivo y habilitante para poder acceder a los otros mecanismos de cooperación como el de asistencia mutua y el de operaciones conjuntas cuando no se estime pertinente su aplicación. En caso de no encontrar avenencia entre las autoridades de control

participantes en el mecanismo de cooperación la autoridad de control principal deberá solicitar la emisión de una decisión vinculante al CEPD que dirima la controversia para que posteriormente se adopte una resolución en el sentido de la decisión vinculante por la o las autoridades de control. Sin duda, el marco legal que se introduce en el RGPD en relación con la resolución de los asuntos en tratamientos de datos transfronterizos supone para el ciudadano grandes beneficios, ya que estos podrán presentar reclamaciones en su lengua de origen y ante la autoridad de control competente dentro del territorio del Estado miembro en el que resida, lo cual procesalmente aminora las cargas del interesado y reduce los costes de las reclamaciones al no necesitar algún traductor o asesor legal en otro Estado miembro en el que se ubique el establecimiento principal del encargado o del responsable. Los mecanismos antes descritos también son aplicables a las distintas autoridades de control establecidas en el territorio de nuestro país, en este caso la AEPD actúa como autoridad representante de las demás frente al CEPD y es la competente para ejercer sus poderes y funciones en casi todo el territorio nacional, pues las CCAA de Cataluña, País Vasco y Andalucía tienen su propia autoridad de control autonómica, las cuales se encargan de vigilar el correcto cumplimiento de la normativa en la materia cuando el sector público de su comunidad autónoma actúa como responsable del tratamiento de datos. En este sentido, al margen de que las autoridades de control dentro del territorio español deban cooperar institucionalmente, el mecanismo de cooperación del art. 60 del RGPD solo será aplicable para los tratamientos transfronterizos, por lo que una autoridad autonómica o la estatal podrán ser autoridades de control principal. En este contexto, las autoridades autonómicas actuarán como autoridad de control principal, cuando el responsable del tratamiento sea parte del sector público de su competencia y se hayan fijado las finalidades y medios por una ley. Ahora bien, la AEPD será la autoridad de control principal para la tramitación de reclamaciones relativas al ejercicio de derechos de los ciudadanos frente a las demás Administraciones públicas que no cuenten con una autoridad independiente en la materia y para la Administración General del Estado, siempre que se hayan fijado los fines y los medios por medio de una ley. En relación con las reclamaciones que puedan presentarse frente a un ente u organismo del sector público de las CCAA con autoridad de control propia, los ciudadanos deberán de seguir acudiendo a las

mismas para presentarla, pudiendo en muchos casos realizar el trámite a través de la sede electrónica de las mismas, lo cual aminora en gran medida las cargas de los ciudadanos.

Décima. — De manera que las Administraciones públicas también están sometidas al cumplimiento de la nueva normativa en la materia si actúan como responsables del tratamiento deben basar el mismo en uno de los supuestos habilitantes del art. 6, en este caso las principales bases de licitud en el que sustentan dicho tratamiento son: el cumplimiento de un deber legal (art. 6.1.c), el cumplimiento de un interés público o el ejercicio de las competencias que le son atribuidas (art. 6.1.e), además deben quedar plasmadas en una norma comunitaria o nacional, ya que las AAPP cuentan con prerrogativas que impiden que el consentimiento sea otorgado de manera libre por los ciudadanos. Aunque en cumplimiento de un deber legal el tratamiento de datos personales puede realizarse también previo consentimiento informado de los ciudadanos para cada finalidad del tratamiento, como es el caso de los realizados, por ejemplo, con fines de investigación biomédica. La introducción de las bases de licitud contempladas en los incisos c) y e) del art. 6.1 del RGPD realmente no suponen un cambio sustancial para las Administraciones públicas, pues su actuar no puede atender a otros intereses que no sean los generales, además de estar sometidas a la ley y al derecho por mandato constitucional. Sin embargo, la introducción de determinadas obligaciones a cargo de la Administración pública puede suponer un esfuerzo adicional a las medidas ya establecidas en materia de seguridad y correcto cumplimiento de la normativa. Como sabemos, el Esquema Nacional de Seguridad (ENS) creado por la Ley 11/2007 y al que se refiere en la actualidad el art. 156.2 de la LRJSP, establece aquellas medidas técnicas y organizativas que deben adoptarse por el sector público cuando traten datos de carácter personal, estas medidas dependen del tipo de datos, las formas de almacenamiento, los soportes físicos o tecnológicos en los que se almacene, los fines de esa información, etc., lo cual supone un sistema complejo en aras de preservar la seguridad de los datos sean personales o no.

Undécima. — El RGPD prevé con el fin de cumplir con el principio de seguridad de los datos también dos medidas cuanto menos oportunas: la evaluación de impacto y la evaluación de riesgos. La primera de ellas debe realizarse antes de

que se inicie el tratamiento de datos, por ejemplo, cuando se traten datos con nuevas finalidades y se implementen nuevas tecnologías. En el segundo de los casos la evaluación de riesgo puede realizarse de manera periódica una vez que se han implementado medidas técnicas y organizativas y se haya iniciado ya el tratamiento de datos, lo cual permite que se conozcan de manera eficaz pasado un tiempo si las medidas adoptadas inicialmente son adecuadas o si por el contrario se deben reforzar o cambiar. Cabe mencionar que, el ENS solamente será aplicable a las Administraciones públicas, en este sentido si el tratamiento de datos es encargado a un tercero no le será aplicable, sin embargo, la Administración puede fijar algún tipo de criterio adicional encaminado a preservar la seguridad de los datos personales como la adhesión a códigos de conducta del art. 40 del RGPD o a normas de control y gestión de calidad como la ISO/IEC 15408, sobre criterios de evaluación de la seguridad informática.

Duodécima —. Otra de las obligaciones de las Administraciones públicas que se introducen en el RGPD consiste en realizar un registro de actividades de tratamiento, en este caso la D.F. 11.1 de la LOPDGDD ha añadido a la LTAIBG el art. 6 bis. Este último precepto prevé que los sujetos del art. 77.1 de la LOPDGDD (los cuales casi en su totalidad se corresponden a los establecidos en el art. 2.1 de la LTAIBG) tengan la obligación de publicar el inventario de sus actividades de tratamiento. En este sentido, esta información se hará pública en la sede electrónica de cada sujeto obligado o en el portal de transparencia, según sea el caso. Sin lugar a duda el medio resulta idóneo gracias al efecto multiplicador de la web para dar conocimiento de esta información, ya que contribuye a la transparencia en el tratamiento de los datos personales, sin embargo, los sujetos obligados tienen que estar atentos a que el contenido esté actualizado en sus sedes electrónicas, no basta con que se publique la información a través de este medio, los responsables deben realizar una revisión periódica sobre la exactitud de la información que se proporciona al ciudadano, pues de manera contraria, se estará informando erróneamente a los ciudadanos pudiendo tener repercusiones negativas en el ejercicio de sus derechos en la materia, además de constituir una infracción contemplada en del art. 83.4 del RGPD y en el art. 73.n) de la LOPDGDD calificada como grave. Aunque muchas de las Administraciones públicas ya han incorporado a

su portal web o a su sede electrónica esta información, todavía no puede decirse que se haya implementado en su totalidad, ya sea porque no se determinen todos los datos que se requieren hacer saber al ciudadano o mismamente porque no exista un apartado dedicado en la web de algunas administraciones al efecto.

Decimotercera. — Siguiendo esta línea resulta pertinente hacer referencia al sistema de infracciones y sanciones en la materia. El RGPD incluye un catálogo de infracciones y determina los parámetros que deberán tomar en cuenta las autoridades de control para imponer multas administrativas, sin embargo, es la LOPDGDD la que se encarga en el ámbito estatal de establecer una escala de gravedad de estas. Las Administraciones públicas, de acuerdo con la LOPDGDD si cometiesen una infracción en la materia podrán ser acreedoras a una sanción de apercibimiento, tal y como se hacía en el régimen jurídico anterior. El RGPD ha dejado en manos de los legisladores nacionales determinar si las autoridades públicas pueden ser acreedoras de multas administrativas como forma de sanción. En nuestro caso el legislador nacional ha determinado que estas solo podrán ser acreedoras a una sanción de apercibimiento. Sin perjuicio de que esta situación se deba a motivos presupuestarios para cumplir con las finalidades de estas, el apercibimiento no se puede comparar con las cuantiosas multas impuestas a responsables de naturaleza privada en caso de determinarse la comisión de una infracción.

Decimocuarta. — Ahora bien, en relación con el tratamiento de datos automatizado por parte de las Administraciones públicas es necesario señalar que la implementación de la administración electrónica ha supuesto un reto para las mismas tanto *ad intra* como *ad extra*, el traslado de los procedimientos, la forma de comunicarse con los ciudadanos y los efectos jurídicos que supone el uso de tecnologías de la información no ha sido una labor fácil. De acuerdo con la AEPD los datos personales tienen un ciclo de vida que está compuesto por distintas fases en las que interviene la administración como responsable del tratamiento: recogida, almacenamiento, tratamiento, comunicación de datos, conservación y destrucción. Los datos personales que son recogidos con motivo de una solicitud deben ser tratados y conservados por la administración ante la cual se siga el procedimiento, a menos de que se haya efectuado una comunicación de datos con otra

administración pública para obtener datos que ya tengan en su posesión siempre que las finalidades del tratamiento sean las mismas, a menos de que se autoricen legalmente las comunicaciones de datos con fines distintos o se realice un examen previo sobre la procedencia de la transmisión de estos y tengan como finalidad cumplir con algún interés general o el ejercicio de una competencia atribuida legalmente a la autoridad requirente. Una vez finalizado el procedimiento que motivó la recogida y tratamiento de los datos deberán archivarse y conservarse de acuerdo con la ley del Patrimonio Histórico, así como por el Real Decreto 1164/2002, de 8 de noviembre, este último aplicable a los archivos y documentos de la AGE. Los documentos serán eliminados o se procederá a su conservación en un formato distinto al original siempre que no tengan valor histórico o aún cuenten con valor probatorio, es decir, que hasta que no se extingan o prescriban los derechos de los interesados titulares de los datos o personas interesadas no se podrá proceder ni a su eliminación, ni a su cambio de soporte.

Decimoquinta. — Recientemente se han introducido cambios sustanciales en la legislación nacional que afecta a la actividad administrativa en la prestación de servicios públicos y a la relación de los ciudadanos con las Administraciones públicas ante el inminente cambio digital por medio del Real Decreto-ley 14/2019, de 31 de octubre. Este Real Decreto-ley (RDL) modificó la forma de transmitir la información entre administraciones públicas tal y como se describió anteriormente. Por medio de este también se determina que los medios técnicos del tratamiento de datos de las formas de identificación de clave concertada y análogos deben estar en territorio de la UE, salvo que se trate de datos de categorías especiales en cuyo caso deberán de situarse dentro del territorio español. Este último caso se antoja cuanto menos de difícil materialización, ya que los sistemas identificativos de clave concertada hasta ahora existentes no asocian o requieren la recogida o tratamiento de datos personales de categorías especiales; otra cosa es que sean utilizados para acceder a la prestación de algún servicio que sí puede estar relacionado con este tipo de categorías de datos, como podría ser la solicitud de una prestación de carácter social o de servicios sanitarios. Por lo tanto, habilitaría la posibilidad a las Administraciones públicas de celebrar un contrato con el objeto de almacenar datos, lo que implicaría que un tercero se convirtiese en un encargado del tratamiento de

datos, por medio de un contrato regulado por la Ley de Contratos del Sector Público (LCSP), en cuyo caso podrían establecerse medidas análogas a las contenidas en el ENS en la utilización de medios electrónicos para su tratamiento automatizado, lo cual podría incorporarse en la prescripción técnica de dichos contratos. El RDL 14/2019 también ha introducido cambios en la LCSP que refuerzan el contenido del RGPD y la LOPDGDD en la protección del derecho fundamental a la protección de datos personales, pues ahora se considera contenido esencial de los contratos que requieran el tratamiento de datos para su ejecución la inclusión de la obligación de la observancia de la normativa en la materia en las cláusulas administrativas particulares, de acuerdo con el art. 122 de la LCSP.

Decimosexta. — En materia de transparencia y reutilización de datos, el derecho a la protección de datos constituye uno de los principales límites a la información que debe ser proporcionada a los ciudadanos. Sin embargo, este límite no se aplicará con la misma intensidad para la transparencia activa, en cuyo caso a nivel estatal por defecto solo se podrán publicar en la sede electrónica o en su caso en el portal de transparencia aquellos datos identificativos del personal de las AAPP obligadas según la Ley de Transparencia, Acceso a la información pública y Buen Gobierno relacionándolos con el cargo que desempeñen en el organigrama de las AAPP o la relacionada con la información económica y presupuestaria de las mismas, como serían los adjudicatarios de algún contrato sujeto a la LCSP, sin que se considere proporcional la publicación de las firmas de las personas. En la vertiente pasiva de la transparencia, este límite se debe ponderar en razón del tipo y categoría de datos personales que contenga la información a la que se pretenda acceder de acuerdo con el contenido del art. 15 de la LTAIBG. Este límite se aplica también para la reutilización de datos de acuerdo con el contenido del art. 3.4 de la Ley 37/2007, de 16 de noviembre sobre reutilización de la información del sector público cuando en la ponderación realizada según la LTAIBG prevalezca el derecho a la protección de datos. De acuerdo con la Directiva 2019/1024, del Parlamento Europeo y del Consejo de 20 de junio, relativa a los datos abiertos y la reutilización de la información del sector público, recientemente aprobada, se respeta de manera plena lo establecido en el RGPD. En los tres casos anteriormente expuestos, el límite del derecho a la protección de los datos personales no se aplicará si los datos de esta

naturaleza han sido disociados o anonimizados de manera que se rompa la cadena de identificación y no pueda afectar a este derecho fundamental, ni a otros de esta misma naturaleza.

Decimoséptima. — El derecho a la protección de datos personales también supone uno de los principales límites en tratamientos de datos realizados por las AA.PP. en cumplimiento de determinadas finalidades: fines archivísticos, estadísticos y de investigación científica o histórica. En este sentido, el archivo de documentos, la investigación científica y la actividad estadística son finalidades que ayudan a cualquier Estado y a la UE a conseguir y cumplir con los intereses generales, ya que a partir de estas actividades se crea conocimiento que es utilizado mayormente con este motivo. De acuerdo con el principio de limitación, los datos solo pueden ser tratados para cumplir con las finalidades por las cuales fueron recogidos, sin embargo, se permite un tratamiento ulterior si está motivado por las finalidades antes descritas, al considerarlas compatibles con las aquellas que motivaron la recogida de datos. En este caso siempre que este determinado por el derecho de la Unión o por el derecho nacional se podrán excepción el ejercicio de algunos derechos contenidos en el RGPD si su ejercicio supusiese una afectación grave a la consecución de estos fines. Sin embargo, en este caso se deben adoptar aquellas medidas técnicas y organizativas adecuadas encaminadas al cumplimiento del principio de minimización de datos. Incluso en el RGPD se determina que siempre que puedan cumplirse con estas finalidades a través de tratamientos deberá ser realizado sin que se identifique o se haga identificable a los interesados. Lo anterior, podría ser aplicable sin mayor problema al tratamiento de datos con fines estadísticos, no así para el resto de estas finalidades, ya que en muchas ocasiones se requiere identificar al titular de los datos personales, en este sentido sí que podría implementarse la seudonimización separando de la documentación los datos que puedan identificar o hacer identificables a los interesados, siempre que no suponga una alteración de la documentación física o un daño para el patrimonio histórico. Para el caso de la investigación científica realizada con motivos de interés público y financiada con fondos de esta naturaleza, la publicación de los resultados normalmente no incluye datos personales, sin embargo, no significa que no se haya tenido acceso a estos. Por tanto, los agentes que intervienen en la realización de

investigaciones y que utilicen datos personales deberán adaptar dicha actividad al nuevo marco normativo. Además, de acuerdo con la nueva Directiva de reutilización de datos los resultados de las investigaciones financiadas con fondos públicos deberán de ser tan abiertos como sea posible.

Decimoctava. — Finalmente, en relación con la utilización de las nuevas tecnologías como las cookies y redes sociales por las Administraciones públicas es preciso señalar que, aunque las sedes electrónicas de las mismas se configuren de tal manera que solamente sean utilizadas aquellas cookies necesarias para su funcionamiento, se debe tener especial cuidado en la información que se proporciona a los ciudadanos, si no se recogen y almacenan datos por estas. En este sentido la introducción de iconos de redes sociales en la web en la sede electrónica supone la recogida de datos personales y la corresponsabilidad, pero con fines distintos de acuerdo con la STJUE de 29 de julio de 2019, pues para las AA.PP. los fines tendrán fundamento en las normas jurídicas y se realizará de manera general para cumplir la ley, el interés general o con motivo de las competencias que tienen atribuidas. En el caso de que sea contratada una empresa para realizar estadísticas de las visitas a las sedes electrónicas, las AA.PP. deben hacer del conocimiento de esta situación a los ciudadanos a través de la información en el aviso de privacidad, de tal manera que los ciudadanos sepan qué datos son recogidos con esa finalidad. Ahora bien, cuando las administraciones públicas utilizan las redes sociales para dar difusión a la actividad y a los servicios que prestan, estas se adhieren a las políticas de privacidad de las grandes empresas y aunque estas últimas en territorio europeo están obligadas al cumplimiento del RGPD sus fines son principalmente de carácter económico, ya que utilizan publicidad para hacer rentable ese modelo de negocio a través de las cookies, de manera que si los ciudadanos visitan las redes sociales de las AA.PP. con regularidad estas visitas contribuyen al perfil personalizado que realizan las redes sociales a partir de esta tecnología. Es por lo anterior que, se debe tener especial diligencia tanto en el uso de redes sociales como en la contratación de herramientas que puedan ayudar a conseguir otros fines como los estadísticos sobre la visita de las sedes electrónicas.

Decimonovena. — Todo un mundo nuevo de actuación se abre para las Administraciones públicas en relación con el uso de nuevas tecnologías y la

protección de los datos personales, motivada principalmente por la reciente Estrategia Europea de Datos y por el surgimiento de la Propuesta de la Comisión Europea del Reglamento relativo a la gobernanza europea de datos. Esta tesis doctoral soy consciente que tendrá una vigencia limitada en el tiempo, pero no por ello su objeto pierde importancia. Los cambios suceden a gran velocidad y las Administraciones públicas tendrán que modificar sus formas y modos de actuación y de relación con los ciudadanos. El Derecho administrativo deberá ser lo suficientemente dinámico para ofrecer respuestas rápidas que se encuadren, como siempre, en el equilibrio entre los poderes y las garantías y el respeto a los derechos de los ciudadanos. Sin duda, como ya ha ocurrido en otros momentos históricos, el reto es complejo y ambicioso donde se pretende que los datos sean «*tan abiertos como sea posible, tan cerrados como sea necesario*»[951].

[951] Considerando 28 de la Directiva 2019/1024 del Parlamento Europeo y del Consejo de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público. También es parte de la Estrategia Europea de Datos (A. Un marco de gobernanza intersectorial para el acceso a los datos y su utilización).

ANEXO I.

GUÍA DE CONCEPTOS PARA EL SEGUIMIENTO DEL TRABAJO: DERECHO Y NUEVAS TECNOLOGÍAS

1. CONCEPTOS RELACIONADOS CON INTERNET Y LA WORLD WIDE WEB.

Actualmente el uso generalizado de Internet abarca casi todos los aspectos de nuestra vida, esta herramienta tecnológica se ha hecho imprescindible especialmente en el ámbito profesional de algunos. Sin embargo, ¿sabemos cómo funciona?[952] Para responder a la pregunta anterior tendremos que definir el medio donde se desarrollan también nuestros derechos: Internet. El Diccionario de la lengua española lo define como la «*Red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación*»[953]. Tiene su origen en 1969 con ARPANET, un proyecto desarrollado por la *Advanced Research Projects Agency*, que a su vez fue creada por el Departamento de Defensa de los Estados Unidos de América, la cual era «*la primera red sin nodos centrales, de la que formaban parte cuatro universidades estadounidenses: Universidad de California Los Angeles (UCLA), Universidad de California Santa Barbara (UCSB), Universidad de Utah y Stanford Research Institite*

[952] Debemos de hacer énfasis al plantear esta pregunta, ya que no debe ser confundido el término de Internet con Informática. La informática, según GÓMEZ DEL CASTILLO SEGURADO, M.A., es el *«tratamiento de la información mediante máquinas, que son los ordenadores»*, *vid.* GÓMEZ DEL CASTILLO SEGURADO, M.A., «Evolución de la Informática en el ámbito Educativo Español», *EA. Escuela abierta: revista de Investigación Educativa*, núm.4, 2001, p. 144. Es decir, que mediante el uso de los ordenadores se trata información, y respecto a esto DÁVARA RODRÍGUEZ, M.A., nos advierte que *«el tratamiento automático de la información puede someter a los datos, o a la información, a un tratamiento específico e incidir en la intimidad de la persona más allá de su alcance o control»*, *vid.* DÁVARA RODRÍGUEZ, M.A., *La protección de datos en Europa: principios, derechos y procedimiento,* Ed. Asnef, Madrid, 1998, p. 16. Así pues, *Internet* es *«un conjunto "suelto" de miles de redes de computadores a las cuales tienen acceso millones de personas en el mundo»*, *vid.* PRIETO SERRANO, R., «Internet», *Ciencia e Ingeniería Neogranadina*, núm. 1, Vol. 4, 1996, p. 9; que para acceder a esa red se necesita un ordenador, que tenga acceso a la misma (de manera alámbrica o inalámbrica) es decir, *«la suma de muchos medios de transporte que consisten en cables, fibra óptica, señales radioeléctricas, conexiones de satélite, etcétera. En Internet, convergen los universos hasta ahora separados de las redes informáticas, el audiovisual, y las telecomunicaciones», vid.* MUÑOZ MACHADO, S., *La regulación de la red: Poder y Derecho en Internet*, Ed. Taurus, Madrid, 2000, p. 18.

[953] En Diccionario de la lengua española (en línea). Disponible en: http://dle.rae.es/?id=LvskgUG (Consulta: 9 de mayo de 2018).

(SRI)»[954]. Internet, en sus orígenes era considerado como una infraestructura que enlazaba ordenadores[955]; actualmente además de cumplir con esta función, se puede decir que es el mayor medio utilizado para transmitir grandes cantidades de información en sus diversos formatos. Ha cobrado relevancia debido a que su uso es a nivel global y a que está presente en la vida diaria de la mayoría de las personas. De acuerdo con TRIGO ARANDA, en 1982 aparece la primera definición de Internet, como el «*conjunto de internets conectadas mediante TCP/IP*»[956]. Internet como concepto proviene entonces de la contracción de «*Interconnected network* (redes interconectadas)» que es el modelo en el cual estaba basada la ARPANET.

Los protocolos de Internet TCP (*Transmission Control Protocol*/ Protocolo de Control de Transmisión)/IP (*Internet Protocol*/Protocolo de Internet) que hacen posible la transmisión y recepción de la información fueron creados «con la finalidad de contar con un lenguaje común»[957] en la conexión y transmisión de datos entre ordenadores, sin importar la marca y sistema operativo de los mismos[958]. El

[954] Lo que quiere decirse sin nodos centrales es que la información no se concentraba en un solo ordenador el cual transmitía la información del ordenador de origen al ordenador receptor. Esto se hizo así según TRIGO ARANDA, ya que, al Departamento de defensa norteamericano, ya que si se dañaba el ordenador central se podía perder la información, con este modelo la información estaría almacenada en los cuatro ordenadores inicialmente conectado, *vid.* TRIGO ARANDA, C., «Historia y evolución de Internet» (en línea), *Manual formativo de acta*, núm. 33, 2004, p. 2. Disponible en: http://www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf (consulta: 31 de octubre de 2018) y en GÓMEZ DÍAZ, D., «La historia económica en Internet» (en línea), *Historia actual online,* núm. 3, 2003, p. 94. Disponible en: https://dialnet.unirioja.es/descarga/articulo/829457.pdf (consulta: 23 de noviembre de 2017).

[955] BERNERS-LEE, T., *Tejiendo la red.* Edición traducida de RUBIO FERNÁNDEZ, M., Weaving the WEB: The Original Desing and Ultimate Destinity of the World Wide Web by Its Inventor, Madrid, Siglo veintiuno de España Editores, 2000, p. 17.

[956] TRIGO ARANDA, C., *op. cit*., p. 2. Estos dos protocolos son parte del carácter definitorio de Internet, LÓPEZ ZAMORA lo hace evidente cuando se trata de definir a este medio de comunicación, el cual consiste en «*una red de ordenadores que usan protocolos TPC/IP*», *vid.* LÓPEZ ZAMORA, P., *El ciberespacio y su ordenación*, Grupo difusión, Madrid, 2006, p. 15.

[957] ESTRADA CORONA, A., «Protocolos TCP/IP de Internet» (en línea), *Revista Digital Universitaria,* México, núm. 8, vol. 5, 2004, p. 4. Disponible en: https://biblat.unam.mx/es/revista/revista-digital-universitaria/articulo/protocolos-tcpip-de-internet (consulta: 14 de mayo de 2018).

[958] Dentro de internet no solo existen solo estos dos protocolos que cumplen con una funcionalidad específica dependiendo del servicio que se preste dentro de Internet. VILLAR PALASÍ establece que «*que constituyen la norma para la intercomunicación entre ordenadores de cualquier naturaleza y a través del medio que sea: teléfono, satélite artificial, fibra óptica, cable coaxial, ondas de radio, etc. Existen protocolos singulares para usos específicos: correo electrónico (el popular e-mail, humorísticamente bautizado como Emilio) que tiene su protocolo propio (SMTP, Simple Mail Transfer Protocol), el envío o transferencia de ficheros o bases de datos (FTP, File Transfer Protocol), y otros. Como es bien sabido, los que más directamente afectan a Internet son el Internet Protocol (IP) y el Transmision Control Protocol (TCP)»,* Cfr. VILLAR PALASÍ, J.L., «Nombres de dominio y Protocolo de internet», CREMADES, J., FERNÁNDEZ-ORDÓNEZ, M. Á. y ILLESCAS, (Coord.), *Régimen jurídico de Internet*, Ed. La ley, Madrid, 2002. p. 395.

primero de estos protocolos hace posible la comunicación en línea, cuenta con diversas funciones como la transmisión de ficheros electrónicos, se hace cargo de dividir la información para el envío, realiza la detección de errores y se encarga de reconstruir la información enviada[959].

El protocolo IP o dirección IP es «un número único para cada equipo o "host", representado por cuatro cifras separadas por puntos, quedando determinado 255 como límite» [960], es decir, es un identificador, ya que «se hace cargo de la domiciliación de la información»[961], identifica el ordenador conectado a Internet que ha solicitado la información para enviarla como respuesta a la petición. El Tribunal de Justicia de la Unión Europea (TJUE) acorde con la descripción técnica ha definido a las direcciones IP como «secuencias de números que se asignan a los ordenadores conectados a Internet para que estos puedan comunicarse entre sí a través de esa red»[962].

[959] Tal y como lo describe LÓPEZ ZAMORA, el protocolo TCP, lleva a cabo «*la transmisión de ficheros electrónicos, divide la información en porciones apropiadas y numeradas para que puedan volver a unirse en su totalidad, o de haber (…) algún error en la transmisión, permite identificarlo al instante. Asimismo, lleva a cabo la labor de la recomposición de la información*», Cfr. LÓPEZ ZAMORA, *Ib.,* p. 16.

[960] ESTRADA CORONA, A., *op. cit*., p. 4. De conformidad con lo establecido por la IANA (*Internet Assigned Numbers Authority)* Autoridad de Números Asignados en Internet, actualmente existen dos tipos de IP: IPv4 y IPv6 *vid.* https://www.icann.org/es/system/files/files/iana-functions-18dec15-es.pdf (consulta y descarga: 11 de noviembre de 2018) . Las direcciones de Internet IPv4, están integradas como se describió antes sin embargo la estructura de las IPv6 «*tiene una arquitectura más complicada (…). El formato del texto de la dirección IPv6 es: xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, donde cada x es un dígito hexadecimal que representa 4 bits*», además de poder estar «*correlacionada*» con una IPv4, *vid.* IBM, comparación de IPv4 y IPv6. Disponible en: https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_73/rzai2/rzai2compipv4ipv6.htm#rzai2compipv4ipv6__compdns (consulta: 11 de noviembre de 2018). Una dirección IPv6 «*permite disponer de un número casi ilimitado de direcciones IP*», *vid.* RODRÍGUEZ RAPOSO, A., «Los nombres de dominio de internet: Presente y futuro de la situación de España» (en línea), *Economía industrial*, núm. 338, 2001, p. 72. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=266339&orden=197762&info=link (consulta: 14 de noviembre de 2018).

[961] LÓPEZ ZAMORA, P. *Ib.,* p. 16. VILLAR PALASÍ, J. L. nos ofrece una explicación del por qué esta secuencia de números no puede superar el 255 en cada uno de sus niveles: «*el conjunto TCP/IP es conocido como la "doted notation", una secuencia de cuatro números separados por puntos, cada uno de los cuales está formado por ocho bits. Dado que el sistema binario, base de toda computación moderna, con ocho bits sólo permite formar 256 números (2 elevado a 8), ninguno de los cuatro números puede superar esta cifra. El TCP/IP forma con los números indicados una estructura de direccionamiento, a modo de la que llevan las cartas: ciudad, distrito, calle, número*», *vid.* VILLAR PALASÍ, J.L., *op. cit*., p. 394.

[962] Esta definición corresponde a la de Dirección IP estática, Cfr. TJUE, Sentencia de 19 de octubre de 2016, asunto C-582/14, Patrick Breyer y Bundesrepublik Deutschland (JUR\2016\268783; ECLI:EU:C:2016:779).

Es menester señalar que las direcciones IP en su origen siempre eran estáticas debido a que el acceso a Internet se realizaba por medio de un módem conectado a un ordenador de sobremesa o portátil según se diera el caso; hoy en día el acceso a diversos servicios dentro de Internet como el *World Wide Web*, aplicaciones o servicio de *e-mail*, se realiza por medio de nuestros dispositivos móviles, es por ello que también existen las direcciones IP dinámicas las cuales cambian «*con ocasión de cada nueva conexión a Internet (…) no permiten relacionar, mediante ficheros accesible al público, un ordenador concreto y la conexión física a la red utilizada por el proveedor de acceso a Internet*»[963].

Con el paso del tiempo el sistema de interconexión de ordenador a ordenador fue cambiando a medida que fue extendiéndose, su funcionamiento actualmente se realiza a través de ordenadores centrales denominados «servidores», en palabras de MARTÍNEZ AYUSO su funcionamiento responde generalmente a una serie de ordenadores que «*permanentemente dan servicio (llamados por ello servidores) a las computadoras de los usuarios (llamados clientes) que puntualmente acceden a esa red»*[964]. Sin embargo, como bien apunta TALENS OLIAG «*Generalmente la conexión es indirecta y en este caso, puede ser de dos formas. La primera es conectarse a una red local a una máquina que este directamente enganchada a Internet. Esto es lo que ocurre en las organizaciones (universidades y multinacionales) que tienen una red propia en la que sólo una o varias máquinas están conectadas y sirven como pasarela e Internet para todas las demás. La otra forma es haciendo uso de un módem y conectándose a un proveedor*»[965].

---

[963] Apartado 16, de la STJUE, de 19 de octubre de 2016 (JUR\2016\268783; ECLI:EU:C:2016:779).

[964] MARTÍNEZ AYUSO, M. Á., «Las redes P2P y la descarga ilegal de contenidos», *Revista Aranzadi de Derecho de Deporte y Entretenimiento* (en línea), núm. 18/2006, 3 parte secciones, p. 2 (consulta: 5 de noviembre de 2018). BIB 2006\1788.

[965] TALENS OLIAG, S. Y HERNÁNDEZ ORALLO, J., *Internet. Redes de computadores y sistemas de información,* segunda edición, Ed. Paraninfo, España, 1998, p. 29. Otro artículo que explica de manera sencilla el funcionamiento de Internet, pero completa es el realizado bajo la autoría de GARCÍA MARTÍNEZ, A. T., Estructura Tecnológica e Institucional de Internet (en línea), en *Puertas a la lectura,* núm. 17, 2004. Disponible en https://dialnet.unirioja.es/descarga/articulo/1071306.pdf (consulta 3 de diciembre de 2018). Esta autora realiza una metáfora para explicar el funcionamiento de Internet: «*donde se pueden considerar los ordenadores como ciudades y los cables como carreteras que comunican unas con otras, por lo que se crearía una red de tráfico varia done para enviar datos de un ordenador a otro deberá pasar por muchos ordenadores intermedios, dependiendo de la ubicación geográfica del ordenador», íb.,* p. 7.

1.1 El correo electrónico

Uno de los servicios de Internet más conocido y utilizado en la actualidad para comunicarnos es el correo electrónico, aunque en los últimos años se ha visto desplazado por nuevas plataformas de comunicaciones electrónicas móviles. El correo electrónico lo creó el ingeniero RAY TOMLINSON, en 1971 «*para enviar mensajes entre ordenadores que (…), formaban parte de ARPANET. También se debe a Tomlinson empleo del popular símbolo @. Enseguida advirtió que necesitaba un carácter para separar el nombre del usuario y el nombre del servidor y, para evitar confusiones, era conveniente que dicho carácter no fuese muy usual*»[966]. Al principio, se necesitaba un *software* especial instalado en el ordenador para poder enviar y recibir *mails*[967].

Posteriormente como resultado del avance tecnológico de la *World Wide Web,* una serie de proveedores de mensajería electrónica lanzaron plataformas que permitían el uso de este servicio mediante una página Web. La falta del uso de un *software* específico para recibir y enviar e-mails supuso también un cambio en el comportamiento de los usuarios de Internet, ya que de esta forma se podía tener acceso al correo electrónico desde cualquier ordenador en cualquier sitio como *Hotmail*, *Yahoo!* o *Gmail*, entre otros[968], lo único que tenía que hacer el usuario para poder acceso a este servicio era registrarse en la plataforma proporcionando algunos de sus datos.

Existen también proveedores de servicios de correo electrónico, que han apostado por la privacidad de sus usuarios, cuando de comunicaciones electrónicas se habla, quizás el ejemplo más destacable sea *ProtonMail.* El cual fue creado en el

[966] TRIGO ARANDA, V., *op. cit*., p. 8 (consulta: 14 de diciembre de 2018).
[967] Como Outlook de Microsoft, en la actualidad todavía es utilizado por un gran espectro de usuarios.
[968] Hay tantos proveedores de servicios de correo electrónico como imaginemos, la mayoría trabaja a través de una plataforma web, sin embargo, la seguridad en las comunicaciones y menos de este tipo, suelen estar al cien por cien aseguradas, ya que de por sí el uso mismo de la web supone riesgos en nuestra privacidad, es un espacio donde todos somos vulnerables también a ataques cibernéticos. A modo de ejemplo, encontramos algunos servicios alternativos al consolidado correo de *Gmail*: Zoho mail, ProtonMail, Tutanota, GMX, Newton, MailDrop, Yambuu y Hushmail, los cuales en mayor o menor medida han mejorado la privacidad de los usuarios. Cfr. El País, Más allá de Yahoo, Outlook o Gmail: estos son los correos alternativos. Disponible en: https://elpais.com/tecnologia/2017/10/11/actualidad/1507722458_050123.html (consulta: 18 de diciembre de 2018).

año 2004 por científicos, ingenieros y desarrolladores del Consejo Europeo para la investigación nuclear (CERN) [969], y actualmente tiene su sede en Suiza [970]. Se autodefine como un «*un servicio de correo electrónico seguro, fácil de usar, con cifrado de extremo a extremo incorporado y características de seguridad de última generación. Nuestro objetivo es crear una internet que respete la privacidad y sea segura contra los ciberataques. Estamos comprometidos a desarrollar y distribuir ampliamente las herramientas necesarias para proteger tus datos en línea*» [971]. Algunos de los beneficios que supone hacerse una cuenta en ProtonMail son: el cifrado de extremo a extremo, el uso de criptografía de código abierto, no se utilizan servicios *Cloud Computing*, los datos se almacenan en Suiza, no hay seguimiento en las comunicaciones e incluso se puede configurar este servicio para que los mensajes se autodestruyan [972]. Este servicio tiene un producto gratuito y otros de pago, con lo cual los usuarios pueden elegir qué tipo de cuenta se ajusta a sus necesidades y actividad. Hasta septiembre de 2018, este proveedor de servicios de correo electrónico ya contaba con cinco millones de usuarios [973].

1.2 World Wide Web, Deep Web y Dark Web.

Actualmente es común el uso indiscriminado de términos de Internet o Web, para referirnos a ese espacio virtual donde es posible encontrar cualquier tipo de información y contenido, para un usuario medio Internet está compuesto por un montón de páginas de diversa índole en un espacio intangible, pero también es el

[969] Siglas del francés: *Conseil Européen pour la Recherche Nucléaire.*

[970] Los creadores consideran que es de suma importancia la privacidad de los usuarios a nivel informático y legal, es por ello que han decidido establecerse en Suiza, por lo cual: «*Todos los datos del usuario están protegidos por la Ley Federal Suiza de Protección de Datos (DPA) y la Ordenanza Federal Suiza de Protección de Datos (DPO) que ofrecen la mayor protección de privacidad en el mundo para personas y empresas. Como ProtonMail está fuera de la jurisdicción estadounidense y europea, solo una orden del Tribunal Cantonal de Ginebra o de la Corte Suprema Federal Suiza puede obligarnos a entregar información limitada de los usuarios*», es por ello, que sus creadores consideran al Derecho Suizo más proteccionista en la materia, *vid.* Protonmail, Detalles de seguridad. Disponible en: https://protonmail.com/es/security-details (consulta: 18 de diciembre de 2018). Como consecuencia de esto, es inevitable pensar en las consecuencias que traería el mal uso de este tipo de servicios, sobre todo porque su configuración responde a las capas de encriptado que también se utiliza en la *Red Tor*.

[971] *Vid.* Protonmail. Disponible en: https://protonmail.com/es/about (consulta: 18 de diciembre de 2018).

[972] *Vid.* Protonmail, «Detalles…», *op. cit.*

[973] De conformidad con lo establecido en KOBEISSI, N., «An Analysis of the ProtonMail Cryptographic Architecture» (en línea), *Cryptology ePrint Archive:Report 2018/1121.* Disponible en: https://eprint.iacr.org/2018/1121 (consulta: 18 de diciembre de 2018).

servicio que ofrecen las empresas (normalmente relacionadas con servicios de telefonía) para que por medio de la instalación de un *router*[974] se pueda tener tienen acceso Internet.

Es necesario señalar que Internet se creó con anterioridad a las páginas Web. Internet es el medio y en las páginas Web encontramos contenido[975] en diferentes formatos, como imágenes, vídeos, sonidos, enlaces[976] a otras páginas de Web o simplemente información escrita. TIM BERNERS-LEE, el padre de la Web, desarrolló esta herramienta tecnológica a partir de una idea que tuvo cuando trabajaba en el CERN[977], sobre la creación de un espacio donde toda la información almacenada en los ordenadores pudiese estar disponible para cualquiera, creándose «*un espacio único y global de información*»[978], y así es como diseño el *Enquire* original. Estaba basado en nodos, se «*podía escribir una página de información acerca una persona, un aparato o un programa. Cada página (…) como una tarjeta de un fichero. El único*

---

[974] Pueden ser definidos como aquellos dispositivos que «*permiten las conexiones entre dos o más redes y seleccionan las rutas por las que envían los paquetes de información*», de conformidad con lo establecido en MIGUEL ASENCIO, P. A. DE., «Caracterización y organización de Internet: perspectiva jurídica» (en línea), *Derecho Privado de Internet.* Aranzadi, enero, 2015, p. 2 (consulta 14 de diciembre de 2018). BIB 2015\8. Técnicamente se trata de «*Un módulo simple que actúa como multiplexor de diversas fuentes TCP/I*P», y que cumple con diversas funcionalidades como «*recibir paquetes TCP/IP procedentes de módulos TCP/IP, almacenarlos (…) y reenviarlos hasta el enlace de salida hacia el módulo de NodoDestino*», así como en un sentido inverso de la comunicación, de conformidad con lo establecido en AGEA LÓPEZ, E., ALCARAZ ESPÍN, J. J. Y GARCÍA HARO, J., Propuesta de Trabajos de Practicas: Simulación de los mecanismos de control de congestión en TCP/IP (en línea), *Escuela Politécnica de Cartagena, Escuela Técnica Superior de Ingeniería de Telecomunicación*, p. 10. Disponible en: http://www.upct.es/~orientap/TCP.pdf (consulta 14 de diciembre de 2018).

[975] LÓPEZ ZAMORA señala que «*La World Wide Web es solamente uno de los servicios de Internet, aunque el más importante, no es el único. La WWW es el más ambicioso proyecto de presentación y catalogación de información en línea basado en un documento. La información, en lugar de estar organizada linealmente lo está como un conjunto de objetos multimedia, cada uno de los cuales remite a otros objetos relevantes. Se trata de un sistema de información hipertextual con enlaces entre los diversos ordenadores conectados a Internet*», *vid.* LÓPEZ ZAMORA, *op. cit*., p. 17.

[976] O también denominados *links* es «*un código HTML que permite, mediante un simple clic del usuario, abrir un archivo o una página, que ya se encuentra dentro del mismo sitio web (link interno) o de otro destino (link externo). El link a su vez puede estar representado por palabras (por ejemplo, un texto o la dirección web a la que se reenvía) o imágenes (fotografías, logos, etc.). debemos tener claro que un enlace cuenta con dos extremos. Sin embargo, el término "enlace" a menudo se utiliza para el ancla origen, mientras que el ancla destino se denomina "enlace de destino" (link target) o "hiperenlace". El enlace de destino más común es un URL, utilizado en la World Wide Web*», Cfr. ORTEGA DOMÉNECH, J., «La difícil convivencia del derecho de cita en el mundo de los enlaces digitales», *Anuario de Propiedad intelectual*, núm. 2011, 2012, pp. 430-431.

[977] Según BERNERS-LEE, ahora, aunque la institución sigue existiendo, ya no define la física que se lleva a cabo ahí. La idea de Berners-Lee, era la siguiente: «*Supongamos que toda la información almacenada en ordenadores de todas partes esté unida entre sí, (...) supongamos que pueda programar mi ordenador para crear un espacio en el que cualquier cosa pueda relacionarse con cualquier otra*». En BERNERS-LEE, *op. cit*., p. 4.

[978] BERNERS-LEE, T. *Íd.*

modo de crear un nuevo nodo era hacer un vínculo a partir de un antiguo nodo. Los vínculos que salían o llegaban a un nodo aparecían como una lista enumerada al pie de cada página, de forma bastante parecida a la lista de referencias al final de un informe académico»[979].

Años más tarde, partiendo del proyecto *Enquire* e introduciendo la idea del hipertexto[980], «un sistema de interconexión»[981], es como nace el *World Wide Web* en el año 1989[982]. El *World Wide Web*, es «un conjunto de documentos de hipertexto[983] y/o hipermedios enlazados y accesibles a través de Internet. La WWW es un sistema distribuido que nos permite navegar con facilidad a través de cantidades ingentes de información. Con un navegador Web, un usuario visualiza páginas que pueden

[979] *Ib.,* p. 9.

[980] Tal y como apunta BERNERS-LEE, de acuerdo con Tom Nelson: «*Ted Nelson, un visionario profesional, escribió en 1965 acerca de "Máquinas literarias", ordenadores que permitirían a la gente escribir y publicar en un nuevo formato no lineal, que llamó hipertexto. El hipertexto era un texto "no secuencial" en el que un lector no estaba obligado a leer en un orden determinado, sino que podía seguir nexos de unión y llegar al documento original a partir de una breve cita (…) En la visión de Ted cada cita tendría un vínculo que la devolvería a su fuente, permitiendo a los autores originales ser compensados con una pequeña cantidad cada vez que se leyese la cita. Tenía el sueño de una sociedad utópica en la que toda la información pudiese ser compartida entre gente que se comunicaba entre sí como entre iguales. Lucho durante años para encontrar financiación para ese proyecto, pero no encontró el éxito*», *vid.* BERNERS-LEE, T. *ib.*, p. 5. Sin embargo, autores como CÁCERES ZAPATERO, *et al.,* le atribuyen la idea del Hipertexto a Vannevar Bush (1945) quien desarrollo el proyecto «Memex», el cual era una máquina considerada como una «*biblioteca mecánica capaz de contener toda la información interesante para las personas*», este posibilitaba «*tener acceso a la información de forma asociativa, uniendo partes de los documentos entre sí*», Cfr. CÁCERES ZAPATERO, Mª D., *et al.*, «Construcción social de la realidad en los nativos digitales: una revisión teórica desde la perspectiva narrativa»(en línea), *Prisma Social. Revista de ciencias sociales*, núm. 3, junio 2010. Disponible en: https://www.researchgate.net/publication/277262741_Construccion_social_de_la_realidad_en_los_nativos_digitales_Una_revision_teorica_desde_la_perspertiva_narrativa (consulta 4 de diciembre de 2018).

[981] NAIK, U. y SHIVALINGAIAH, D., «Comparative Study of Web 1.0, Web 2.0 and 3.0» (en línea) Disponible en: DOI: 10.13140/2.1.2287.2961 (consulta 27 de noviembre de 2018).

[982] De conformidad con lo que establece MENON, S., *et al.*: «*Web was founded in the year 1989 by Tim Berners-Lee», vid.* MENON, S., *et al.*, «Progression of Web 3.0 (semantic Web) from Web 1.0: A survey» (en línea), 2009, pp. 5. Disponible en: https://www.researchgate.net/publication/305443181_PROGRESSION_OF_WEB_30SEMANTIC_WEB_FROM_WEB_10_A_SURVEY (Consulta: 17 de mayo de 2018).

[983] El hipertexto puede ser definido como «*un sistema mecánico (computarizado) de lectura y escritura, en el que el texto se organiza mediante una red de fragmentos y las conexiones existentes entre ellos*», definición de AARSETH ESPEN, Cfr. GARCÍA GUARDIA, Mª L., GARCÍA GARCÍA, F y NÚÑEZ GÓMEZ, P., «Teorías sobre el hipertexto» (en línea), *Admira,* núm. 1, p. 143. Disponible en: https://idus.us.es/xmlui/handle/11441/76104 (consulta 4 de diciembre de 2018).

contener texto, imágenes, vídeos u otros contenidos multimedia, y navega a través de ellas usando hiperenlaces»[984].

La *Web 1.0* estaba formada de una serie de páginas *Web* estáticas y programadas por *Hipertext Mark Lenguaje* (HTML)[985] «*cuyo principal activo es el texto*»[986]. Esta primera generación de páginas Web, necesitaban otros dos recursos además de la configuración HTML, para hacer posible y fácil la transmisión y acceso a la información de ese espacio virtual, estos son, el Protocolo de Transferencia de Hipertexto (HTTP, *Hipertext Transfer Protocol*)[987] encargado de hacer posible la transmisión y visualización de la información solicitada y enviada, y el Identificador de recursos universal (URI, *Uniform Resource Identifier*), que como su propio nombre lo dice servía para identificar el tipo de protocolo de comunicaciones, el servidor y en su caso el recurso específico solicitado, el cual posteriormente paso a denominarse Localizador Uniforme de Recursos (*Uniform Resource Locator* - URL)[988], el cual también tiene la funcionalidad de localizar contenidos.

Estos recursos electrónicos funcionan a modo de engranaje en la Web diariamente. El creador de la Web nos ofrece un ejemplo sobre la funcionalidad de

---

[984] ABUÍN VENCES, N. Y VINADER SEGURA, R., «El desarrollo de la World Wide Web en España» (en línea), *Razón y palabra*, núm. 75, 2011, p. 5. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3689999&orden=304611&info=link (consulta: 4 de diciembre de 2018).

[985] Este formato permitía a los ordenadores sin importar el software que utilizasen transmitir la información, un formato accesible para todos, BERNERS-LEE creador de la WWW determina que «*cuando dos ordenadores se ponen de acuerdo de representar sus datos para poder compartirlos. Si usan el mismo software para documentos o gráficos pueden compartirlos directamente. Si no, pueden traducirlos ambos a HTML*», Cfr. BERNERS-LEE, T., *op. cit.,* p. 34. Así también lo establece MENON, S., *et al.*: «*It consisted of static pages. Once information on a particular page is over, the users must get connected to external links to wiew further information*», MENON, S., *op. cit.*

[986] DAVARA FERNÁNDEZ DE MARCOS, L., *Implicaciones Socio-Jurídicas de las Redes Sociales,* Ed. Aranzadi, Navarra, 2015, p. 39.

[987] El Http es el Protocolo que se utiliza para transferir archivos, supone un lenguaje universal para que los clientes se puedan comunicar con los servidores, para un análisis más profundo de cómo es que se realiza este protocolo respecto a la transferencia de archivos, véase BERNERS-LEE, T., *op. cit.*, pp. 38-39. Actualmente el protocolo HTTP, en la mayoría de las páginas Web ha sido sustituido por el HTTPS el cual significa *Hypertext Transfer Protocol Secure*, debido a la seguridad que ofrece a los usuarios la transferencia mediante este Protocolo.

[988] Como su nombre lo indica sirve para localizar contenidos, es un esquema de dirección estandarizado a través de un navegador Web, de esta misma manera lo determina NAVARRO SCHLEGEL, A. *Diccionario de términos de comunicaciones y redes. Ed. Pearson Educación, Madrid, 2003, p. 358.* Tiene la función de especificar «*primero, mediante el protocolo correspondiente («http», «fhp», «mailto»), la aplicación electrónica deseada y, después, la dirección concreta del ordenador con el que se quiere conectar; también pueden añadirse referencia de archivos o directorios específicos siempre que se conozcan*» de conformidad con CARBAJO CASCÓN, F., *Conflictos entre signos distintivos y nombres de dominio en Internet*, Ed. Aranzadi, Navarra, 1999, p. 35.

cada uno de estos conceptos*: «"http://www.foobar.com/doct1", el www.foobar.com define el servidor real donde esos documentos existen. Doct1 es un documento específico en el servidor www.foobar.com (puede haber cientos, cada uno con un nombre diferente tras la barra simple). Las letras que hay antes de la doble barra significan el protocolo de comunicaciones que usa ese servidor… la última parte del URI significa cualquier cosa que un servidor determinado quiera que signifique. No tiene que ser un nombre de archivo. Puede ser el nombre de una tabla, el nombre de una cuenta, las coordenadas de un mapa, o lo que sea»*[989].

Las páginas Web 1.0 contaban con un administrador de contenidos denominado *Webmaster,* como se puede intuir era el encargado de generar y administrar los contenidos, por lo que podía controlar lo que se publicaba en ella e incluso realizar censuras previas a la información, tal posición lo convertía en personaje principal en este tipo de Web. Por su parte quienes asumían el papel secundario eran los usuarios ante restrictiva participación que tenían derivada de la imposibilidad de interacción y participación en la creación de contenido.

Aproximadamente en 2004 [990], llegó la de nominada *Web* 2.0 [991] o colaboracionista, *«la cual otorga una especial importancia a lo social»* [992], HEREDERO CAMPO la definía como «*una nueva tendencia en el uso de las páginas Web, en la cual el usuario es el centro de la información y se convierte en generador de contenidos. Supone un cambio en la filosofía, una actitud, una forma de hacer las cosas que identifica el uso actual de Internet que hacen tanto los internautas como las empresas,*

[989] BERNERS-LEE, T., *op. cit*., p. 37.
[990] Tal y como lo establece CEBRIÁN HERREROS, M., «La Web 2.0 como red social de comunicación e información», *Estudios sobre el mensaje periodístico,* núm. 14, 2008, p. 346. De igual manera lo establece NAIK, U. y SHIVALINGAIAH, D., *op. cit.:* «*According to some sources, the term Web 2.0 has been around about October 2004*».
[991] Denominada así por primera vez por Dale Dougherty, según MENON, S., *et al.*, este término se acuño durante una mesa redonda sobre el potencial futuro de la Web en la Conferencia Nacional de Microelectrónica y Comunicación, a tenor literal señala lo siguiente: «*The term "Web 2.0" was officially determined in 2004 by Dale Dougherty, a vice president of O´Reilly Media Inc (the Company famous for its tecnology-related conferences and high quality books) during a team discussion on potential future conference about the Web. "Web 2.0" is a term that is used to denote several different concepts: Web sites which incorpórate a strong social component, involving user profiles, friend links;Web sites which encourage user-generated content in the form of test, video or just Web sites that have gained popularity in recent years*», *vid.* MENON, S., *et al., op. cit.*
[992] CALDEVILLA DOMINGUEZ, D., «Las Redes Sociales. Tipología, uso y consumo de las redes 2.0 en la sociedad actual», *Documentación de las Ciencias de la Información.* 2010, núm. 33, p. 47.

pasando de ser meros consumidores a productores y creadores de contenidos»[993]. También puede ser definida como «*todas aquellas utilidades y servicios de Internet que se sustentan en una base de datos, la cual puede ser modificada por los usuarios del servicio, ya sea en su contenido (añadiendo cambiando o borrando información o asociando metadatos a la información existente), bien en la forma de presentarlos o en contenido y forma simultáneamente. Dicho de otra forma, una aplicación online podrá considerarse como Web 2.0 cuando permita procesos de interactividad de contenidos contributiva*»[994].

Respecto al cambio de nomenclatura, RIBES determina que el cambio del digito colocado antes del «punto» o que es lo mismo a la izquierda de este, de igual forma que en los programas informáticos[995], sugiere una modificación sustancial de la versión. El cambio de una a otra supuso un giro radical en su uso y formato, lo que era una Web estática controlada por el *Webmaster* se convirtió en una *Web* dinámica donde no solo este último podía emitir comentarios y crear contenidos, también los usuarios, lo cual genera una nueva forma de entender el funcionamiento de la *Web*, ahora los usuarios se convertirían en «prosumidores»[996].

---

[993] HEREDERO CAMPO, M.T., «Web 2.0: Afectación de derechos en los nuevos desarrollos de la Web corporativa», *Cuadernos Red de Cátedras Telefónica*. 2012, núm. 6, p. 8.

[994] El autor con «*interactividad de contenidos contributiva*» se refiere a las acciones que pueden realizar los usuarios el propio sistema compartan la información con los otros usuarios, para ello se necesita que la información se interrelacione y combine de distintas bases de datos (lo denomina procesos de interacción de contenidos combinatoria), pudiendo ser: a)«*de preferencias estéticas o de funciones (cuando el usuario puede ubicar los contenidos en diferentes lugares de la pantalla o decidir qué contenidos aparecen)»;* b)generativa «*(cuando el sistema, a partir del análisis del modo de operar del usuario con la interface, decida por el usuario cómo o qué datos presentar*», Cfr. RIBES I GUÀRDA, F. X., El valor de los metadatos y la inteligencia colectiva (en línea), *Telos,* Disponible en: https://telos.fundaciontelefonica.com/archivo/numero073/el-valor-de-los-metadatos-y-de-la-inteligencia-colectiva/ (consulta: 1 de diciembre de 2020).

[995] Este autor explica que este símil se debe al cambio de nomenclatura de la Web: «*Esta denominación sigue el símil de los programas informáticos: las versiones de un mismo producto se identifican con dos o más números separados por puntos. Las variaciones realizadas en el programa se indican incrementando la numeración con la lógica de que en cuanto más a la derecha está el número que varía, de menor importancia resulta la mejora o la corrección realizada. Pero si es el primer dígito el que cambia, se está indicando que se han producido modificaciones* sustanciales», *vid.* RIBES, X., *op. cit.*

[996] El término viene del inglés «*prosumers*» acuñado por Alvin Toffler en su obra «The third wave» (la tercera ola). Para ISLAS CARMONA: «*Alvin Toffler se aventuró a señalar que los principales medios de comunicación en las sociedades de la "tecera ola", serían "desmasificadores", como precisamente es el caso de Internet*», Cfr. ISLAS CARMONA, O., «Internet 2.0: El territorio digital de los prosumidores» (en línea), *Revista Estudios Culturales*, núm. 5, 2010, p. 8 (50). Disponible en: https://dialnet.unirioja.es/descarga/articulo/3739971.pdf (consulta: 6 de abril de 2019). Respecto

Gracias a este cambio los usuarios empiezan a contar con la posibilidad de compartir información u opiniones directamente, ya sea por medio de aplicaciones[997], redes sociales, *wikis*, *blogs*[998], plataformas de vídeos como *YouTube* o en plataformas educativas[999]; incluso en este tipo de *Web* podían comentar las publicaciones realizadas por otros usuarios o por el *Webmaster* y, crear contenidos a partir de algo previamente compartido. Es por ello que el *Webmaster*, deja de tener gran parte del control que ejercía, sin embargo, no está exento de poder realizar censuras posteriores si la información no es acorde con la línea ideológica y valores que ostenta la página *Web.* El carácter global de estas páginas y la gran información publicada en tiempo real ralentizan el control de contenidos en las páginas web[1000]. Esta nueva Web se convierte así en un hito en el campo de la informática, pues a partir de este cambio sustancial surgen nuevas tecnologías basadas en este tipo de

a esta palabra traída al español, la Fundación del español urgente (Fundéu) señala que: «*es un término bien formado en español de productor (o profesional o proveedor) y consumidor»,* continua diciendo que: «*aunque la palabra aún no está registrada en el Diccionario de la Real Academia Española, está bien formada en español, tal como otras creadas mediante el mismo procedimiento de acronomia*», Disponible en: https://www.fundeu.es/recomendacion/prosumidor-en-espanol-mejor-que-prosumer-1292/ (consulta: 6 de abril de 2019).

997 Es decir «*aquel software social que posibilita y facilita la interacción social y da soporte a la configuración de redes sociales*», Cfr, GARCÍA AREITO, L., «¿Web 2.0 vs Web 1.0?» (en línea), *Didáctica, Innovación y Multimedia,* núm. 10, 2007, p. 4. Disponible en: https://www.raco.cat/index.php/DIM/article/view/76637/98327 (consulta 30 de noviembre de 2018). Para la autora DAVARA FERNÁNDEZ DE MARCOS, L. también es un rasgo definitorio de la Web 2.0, pues el contenido Web, también se hace accesible mediante aplicaciones, gracias al uso de los *Smartphones,* y tabletas, Cfr. DAVARA FERNÁNDEZ DE MARCOS, L., *op. cit*., p. 47.

998 Como establecen DÍAZ VICARIO, A., FERNÁNDEZ DE ÁLAVA, M., Y BARRERA-COROMINAS, A. en su obra Creación y gestión del conocimiento en redes profesionales virtuales: Análisis de experiencias en empresas, es: *«Un espacio para la publicación secuencial de contenidos. Destacan las posibilidades de participación, de publicación conjunta y de suscripción a otros blogs»,* DÍAZ VICARIO, A., FERNÁNDEZ DE ÁLAVA, M., y BARRERA-COROMINAS, A., «Creación y gestión del conocimiento en redes profesionales virtuales: Análisis de experiencias en empresas» (en línea), GUERRA LÓPEZ, F., GARCÍA RUIZ, R., GONZÁLEZ FERNÁNDEZ, N., RENÉS ARELLANO P., y CASTRO ZUBIZARRETA A. (Coords.), *Estilos de aprendizaje: investigaciones y experiencias: V Congreso Mundial de Estilos de Aprendizaje,* Santander: 27, 28 y 29 de junio de 2012, p. 3 Disponible en: https://dialnet.unirioja.es/descarga/articulo/4664051.pdf (consulta: 10 de junio de 2019). En otras palabras, es un espacio con la finalidad de que los usuarios escriban sobre un tema elegido por ellos y compartirlo con otros usuarios, quienes a su vez podrán, comentar la entrada (es como se llaman a los textos subidos en blogs por los usuarios), algunos de los ejemplos más destacables de este tipo de servicios son los proporcionados por *WordPress* y *Blogger*.

999 Por ejemplo, el campus virtual de las Universidades que están normalmente basadas en plataformas *Moodle*.

1000 Si está habilitada para ello, pensemos por ejemplo en la página Web de un diario electrónico, dónde normalmente el creador de la página web por instrucciones del dueño del dominio o mejor conocido como propietario de la misma, ha habilitado una especie de micro-foro dentro de cada noticia, lo cual habilita a los usuarios previo registro, creación de cuenta y sobre todo la aceptación de sus condiciones de uso, para poder dar una opinión en relación con la noticia publicada.

web, que hacen más fácil la navegación, la búsqueda, la creación y la interacción con otros usuarios. Quizás uno de los cambios más trascendentales sea la tecnología móvil y el desarrollo de aplicaciones. Con esta nueva era tecnológica la sociedad de forma individual y colectiva empieza a tener presencia en este tipo de tecnologías, quizás los ejemplos más claros son las redes sociales, profesionales y educativas.

Años más tarde, como resultado del desarrollo de mejoras y aplicaciones para la web colaborativa, se realiza el segundo cambio sustancial en el diseño de la misma, surge entonces la «web semántica» [1001] o «web 3.0», la cual relaciona «*contenido y conocimiento*» [1002]. La información que los usuarios vierten dentro de la web y aplicaciones como su ubicación, las preferencias con base al número de clics y las palabras clave utilizadas en sus búsquedas, se almacenan y arrojan información valiosa que es utilizada principalmente por redes de publicidad y motores de búsquedas, utilizada para ofrecer al usuario una «mejor» experiencia, debido a que le permite hallar «*respuestas a sus preguntas de forma rápida y sencilla, gracias a una información mejor definida, jerarquizada y ordenada*» [1003].

La implementación de este cambio se hace evidente sobre todo en las listas de resultados que arrojan los motores de búsqueda a los usuarios, de manera que también se identifica «*el contexto en el que las palabras se presentan a través de las relaciones entre ellas y, por lo tanto, proporciona un resultado de datos preciso. También identifica los sinónimos asociados y muestra los datos relacionados con sus sinónimos*» [1004].

La web semántica [1005] también nos permite la interconexión entre páginas de internet y aplicaciones móviles cuando la navegación por internet se realice a través

[1001] MENON, S., *et al.* Establecen que ha sido definida así por Berners Lee en su artículo MENON, S., *et al.*, *op. cit.*: «*Web 3.0 was also called as Semantic Web by its founder Tim Berners Lee».*
[1002] TOURIÑO PENA, A. *El derecho al olvido y a la Intimidad en Internet*. Madrid, Ed. Catarata, 2014, p. 19.
[1003] TOURIÑO PENA, A. *Íd.*
[1004] MENON, S., *et al.*, *op. cit.*
[1005] Incluso actualmente se habla de la Web 4.0 que «*estará basada en el Internet de las Cosas (Internet of Things –IoT), donde el flujo de la información será altamente personalizado*» más si aún cabe, Cfr. ALMEIDA, F., «Concept and Dimensions of web 4.0» (en línea), *International Journal of Computers & Technology* Disponible en: https://doi.org/10.24297/ijct.v16i7.6446 (consulta 28 de noviembre de 2018). En este artículo se hace referencia a varios autores que defienden la existencia de este tipo de web y la definen de manera muy breve, sin embargo, nos hace ver que este concepto aún es bastante «irregular y mutable», como para aceptarse de manera general. Lo anterior, debido a que el Internet

de un teléfono inteligente o incluso si la navegación es llevada a cabo desde un ordenador, me atrevería a decir que en la actualidad casi todas las marcas de ordenadores tienen acceso a tiendas propias y/o de terceros como *Apple Store* o *Microsoft Store* donde pueden adquirir aplicaciones para ordenadores de sobremesa o portátiles.

En este tipo de red, prácticamente todas las páginas y aplicaciones están conectadas con otras sin importar el servicio que se ofrezca, un ejemplo claro de interconexión son las palabras en negrita o cursivas en el cuerpo del texto de una página web, las cuales también funcionan como enlaces, de manera que, si son clicados, se remite al usuario a otra página web la fuente de la información o a otra página donde se alberga información relacionada con la palabra clave del texto original. La web semántica también facilita la labor de difusión de contenidos por medio de enlaces ubicados en las páginas web, estos suelen ser compartidos por medio de herramientas simplificadas como iconos que directamente lo envían a otra red social, a una dirección de correo electrónico y hasta por medio de una plataforma de mensajería instantánea, sin la necesidad de copiar y pegar el enlace. Es por ello, que con base en este tipo de acciones por parte de la comunidad de usuario de la Web se sopese la generación de la inteligencia colectiva basada en las acciones de los usuarios y en la generación de contenido, tal y como lo establece GILMORE «*cada internauta constituye una neurona y que acabará generando algún tipo de inteligencia colectiva que produzca pensamientos e ideas por encima de cada una de las capacidades de las pequeñas partes*»[1006]. En relación con lo anterior,

---

de las cosas ya es una realidad y se compatibiliza con la actual Web 3.0. Aunado al hecho de que no supondría un cambio sustancial como para cambiar de nuevo el dígito. También es menester mencionar que este tipo de Web, tampoco puede ser confundida con la Industria 4.0 o la cuarta revolución industrial caracterizada por el uso de tecnologías como Internet de las cosas (IoT), el *Cloud Computing* y el *Big Data*, término que fue «*acuñado por el Gobierno alemán para describir la digitalización de sistemas y procesos industriales y su interconexión mediante el Internet de las cosas; entre otras palabras, conseguir la transformación digital de la industria*», Cfr. JOYANES AGUILAR, L., «Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial, Industria 4.0 versus ciberseguridad 4.0» (en línea), *Cuadernos de estrategia*, núm. 185, 2017, p. 25. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6115620.pdf (consulta 29 de noviembre de 2018).

[1006]Cita de DAVARA FERNÁNDEZ DE MARCOS, L., *op. cit*., p. 50. Esta autora afirma que la Web semántica «*se trata de una web extendida y basada en el significado que se apoya en lenguajes universales que resuelven los problemas ocasionado por una Web carente de semántica en la que, en ocasiones, el acceso a la información se convierte en una tarea difícil y frustrante. La idea radica, más allá de que los*

DAVARA FERNÁNDEZ DE MARCOS, L. determina que «*la idea radica, más allá de que los usuarios proporcionen información y los sometan a sistemas de etiquetado comprensibles que faciliten la búsqueda a la posibilidad de que sea el propio software y no, por tanto, labor de los usuarios- el que sea capaz de procesar su contenido, razonar con este, combinarlo y realizar deducciones lógicas para resolver problemas cotidianos automáticamente*»[1007]. De lo anterior se atisba la especial importancia los datos y metadatos, pues a partir de ellos se genera la construcción de conocimiento en la Web, los cuales han creado un nuevo nicho de mercado, en el tratamiento más automatizado de como los que realiza el Big Data[1008] y la minería de datos[1009].

usuarios proporcionen información y los sometan a sistemas de etiquetado comprensibles que faciliten la búsqueda a la posibilidad de que sea el propio software –y no, por tanto, labor de los usuarios- el que sea capaz de procesar su contenido, razonar con este, combinarlo y realizar deducciones lógicas para resolver problemas cotidianos automáticamente», *vid. Ib.,* p. 51.

[1007] DAVARA FERNÁNDEZ DE MARCOS, L. *Íd.*

[1008] De conformidad con lo establecido por GIL GONZÁLEZ, E. puede definirse como «*el conjunto de tecnologías que permiten tratar cantidades masivas de datos provenientes de fuentes dispares, con el objetivo de poder otorgarles una utilidad que proporcione valor*», *vid.* GIL GONZÁLEZ, E. *Big data, privacidad y protección de datos* (en línea), Agencia Española de Protección de Datos, 2016, p. 15. Disponible en: https://www.aepd.es/media/premios/big-data.pdf (consulta: 10 de junio de 2019).

[1009] O *Data Mining* es «*el proceso de extraer conocimiento útil, comprensible y novedoso de grandes volúmenes de datos, siendo su principal objetico encontrar información oculta o implícita, que no es posible obtener mediante métodos estadísticos convencionales (…)»,* Cfr. MOINE, J. M., HAEDO, A. S. y GORDILLO, S. E., «Estudio comparativo de metodologías para minería de datos» (en línea), *XIII Workshop de Investigadores en Ciencias de la Computación: mayo 2011* Disponible en: http://sedici.unlp.edu.ar/handle/10915/20034 (consulta 5 de diciembre de 2018). Por su parte VALCÁRCEL ASENCIOS considera que la minería de datos «*es una etapa dentro del proceso completo del descubrimiento del conocimiento, este intenta obtener patrones o modelos a partir de los datos recopilados*», *vid.* VALCÁRCEL ASENCIOS, V., «Data Mining y el descubrimiento del conocimiento» (en línea), *Indutrial Data,* vol. 7, núm. 2, julio-diciembre 2004, p. 84. Disponible en: https://www.redalyc.org/pdf/816/81670213.pdf (consulta 5 de diciembre de 2018); RIQUELME, J. C., RUÍZ, R. Y GILBERT, K., establecen que: «*En realidad, los términos MD y KDD son a menudo confundidos como sinónimos. En general se acepta que la MD es un paso particular en el proceso consistiendo en la aplicación de algoritmos específicos para extraer patrones (modelos) de los datos. Otros pasos en el proceso KDD, son la preparación de los datos, la selección y limpieza de los mismos, la incorporación de conocimiento previo, y la propia interpretación de los resultados de minería. Estos pasos aplicados de una manera iterativa e interactiva aseguran que un conocimiento útil se extraiga de los datos*», Cfr. RIQUELME, J. C., RUÍZ, R. Y GILBERT, K., «Minería de Datos: Conceptos y Tendencias» (en línea), *Inteligencia Artificial. Revista Iberamericana de Inteligencia Artificial,* vol. 10, núm. 29, 2006, p. 12. Disponible en: https://www.redalyc.org/pdf/925/92502902.pdf (consulta y descarga: 5 de diciembre de 2018). MOINE, *et al.* consideran que *«En los inicios del año 1996, el modelo KDD (Knowledge Discovery in Databases) constituyó el primer modelo aceptado en la comunidad científica que estableció las etapas principales de un proyecto de explotación de información. Formalmente el modelo establece que la minería de datos es la etapa dentro del proceso en la cual se realiza la extracción de patrones a partir de los datos. Sin embargo, actualmente, en la comunidad científica y en la literatura, el término KDD y minería de datos se utilizan indistintamente para hacer referencia al proceso completo de descubrimiento de conocimiento*», *vid.* MOINE, J. M., *et al., íd.*

Dentro de la web existen diferentes niveles dependiendo de las herramientas se utilicen para su accesibilidad, el primer nivel accesible para todos los usuarios lo constituyen las páginas web de superficie, las cuales son visibles para los usuarios por medio de un navegador, a este tipo de Web también se le denomina *Surfaceweb* o web de superficie-visible, está formada por aquellas páginas que pueden ser indexadas por los tradicionales motores de búsqueda[1010] como *Google*, *Yahoo, Bing*, etc. y, normalmente configuradas en HTML o CSS[1011]. Sin embargo, solo representan el 4%[1012] de las páginas web disponibles al público. Entonces el 96% del porcentaje restante corresponde al contenido albergado en la Web oculta o profunda, la cual está integrada por la *Deep Web* y la *Dark Web*, cuya característica principal es su falta de indexación por un motor de búsqueda de superficie, para poder tener acceso a este tipo de web se requiere un navegador especial.

La *Deep Web* en palabras de ÉCIJA BERNAL «*es el nombre que recibe el conjunto de páginas de internet que no aparecen en los buscadores tradicionales como Google o Bing, páginas a las que solo se puede acceder si se conoce su dirección URL y que normalmente tratan temas ilegales o polémicos como el contrabando, el cibertráfico de personas o el terrorismo y por este motivo no aparecen en estas páginas de búsqueda*»[1013]. Adquiere su nombre del término «*Deep*» que significa profundo, ya que el acceso a estas páginas se encuentra restringido «*ya sea por contraseña -como ocurre con los correos electrónico o sistema de bases de datos en línea de las empresas o de instituciones de gobierno- o mediante el llenado de un formulario que le permite al usuario solicita información para acceder a ésta*»[1014]. Este tipo de web sirve como

---

[1010] AMARO LÓPEZ, J.A. *et al*, en su trabajo «La web oculta y cómo los buscadores encuentran la información», utilizan la definición de LÓPEZ-BARBERÁ MARTÍN para referirse a la Web de superficie de la siguiente manera: «*es el conjunto de páginas que en la actualidad podemos consultar mediante los buscadores*», Cfr. AMARO LÓPEZ, J.A., *et al.*, «La web oculta y cómo los buscadores encuentran la información» (en línea), *Paakat: Revista de tecnología y sociedad*, vol.4 núm. 7, 2014-2015, p. 2. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5695439.pdf (consulta: 23 de octubre de 2017).

[1011] De conformidad con lo establecido por AMARO LÓPEZ, J. A., *et al.* «CCS» son las siglas de lo que se denomina en inglés «*Cascading Style Sheets u Hojas de Estilo en Cascada, se utiliza para maquetar las páginas elaboradas mediante lenguaje HTML*», AMARO LÓPEZ, J. A., *íd.*

[1012] De conformidad con GUDÍN RODRÍGUEZ-MAGARIÑOS, F., «La lucha contra el ciberblanqueo como vía para acabar con el phishing» (en línea) *Revista Aranzadi Doctrinal* (estudios) núm. 9, 2014, p. 20 (consulta: 6 de diciembre de 2018). BIB 2014\4287.

[1013] ÉCIJA BERNAL, Á., *El ciberespacio, un mundo sin Ley. Internet: la revolución que cambió las normas del juego* (en línea), Wolters Kluwer, 2017, p. 43. Disponible en: http://ciberderecho.com/El_ciberespacio_un_mundo_sin_ley.pdf (consulta 7 de diciembre de 2018).

[1014] AMARO LÓPEZ, J. A., *et al*., *op. cit.*

plataforma para potenciar la venta, distribución de sustancias y objetos legales[1015] o ilegales como el tráfico de órganos o armas de fuego, además de potenciar el consumo de pornografía de todo tipo, e incluso se pueden contratar servicios de realización de conductas ilegales[1016], por ello no es recomendable el uso de este tipo de Web. Por su parte la *Dark Web* o *DarkNet* lo constituyen las páginas web que «*están restringidas para su acceso libre y solo con autorización, o a través de ciertos contactos o sistemas (sistemas proxy, VPN´s o autenticación)*»[1017], en este tipo de web también se puede encontrar contenido ilegal.

La empresa *Panda Security* en su página Web utiliza un *Iceberg* como metáfora para explicar las distintos niveles de la web, para esta empresa la constituyen cinco niveles[1018], el primero lo constituyen las páginas que son indexadas por los buscadores y accesibles para todos los usuarios, el segundo nivel está integrado por páginas web no indexadas accesibles «*solo por gente "cualificada"»,* el tercer nivel está constituido mayoritariamente por páginas con contenido ilegal, el cuarto nivel está integrado por páginas con contenido ilegal mayormente «*monitorizadas por el Gobierno de los EE.UU., como por ejemplo las páginas de pornografía infantil*», y finalmente el nivel cinco se encuentra la *darknet,* este nivel es «*el verdadero reino de los hackers está compuesto por una serie de redes*

[1015] Se pueden encontrar miles de obras sujetas a Derechos de autor con acceso libre para su descarga.

[1016] Tal y como lo evidenciaba la serie de televisión *House of cards*. Actualmente hay series de televisión y documentales, que evidencian los posibles riesgos del uso de este tipo de web o de los riesgos futuros como lo hace *Black Mirror* o *Dark Net.* También nos ayudan a adquirir una mayor visión sobre el uso por parte de los usuarios de la Web en general.

[1017] ÉCIJA BERNAL, Á., *op. cit*., p. 43.

[1018] Los niveles son: «*Nivel 1. En la punta del iceberg podemos encontrar todas las páginas a las que podemos acceder por medio de buscadores. Es la parte visible y accesible para "los comunes de los mortales" y toda la información en ella contenida es totalmente rastreable. Nivel 2. Por debajo de la superficie del agua encontramos las páginas o los sitios que no están indexados (es decir, visibles) por los buscadores tradicionales (Google o Yahoo, por ejemplo). Por lo tanto, son accesibles solo por gente "cualificada". Nivel 3. Buceando todavía más en las frías aguas alrededor de nuestro iceberg empezamos a encontrarnos con contenido muy difícil de rastrear porque es, principalmente, ilegal. Nivel 4. A medida que nos acercamos a la punta inferior del iceberg podemos encontrar todo tipo de páginas ilegales, muchas de ellas monitorizadas por el Gobierno de EE.UU, como por ejemplo las páginas de pornografía infantil. Nivel 5. Una vez que se hayan pasado los 4 niveles de la Deep Web se llega a la punta del iceberg, la parte mejor conocida como "The Darknet". El verdadero reino de los hackers está compuesto por una serie de redes privadas a las que pueden acceder solamente usuarios de "confianza". La parte más oscura del web es la que no se rige bajo los protocolos standard y no tiene seguridad*», en https://www.pandasecurity.com/spain/mediacenter/seguridad/tor-y-deepweb-todos-los-secretos/ (consulta 7 de diciembre de 2018).

privadas a las que pueden acceder solamente usuarios de "confianza"» y «*no se rige bajo los protocoles standard y no tiene seguridad».*

Dentro de la *deep web* encontramos a la red Tor o *Tor Network,* cuya principal cualidad es el cifrado del tráfico de la comunicación entre servidor y usuario, es por lo que no se puede saber la dirección IP de las personas intervinientes en la comunicación. Inicialmente este proyecto fue financiado por el laboratorio de investigación naval de los Estados Unidos, actualmente es manejado por una organización sin ánimo de lucro la cual se financia a base de donaciones de nominada *Tor Project*[1019].

Esta red funciona de manera diferente que la web convencional y así lo explica de manera clara RECARTE PÉREZ, J. M.: «*A diferencia del modelo de enrutado que seguimos tradicionalmente para conectarnos a Internet que es directo (el cual obviamente es el más rápido) el sistema onion routing, que como hemos visto fue diseñado de cara a proteger informaciones de la marina, cambia su enrutamiento para tratar de garantizar tanto la privacidad de la información como el anonimato. El enrutado tradicional sigue un orden muy sencillo, ordenador, router, enrutador ISP (router de nuestro proveedor de internet) y servidor del lugar al que queremos acceder. Mientras que el enroutado onion solo pasa por varios nodos (puntos de intersección, conexión o unión de varios elementos informáticos) aleatorios, también cifra por capas de forma asimétrica por los que pasa, es decir que, si pasa por tres router, solo el "router a" podrá decodificar el cifrado del "router b" y solo el "router b" podrá descodificar el "router c"*»[1020].

Es menester señalar que la Red Tor[1021], se creó ante la ingente cantidad de información que se comparte y genera en la web, información que puede «*ser*

[1019] *Íd.*

[1020] RECARTE PÉREZ, J. M., «Diseccionando la red Tor» (en línea), *Qadernos de criminología: revista de criminología y ciencias forenses,* núm. 41, 2018, p. 47-48. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6478986.pdf (consulta: 10 de junio de 2019).

[1021] Red Tor cuenta con un canal de YouTube integrado por diversos tipos de vídeos explicativos de su labor. Uno de sus principales vídeos tiene por objeto explicar en diferentes idiomas los diversos problemas que plantea poder ser rastreado en la web y las repercusiones que tienen en su privacidad, bajo esa bandera es que se justifica el encriptado en tres capas de cifrados. Otros motivos que se argumentan en este video que legitiman la existencia de Tor es la protección de nuestros datos ante la vigilancia de los Gobiernos represivos que «*intentan controlar internet»,* el simple deseo de los

interceptada y decodificada por un tercero, el cual puede obtener acceso a cuentas de bancos, contraseñas de correos electrónicos, copiar archivos del disco duro, mensajes de WhatsApp, documentos personales, fotografías, controlar la computadora infiltrada de manera remota, etcétera »[1022]. Sin embargo, la bienintencionada idea de mantener completa privacidad sin desvelar quizás el más importante de nuestros datos personales en la web, no está exenta de manipulaciones por algunos de los usuarios que bajo el amparo de esta «privacidad», puede ser utilizada como medio de distribución de servicios u objetos ilícitos[1023].

Tor utiliza la técnica de *Onion Routing* o enrutamiento cebolla para que la comunicación sea anónima y su contenido cifrado, cuando un usuario quiere mandar un mensaje a otro, su ordenador traza una ruta para el envío del mensaje el cual pasa por tres nodos (ordenadores) el de entrada, el de en medio y el de salida antes de llegar al destinatario final. De forma aparente proporciona un nivel de seguridad alto tanto del remitente del mensaje como del contenido de la información.

También dentro del *Surface Web* encontramos sistemas de cifrados de mensajes, sin embargo, los mensajes no son anónimos ya que se conoce tanto el remitente como el destinatario, pues al usarse este tipo de Web, el envío del mensaje

---

usuarios de que las «*grandes compañías, se aprovechen de su información personal*», la igualdad entre los usuarios, la no persecución comercial por parte de los anunciantes, que no se identifique tu país de procedencia «*a menos que te identifiques*», la protección de personas que «*necesitan anonimato, por ejemplo activistas, periodistas o bloggeros*». Disponible en: https://www.youtube.com/watch?v=Sz_J6vJ4MYw&list=PLwyU2dZ3LJErtu3GGElIa7VyORE2B6H1H&index=4&t=0s (consulta: 11 de diciembre de 2018).

[1022] AMARO LÓPEZ, J. A., «El proyecto Tor» (en línea), *Paakat: Revista de Tecnología y Sociedad*, núm. 9 Disponible en: http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/246/385 (consulta: 11 de noviembre de 2018).

[1023] Se pueden contratar diversos productos o servicios dentro de la Red Tor, que pueden considerarse perfectamente ilícitos. Dentro de los ejemplos que nos señala RECARTE PÉREZ, J. M., se encuentran: la contratación de sicarios (ejemplifica diciendo que «*el caso más famoso que se ha revelado a la información pública fue el francés de iniciales A.J., arrestado en Bulgaria, que ofrecía sus servicios en la Deep Weeb para acabar siendo rastreado por la Interpol. el resultado fue su puesta en libertad por falta de pruebas debido a la inconexión de su persona con los asesinatos),* puesta a disposición de material con contenido gore (específica el autor que «*de hecho hay foros para que todo tipo de gente comparta vídeos de asesinatos. Uno de los más famosos que existieron llevaba por título "Tres hombres y un martillo" (Three guys and one hammer)»)* o pornográfico en su mayoría pornografía infantil, venta de armas y drogas, cuentas robadas (desde las más usuales que suelen ser las bancarias, hasta credenciales que dan acceso a un videojuego, pues señala el autor «*funcionan de forma similar»),* venta de documentación falsa, entre los más destacables, véase RECARTE PÉREZ, J. M., *op. cit.*, p. 49-52.

es directo y como consecuencia de ello se conoce tanto la dirección IP de origen como la de destino, la cual arroja datos sobre la ubicación geográfica, y también es considerada como un dato personal.

El cifrado es parte de una serie de mecanismos creados para para dar una mayor seguridad y confianza a los usuarios de la Web traducidos en autenticación, privacidad, integridad, fiabilidad y disponibilidad [1024], en lo que respecta a sus comunicaciones.

La criptografía es aquella «*técnica que permite cifrar los mensajes de su transmisión*» [1025], cuando se encripta o cifra un mensaje se utiliza un software específico el cual mediante el uso de algoritmos modifican la apariencia de la información durante su tránsito de envío, el procedimiento sucintamente explicado es el siguiente: «*un remitente quiere enviar un mensaje "Hola" a un destinatario. El mensaje original, también llamado texto claro, se convierte en bits aleatorios conocidos como texto cifrado mediante el uso de una clave y un algoritmo. El algoritmo que se utiliza puede producir una salida diferente cada vez que se usa, basado en el valor de la clave. El texto cifrado se transmite a través del medio de transmisión. Al final del destinatario, el texto cifrado se convierte de nuevo al original utilizando el mismo algoritmo y la clave que se utilizó para cifrar el mensaje*» [1026]. Entre los métodos criptográficos para cifrar información, existen dos principalmente: el cifrado simétrico y el asimétrico, en el primero se utiliza una clave única que solo el remitente y el destinatario conocen y determinan, en cambio cuando se cifra información por medio del método criptográfico asimétrico se hace uso de una clave

[1024] De conformidad con MEDINA VARGAS, Y. T. y MIRANDA MNEDEZ, H. A. la criptografía cuenta con cinco objetivos principales para «*asegurar el secreto del sistema»,* los cuatro anteriores mencionados en el texto principal (siendo un solo objetivo el de fiabilidad y disponibilidad) y el de no repudio. El principio de no repudio consiste según estos autores en «*un mecanismo para probar que el remitente envío este mensaje. Significa que ni el emisor ni el receptor pueden falsamente negar que hayan enviado un mensaje determinado*», el cual según mi perspectiva puede quedar inmerso dentro del de autenticidad el cual consiste en «*el proceso de probar la identidad de uno. Esto significa que antes de enviar y recibir datos utilizando el sistema, la identidad del receptor y el remitente debe ser verificada».* Derivado de este proceso tanto el receptor como el destinatario no pueden reprocharse mutuamente su identidad, *vid.* MEDINA VARGAS, Y. T. Y MIRANDA MNEDEZ, H. A., «Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES» (en línea), *Mundo FESC,* vol. 5, núm. 9, 2015, p. 15-16 Disponible en: https://dialnet.unirioja.es/descarga/articulo/5286657.pdf (consulta: 10 de enero de 2019).

[1025] NAVARRO SCHLEGEL, A., *op. cit*., p. 89.

[1026] MEDINA VARGAS, Y. T. Y MIRANDA MNEDEZ, H. A., *op. cit*., p. 15.

pública, la cual es conocida por el público generalmente y una clave privada que solo conocen el remitente y el destinatario de la información[1027].

El cifrado de los datos no son la única medida de seguridad que se puede adoptar para proteger los intereses de los usuarios frente las diversas amenazas que existen en la red, el riesgo no solo está en el flujo de la información, actualmente existe una gran variedad de software malicioso, mejor llamado *malware*[1028] que no resulta nada baladí.

1.3 Navegador

Para poder tener acceso y localizar contenido en la web se necesita tener instalado un navegador o *browser*, el cual es un programa de *software*[1029] tanto para ordenadores como para dispositivos móviles que se encargan de leer su código, ejecutarlo y mostrar la página Web correspondiente[1030] tal y como la vemos. Así pues, entonces «*los navegadores sirven de unión entre el internauta y la información, obviando y haciendo transparente todo ese conglomerado de siglas, protocolos y*

[1027] Para una mayor profundización del tema se pueden consultar artículos como el de AMARO LÓPEZ, J. A. y RODRÍGUEZ RODRÍGUEZ, C. R. Seguridad en Internet (en línea), *Paakat: Revista de tecnología y sociedad,* p. 3. Disponible en: http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/280/html (consulta: 27 de octubre de 2017) y MEDINA VARGAS, Y. T. y MIRANDA MNEDEZ, H. A., *op. cit.* y PÉREZ LUÑO, A. E., «Impactos sociales y jurídicos de Internet» (en línea), *Argumentos de razón técnica: revista española de ciencia, tecnología y sociedad y filosofía de la tecnología*, núm. 1, p. 33-48 Disponible en: https://idus.us.es/xmlui/handle/11441/57678 (consulta: 11 de enero de 2019).

[1028] De conformidad con lo establecido por ÉCIJA BERNAL, además de ser la abreviatura del inglés «*malicious software*», esta se utiliza para definir a «*todo tipo de programa o código malicioso diseñado para introducirse en un sistema informático, sin consentimiento de su propietario, y provocar daños, causar un mal funcionamiento o robar información*», Cfr. ÉCIJA BERNAL, Á., *op. cit.*, p. 66. Entre los tipos de *malware* más conocidos encontramos a los virus, gusanos de internet, troyanos *keyloggers, botnets, spywere, adware, ransomware*, etc. *vid. íd.*, p. 67-68.

[1029] El Diccionario de la lengua española lo define como: «*Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora*». Disponible en: http://dle.rae.es/?id=YErlG2H (consulta 10 de diciembre de 2018). De acuerdo con RODRÍGUEZ DE LAS HERAS BALLELL, T., este término «*se contrapone, o mejor, complementa, a la de hardware. Es el alma que da vida a ese cuerpo compuesto de redes, engranado por nodos de conexión, ramificado en periféricos y sistemas de información, que se denomina hardware. De hecho, el software es el motor de los entornos electrónicos, la esencia de los sistemas técnico-informáticos*». Esta autora en aras de especificar con más claridad cuál es la funcionalidad de cada uno de estos, es como cita a GÓMEZ SEGADE, J. A., en la nota de pie núm. 1: «*Los programas de ordenador, aplicaciones informáticas o sencillamente software contienen las instrucciones que determinan la ejecución por el hardware de las operaciones programadas*», Cfr. RODRÍGUEZ DE LAS HERAS BALLELL, T., «La responsabilidad por «software» defectuoso en la contratación mercantil» (en línea), *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 10, 2006-1, parte Doctrina (consulta: 10 de diciembre de 2018). BIB 2006\108.

[1030] TRIGO ARANDA, V., *op. cit.*, p. 4.

normas»[1031]. El diccionario *Merriam Webster* define *Browser* como «*un programa usado para el acceso a sitios o información en la red*»[1032]. Su nombre en español se debe a que en 1995 se fundaba *Navigator Netscape,* el cual fue por muchos años hasta que se popularizó *Internet Explorer* de *Microsoft*[1033], el navegador líder en el mundo, por lo que se *acabó identificando el programa líder con el programa genérico (…) se popularizaron los términos "navegador" y "navegar" para referirse a cualquier browser y a la acción de visitar páginas Web, respectivamente*[1034].

Los navegadores Web normalmente se ciñen al modelo cliente-servidor o en su caso a la utilización de protocolos SLIP o PPP, mejor llamado protocolo punto a punto el cual «*permite a un Proveedor de Servicios de Internet, o ISP, conectar, autentificar y asignar una dirección IP a un particular mediante un módem. Esta es la única forma de garantizar que la información y contenidos esté siempre a nuestra disposición: acceder en cualquier momento a la última noticia de nuestro diario online preferido, disponer de la legislación que requerimos, realizar compras online, etcétera. Cuando visitamos una página web es posible que podamos "descargar" algún archivo que nos pueda interesar. El acto de "descargar" es, ni más ni menos, copiar un determinado archivo informático que se encuentra en un determinado servidor en nuestro propio ordenador*»[1035].

Es indudable la envergadura que tienen en el mundo online, ya que sin estos no sería tan fácil localizar el contenido de la página, visualmente tampoco sería muy fácil de interpretar y sobre todo buscar dentro de los sitios Web. Gracias a estos podemos acceder de manera directa a los sitios web si contamos con la dirección

---

[1031] SENSO J. A., «Navegadores semánticos o semantizar el navegador» (en línea), *Anuario ThinkEPI*, 2008, p. 30. Disponible en: https://recyt.fecyt.es/index.php/ThinkEPI/article/download/32033/17026 (consulta: 10 de diciembre de 2018).

[1032] Trad. del inglés «*a computer program used for accessing sites or information on a network (such as the World Wide Web)*» en *Merriam-Webster.* Disponible en: https://www.merriam-webster.com/dictionary/browser (consulta: 6 de noviembre de 2018)

[1033] Este navegador fue creado casi a la par que *Netscape Navigator* en 1995, sin embrago, lo que hizo que el mercado se inclinara a su uso fue la gratuidad de este, pues se incluida dentro de la paquetería que ofrecía *Windows Microsoft*. Más tarde *Microsoft* es acusada de violar las Leyes antimonopolio de EEUU y la empresa es condenada por ello en el año 2000; en relación con esto se puede consultar TRIGO ARANDA, V., *op. cit*., p. 3. y BUSTILLO SÁIZ, Mª M., «Hacia la patentabilidad de los programas de ordenador: Un diálogo particular entre Derecho y la Economía», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm.16, 2008. BIB 2008\109.

[1034] TRIGO ARANDA, V., *op. cit*., p. 4.

[1035] MARTÍNEZ AYUSO, M. Á., *op. cit.,* p. 2.

URL de los recursos a los que pretendemos tener acceso, y sin estos no sería tan fácil el acceso a los denominados motores de búsqueda[1036] que hacen aún más fácil nuestra experiencia en la Web.

Los navegadores han ido evolucionando y adquiriendo mejoras conforme a las de la Web. Actualmente se habla de la existencia de navegadores semánticos, quizás los más conocidos sean *Tabulator*[1037] y *Piggy Bank*[1038], que más que navegadores semánticos son extensiones dentro de un navegador[1039]. En el caso del primero, esta extensión está disponible para los navegadores Firefox u Opera, es decir que este «*trabaja como un navegador dentro de otro, lo lógico es que con el paso del tiempo la evolución lo convierta en un software independiente*»[1040].

También dentro de la *Deep Web* existen navegadores un poco más específicos y con cualidades diferentes, ya que la mayoría no revelan la dirección IP de los usuarios en la denominada Red Cebolla[1041]. Para acceder a la Red Tor se necesita *Tor Browser*, «*el cual le permite a una persona conectarse de manera automática a la red Tor o configurar la conexión según las necesidades del usuario*»[1042], estableciendo preferencias sobre todo relativas a la privacidad.

1.4 Nombres de Dominio

Cada sitio Web a su vez cuenta con un nombre de dominio o *Domain Name Server* (DNS), el cual es «aquella dirección fácilmente comprensible para el usuario, de un ordenador, normalmente en forma fácil de recordar o de identificar»[1043], los

---

[1036] *Vid.* p. 47.
[1037] Según SENSO RUÍZ, J. A. es obra de BERNERS LEE, Cfr. SENSO RUÍZ, J. A., *op. cit.*, p. 31. La página Web del *Tabulator* puede consultarse en el siguiente enlace: https://www.w3.org/2005/ajar/tab (consulta: 11 de diciembre de 2018).
[1038] Véase también es una extensión para *Firefox* y no cuenta en la actualidad con un *software* independiente.
[1039] En *About the Tabulator* dentro de la página web, determina que *es una forma posible de navegador semántico* (trad. del inglés: «*This is one possible form of a semantic web browser*»).
[1040] SENSO, J. A., *op. cit.,* p. 31.
[1041] Debido a su forma de encriptación de la dirección IP, técnicamente a este tipo de encriptación se le denomina «enrutamiento», debido a que cada servidor-*router* genera una de las tres capas de anonimato. Su nombre también hace referencia a este proceso pues TOR son las siglas de *The Onion Router.*
[1042] AMARO LÓPEZ, J. A., «El proyecto…» *op. cit.*
[1043] OMPI, «La gestión de los nombres y direcciones de internet: cuestiones de propiedad intelectual» (en línea), 30 de abril de 1999, p. 2 Disponible en: http://www.wipo.int/export/sites/www/amc/es/docs/report.pdf (consulta: 28 de noviembre de 2017).

cuales «forman parte de la dirección electrónica»[1044]. Un nombre de dominio no es técnicamente lo mismo que una URL, aunque dentro de esta se encuentra el nombre de dominio. Los nombres de dominio tienen como principal función la identificación de un sitio web a la que le ha sido asignado este, ya que traducen la secuencia numérica IP a una palabra o conjunto de ellas que hacen más fácil ser recordadas para la accesibilidad de este. El sistema de nombres de dominio es entonces, «una gran base de datos que relaciona cada nombre de dominio con el número IP del equipo al que está asociado»[1045], este sistema tiene una estructura jerárquica, de la cual se derivan varios niveles dentro del sistema de nombres de dominio.

Un nombre de dominio se divide en dos partes separadas por un punto, «en la parte derecha del punto se encuentra el dominio de primer nivel o TLD[1046], y corresponde con las terminaciones ".com", ".net" u ".org", entre otras (...)»[1047]. Los nombres de dominio de nivel superior, de primer nivel o raíz, se dividen a su vez en dos categorías: los dominios de nivel superior genéricos (*generic Top-Label Domain* por sus siglas gTLD)[1048] y los dominios de nivel superior correspondientes a cada

[1044] CARBAJO CASCÓN, F., *op. cit.* p.,35.
[1045] RODRÍGUEZ RAPOSO, A., *op. cit.,* p. 72.
[1046] Siglas del término *Top Level Domain*, que significa: «Dominio de nivel superior». De conformidad con BARRIO ANDRÉS, M.: «*los dominios de ese tipo existentes inicialmente solo incluían .com, .org, .net, .edu, .int, .gov y .mil, que fueron ampliados por la ICANN en 2000 –para incluir .aero, .biz, .coop, .info, .museum, .name y .pro–, y luego en 2004 –añadiendo .asia, .cat, .jobs, .mobi, .tel y .travel–. Más recientemente, la ICANN ha puesto en marcha un proceso de expansión de las categorías de los nombres de dominio de nivel superior disponibles, posibilitando el uso desde 2013 como tales de, por ejemplo, marcas, nombres de personas o territorios»,* Cfr. BARRIO ANDRÉS, M., *Fundamentos de Derecho de Internet*, Centro de Estudios Políticos y Constitucionales, Madrid, 2017, p. 188.
[1047] *Vid.* https://www.icann.org/resources/pages/what-2012-02-25-es (consulta: 9 de julio de 2019).
[1048] De acuerdo con lo establecido por la Organización Mundial de la Propiedad Intelectual (*World Intellectual Property Organization,* por sus siglas WIPO) en su reporte «La gestión de los nombres de dominio y direcciones de Internet: Cuestiones de propiedad intelectual», las gTDL pueden ser abiertas o restringidas, dentro de las abiertas encontramos a los dominios: «.com», «.net» y «.org», por lo cual no deberán cumplir ningún requisito para que se pueda registrar con este gTDL. Caso contrario sucede con las restringidas, por lo cual «*únicamente pueden registrar nombres ciertas entidades que satisfacen algunos criterios. Estos son .int, limitado al uso de las organizaciones internacionales; .edu, cuya utilización se limita únicamente a universidades e instituciones de educación superior con cursos de cuatro años y concesión de títulos profesionales; .gov, cuyo uso está limitado a organismos del Gobierno Federal de los Estados Unidos de América; y .mil, cuyo uso está restringido a las fuerzas armadas de los Estados Unidos de América*», Cfr. OMPI, «La gestión…», *op. cit.,* p. 12.

país (*country code Top Label Domain* por sus siglas ccTLD)[1049], que se asigna con ayuda del estándar ISO-3166[1050].

Los nombres de dominio de segundo nivel (*Second Level Domains, SLDs*), se sitúa después de «www.» o en su caso después del signo «@»[1051] de una dirección de correo electrónico y siempre antes del punto, normalmente «*se utiliza para ofrecer sistemas en línea como sitios web o correo electrónico*»[1052], como establece BARRIO ANDRÉS, «*es el correspondiente a la persona física o jurídica con presencia en Internet(…)Generalmente consiste en incorporar el nombre de la persona física o jurídica o la marca correspondiente. En determinados dominios de segundo nivel se permite el registro de niveles inferiores (por ejemplo, mjusticia.gob.es)*»[1053]. Estos se sitúan en un plano comercial, pues normalmente el nombre de dominio registrado se relaciona con el nombre una marca, tal y como afirma RODRÍGUEZ RAPOSO: «*los nombres de dominio tienen una doble naturaleza; técnica, muy relacionada con las telecomunicaciones y otra de imagen de las organizaciones, relacionada con los derechos de propiedad industrial y los derechos de marcas*»[1054]. En la figura 3 se puede observar claramente la jerarquía y clases de los nombres de dominio.

Los nombres de dominio de primer nivel o «raíz»[1055] están gestionados a nivel global por la Corporación de Internet para la Asignación de Nombres y

---

[1049] Es decir «*Cada uno de estos dominios lleva un código de país de dos letras derivado de la Norma 3166 de la Organización Internacional de Normalización (ISO 3166), por ejemplo, .au (Australia), .br (Brasil), .ca (Canadá), eg (Egipto), .fr (Francia), .jp (Japón) y .za (Sudádrica). Algunos de estos sominios son abiertos en el sentido de que nos hay restricciones sobre las personas o entidades que pueden registrarse con ellos. Otros restringen los nombres únicamente a las personas o entidades que satisfagan ciertos criterios (por ejemplo, domicilio dentro del territorio)», íd.* Los códigos de cada país pueden consultarse en la página de la *Internacional Organization for Standarization* (ISO) en el siguiente enlace: https://www.iso.org/obp/ui/#search (consulta: 31 de noviembre de 2018).

[1050] En la primera parte de este estándar, se le asignan dos letras a cada país, y segunda parte es utilizado para asignar subdivisiones a los países de la primera parte relativos a sus provincias o estados.

[1051] *Google* ha realizado definiciones básicas que ayudan a los usuarios a comprender la diferenciación entre conceptos relacionados con la web como nombres de dominio, URL, página web, las cuales pueden ser consultadas en el siguiente enlace: https://domains.google/intl/es-419_ALL/learn/the-difference-between-a-url-domain-website-more.html#/ (consulta: 7 de noviembre de 2018).

[1052] *Vid.* terminología y funciones ICAAN: https://www.icann.org/resources/pages/what-2012-02-25-es (consulta: 9 de noviembre de 2018).

[1053] BARRIO ANDRÉS, M., *op. cit.*, p. 187.

[1054] *Vid.* RODRÍGUEZ RAPOSO, A., *op. cit.*, p. 73.

[1055] *Vid. Ib.,* p. 72.

Números (ICANN, *The Internet Corporation for Assigned Names and Numbers*)[1056], creada en 1998 como una corporación sin fines de lucro y «*constituida al amparo de la legislación de California (su Nounprofit Public Benefit Corporation Law de 1978). Fue creada el 18 de septiembre de 1998 para hacer posible la gestión privada de la arquitectura técnica de Internet, para ello asumió una serie de funciones que antes realizaba directamente en nombre del gobierno norteamericano otras organizaciones, en particular la citada IANA, la cual –según se acaba de indicar- pasó a integrarse en la ICANN como uno de sus departamentos. (…) la ICANN la que decide los criterios que determinan qué categorías de nombres de dominio de primer nivel pueden existir y adopta las decisiones fundamentales sobre cómo se asignan* »[1057].

Los nombres de dominio de nivel superior genéricos (gTLDs) deberán ser registrados ante la ICANN, específicamente ante la *Public Technical Identifiers* (PTI)[1058] (de la cual se hablará posteriormente), antes de la creación de la ICANN, la labor de registro la realizaba la IANA (*Internet Assigned Numbers Authority)* [1059], «*una de las Instituciones más antiguas de Internet, e inicialmente actuó como órgano*

[1056] Anteriormente aproximadamente entre los años 91-92, la *National Science Foundation* «asumió la responsabilidad de coordinar y financiar la gestión de la parte no militar de la infraestructura de internet» entre los que se incluían los Nombres de Dominio, trad. Del inglés: «*NSF assumed responsibility for coordinating and funding the management of the non-military portion of the Internet infrastructure*», *vid.* United States Department of Commerce, The White paper (en línea) Disponible en: https://www.icann.org/resources/unthemed-pages/white-paper-2012-02-25-en (consulta: 9 de julio de 2019). Posteriormente la NSF, realizó un convenio de cooperación el 31de diciembre de 1992 con *Network Solutions, Inc.,* para que esta última se hiciera cargo (entre otras) de los servicios de registro de los nombres de dominio, después esta función fue asumida por la IANA hasta mediados de los noventas «*en virtud de un contrato celebrado con el Instituto de Ciencias de la Información de la Universidad de Southern California (USC) en lo que se denominaba las funciones de IANA*» (*vid.* BARRIO ANDRÉS, M., *op. cit*., p. 172), hasta que, en 1998, esta función de registro de los nombres de dominio pasa a ser parte de la ICANN.

[1057] BARRIO ANDRÉS, M., *op. cit*., p. 169.

[1058] *Vid.* Página web de la *Public Technical Identifiers*: https://pti.icann.org/ (consulta: 11 de julio de 2019).

[1059] El ICAAN ha asumido las funciones de la IANA (*Internet Assigned Numbers Authority*) desde 1998, actualmente es parte de uno de sus departamentos. Se encarga entre otras cosas del registro de los nombres de dominio de nivel superior como «.int», el cual corresponde a instituciones trasnacionales como la OMS (*World Health Organization*) *In fine: who.int*. *vid.* https://www.icann.org/resources/pages/what-2012-02-25-es (consulta: 11 de julio de 2019). También se encarga de administrar los servidores raíz, que son «*el nivel más alto de jerarquía del DNS*», *vid.* RODRÍGUEZ RAPOSO, A., *op. cit*., p. 73. Los cuales *«almacenan una copia del mismo archivo que actúa como índice principal de las agendas de direcciones de Internet»,* estas copias se almacenan en diferentes ubicaciones geográficas por seguridad en https://www.icann.org/resources/pages/what-2012-02-25-es (consulta: 12 de noviembre de 2018); también se encarga de administrar «*algunos recursos de nombres de dominio internacionalizados (aunque no utilizan el alfabeto latino)», vid.* BARRIO ANDRÉS, M., *op. cit*., p. 168.

central de coordinación, asignación y registro de direcciones IP, nombres de dominio y parámetros de fundación de Internet»[1060]. Actualmente se utiliza el término IANA para hacer referencia al conjunto de funciones que tienen que ver con las direcciones IP, los nombres de dominio y los protocolos de internet[1061].

Respecto a la administración y gestión de dominios de segundo nivel, el ICANN delega estas funciones a «*otras entidades, las cuales, a su vez, se encargan de delegar dominios de segundo nivel a usuarios finales*»[1062], por ejemplo, para el registro de un nombre de dominio de segundo nivel con el ccTLDs «.es», este se deberá realizar ante la Entidad pública Empresarial «Red.es», quien a su vez habilitará a Agentes registradores para la realización de esta actividad[1063].

En relación a los códigos de países de nivel superior, en Europa existe una Asociación denominada *Council of European National Top-Level Domain Registries,* cuyo objetivo es promover y desarrollar estándares de buenas prácticas entre los registros de ccDTL[1064]. Sin embargo, los códigos geográficos nacionales (ccTLDs) son gestionados directamente por las autoridades de cada país, tal como se mencionó antes «*por delegación de la ICANN, a las distintas autoridades nacionales de registro de dominios nacionales (Network Information Centers o NICs), en las que con el paso del tiempo los gobiernos estatales han venido desempeñando un creciente papel, al considerarlos un aspecto vinculado con su soberanía y con los intereses nacionales*»[1065]. Excepcionalmente esta circunstancia no opera para el dominio «.eu», este ccTLDs está gestionado por el Registro Europeo de Dominios de Internet

---

[1060] BARRIO ANDRÉS, M., *op. cit*., p. 168.

[1061] De conformidad con lo establecido por FRÍAS, Z., PÉREZ, J. Y STECK, CH., «Gobernanza de Internet y derechos digitales», QUADRA-SALCEDO, T. y PIÑAR MAÑAS, J. L. (Dirs.), *Sociedad digital y derecho*. B.O.E., Madrid, 2018, p. 536; TORRE DE SILVA Y LÓPEZ DE LETONA, J., *Internet, propiedad industrial y competencia desleal,* Centro de Estudios Políticos y Constitucionales, Madrid, 2002, p.47: «*Habitualmente se menciona a IANA como si fuera una entidad. No obstante, propiamente es una forma de denominar un conjunto de funciones*»; y BARRIO ANDRÉS, M., *op. cit.,* p. 169.

[1062] RODRÍGUEZ RAPOSO, A., *op. cit*., p. 72.

[1063] También se puede solicitar directamente el registro de un nombre de dominio de segundo nivel ante «Red.es», pero solo se realizará «*para situaciones muy concretas que no requieran intermediarios por circunstancias especiales. El registro directo a través de Red.es ofrece solamente el nombre de dominio (ningún servicio adicional) y por sus condiciones particulares supone un precio elevado regulado por instrucción interna*», *vid.* página web de «Red.es»: https://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/sobre-registros-de-dominios/cuanto-cuesta (consulta: 9 de julio de 2019).

[1064] *Vid.* https://centr.org/about/about-centr.html (consulta: 13 de noviembre de 2018).

[1065] BARRIO ANDRÉS, M., *op. cit*., p.189.

(*European Registry for Internet Domains* –EURid-), quien mantiene un acuerdo con la ICANN desde el 2014[1066], entidad que desempeñará las funciones de «registro», de conformidad con el nuevo Reglamento (UE) 2019/517 del Parlamento Europeo y del Consejo de 19 de marzo de 2019, sobre la aplicación y el funcionamiento del nombre de dominio de primer nivel «.eu», por el que se modifica y deroga el Reglamento (CE) nº 733/2002 y se deroga el Reglamento (CE) nº 874/2004 de la Comisión.

En España, «la normativa reguladora de los dominios bajo ".es" ha experimentado una gran evolución en el tiempo transcurrido desde su implantación. Las funciones de Registro Delegado de Internet en España, encargado de la administración del dominio de nivel superior .es, conocido como ES-NIC, fueron inicialmente desempeñadas por Red IRIS, que era un departamento del Consejo Superior de Investigaciones Científicas (CSIC)»[1067]. Posteriormente, de conformidad con la Disposición adicional sexta de la Ley 11/1998, de 24 de abril, General de Telecomunicaciones, fue creada la entidad «Red.es», configurándose como una entidad pública empresarial conforme a lo previsto en la entonces Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado[1068] adscrita al entonces Ministerio de Industria, Energía y Turismo, a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.

Finalmente la Ley 11/ 1998 es derogada por la Disposición derogatoria única de la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, sin embargo, se prevé la conservación de la entidad empresarial «Red.es», de conformidad con la Disposición adicional decimosexta, atribuyéndole entre otras, las funciones de gestión del registro de los nombres y direcciones de dominio de internet bajo el código de país correspondiente a España (.es); de participación en los órganos que coordinen la gestión de Registros de nombre y dominios de la Corporación de

[1066] *Vid.* Informe de la Comisión al Parlamento Europeo y al Consejo sobre la aplicación, funcionamiento y eficacia del dominio de primer nivel «.eu», de 18 de diciembre de 2015 –COM (2015) 680 final–. Disponible en: http://ec.europa.eu/transparency/regdoc/rep/1/2015/ES/1-2015-680-ES-F1-1.PDF (consulta: 11 de julio de 2019).
[1067] BARRIO ANDRÉS, M., *op. cit.*, p.189.
[1068] Arts. 43. Apartado 1.b) y 3 de la Ley 6/1997, de 14 de abril, de Organización y Funcionamiento de la Administración General del Estado.

Internet para la Asignación de Nombres y Números (ICANN); y de asesoramiento especialmente frente al Comité Asesor Gubernamental de la ICANN (GAC)[1069] y, en general cuando le sea solicitado, el asesoramiento a la Administración General del Estado en el resto de los organismos internacionales y, en particular, en la Unión Europea, en todos los temas de su competencia. Sin embargo, los criterios de asignación de los nombres de dominio «.es», están regulados a su vez por la Disposición adicional sexta de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico; por el Plan Nacional de Nombres de Nombres de Dominio de Internet bajo el código de país correspondiente a España («.es»)[1070]y por las instrucciones realizadas por el Director General de la Entidad Pública empresarial «red.es»[1071].

La asignación de nombres de dominio junto con otros «recursos nucleares» de Internet[1072], son parte de lo que hoy se denomina «gobernanza de Internet»[1073], locución acuñada en los años noventa por miembros del Proyecto de infraestructura de Información de la Universidad de Harvard (*Information Infrastructure Proyect - HIIP-)* [1074] , «*describía un mecanismo de gestión de la Red sin fronteras, sin*

[1069] El Comité Asesor Gubernamental sirve como la voz de los gobiernos y organizaciones gubernamentales internacionales en la estructura representativa de múltiples partes interesadas de la ICANN, trad. Del inglés: «*The GAC serves as the voice of Governments and International Governmental Organizations in ICANN's multi-stakeholders representative structure*». *Vid.* https://gac.icann.org/ (consulta: 9 de julio de 2019).

[1070] Orden ITC/1542/2005, de 19 de mayo, que aprueba el Plan Nacional de nombres de dominio de Internet bajo el código de país correspondiente a España («.es»), *vid.* https://www.boe.es/diario_boe/txt.php?id=BOE-A-2005-8902 (consulta: 9 de julio de 2019).

[1071] Por ejemplo, la relativa al «*desarrollo de los procedimientos aplicables a la asignación y a las demás operaciones asociadas al registro de nombres de dominio bajo el ".es"*», y la relativa al «*establecimiento del procedimiento de reasignación para nombres de dominio de excepcional interés general*», *vid.* https://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/normativa/instruccion-procedimientos-de-dominios (consulta: 9 de julio de 2019).

[1072] Tales como las direcciones IP, los protocolos de red, de conformidad con lo establecido por BARRIO ANDRÉS, M., *op. cit*., p. 160.

[1073] El diccionario de la Lengua Española define como gobernanza al «*Arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía*», *vid.* https://dle.rae.es/?id=JHRSmFV (consulta: 10 de julio de 2019). Sin embargo, tal y como establecen FRÍAS, Z., PÉREZ, J. Y STECK, CH. el caso de Internet es totalmente distinto al de las telecomunicaciones, ya que «*el modelo de gobernanza de Internet responde a unos principios de soberanía compartida que permiten la participación de, además de los gobiernos, la comunidad técnica, la sociedad civil, la academia y el sector privado*», *Vid.* FRÍAS, Z., PÉREZ, J. Y STECK, CH., *op. cit.*, p. 533.

[1074] KLEINWÄCHTER, W., «Good governance of the borderless Internet: Who should do what?» (en línea), *Telos,* núm. 80 Disponible en: https://telos.fundaciontelefonica.com/archivo/numero080/good-governance-of-the-borderless-internet-who-should-do-what/ (consulta: 5 de julio de 2019).

participación directa de los gobiernos»[1075]. Posteriormente, derivado de la necesidad de los gobiernos en buscar soluciones idóneas en relación con la sociedad de la información y específicamente respecto a Internet, se lleva a cabo la Cumbre Mundial sobre la Sociedad de la Información (CMSI)[1076], donde se consolidó el contenido de lo que se entiende por gobernanza de Internet, utilizándose «*para hacer referencia al desarrollo de principios, reglas y mecanismos de toma de decisión acerca del funcionamiento y desarrollo de Internet. Clave en la idea de gobernanza de Internet es la pretendida participación de las múltiples partes interesadas, como gobiernos, organizaciones gubernamentales e internacionales, sector privado, sociedad civil y comunidades académica y técnica»* [1077]. De conformidad con lo establecido por FRÍAS, PÉREZ Y STECK, la gobernanza de Internet cuenta con dos planos diferenciados, el técnico y el social, la gobernanza técnica «*tiene una estructura muy definida que gira alrededor de las llamadas funciones IANA y en la que las organizaciones participan en un área específica (nombres, números, estándares o infraestructura)* »[1078], mientras que la gobernanza social «*está formada por un compendio de instituciones que participan en el ecosistema en el ámbito de sus competencias o soberanía*»[1079].

La gobernanza de Internet se hace tangible dentro de la ICANN con el anuncio en 2014 del Departamento de Comercio de los Estados Unidos de América de finalizar la labor supervisora que hasta el momento realizaba a la corporación, «*siempre y cuando se encontrara un mecanismo que sirviera de reemplazo (NTIA, 2014) y que: i) apoyara el modelo multistakeholder, ii) mantuviera la seguridad, estabilidad y resiliencia del sistema de nombres de dominio, satisficiera las necesidades y expectativas de los clientes y socios de los servicios de IANA, y iii) mantuviera la naturaleza abierta de Internet*», llevándose a cabo efectivamente hasta el 1 de octubre de 2016[1080]. A partir de este momento la ICANN «*ha adoptado un modelo de gestión de múltiples partes interesadas (multistakeholder governance*

[1075] *Íd.*
[1076] En dos fases: 2003 en Ginebra y 2005 en Túnez.
[1077] BARRIO ANDRÉS, M., *op. cit.,* p. 161. Los documentos finales de la CMSI, pueden consultarse en el siguiente enlace: https://www.itu.int/net/wsis/index-es.html (consulta: 1 de diciembre de 2020). El término es usado por vez primera en el documento final- compromiso de Túnez.
[1078] FRÍAS, Z., PÉREZ, J. Y STECK, CH., *op. cit*., p. 535.
[1079] *Íd.*
[1080] BARRIO ANDRÉS, M., *op. cit.,* p. 173.

model), que incluye además de los Estados, agentes económicos, organismos técnicos y organizaciones sociales» [1081]. La ICANN bajo la adopción de este modelo «*ha conseguido desarrollar una organización adaptada a los retos del siglo XXI, en el que el mundo es cada vez más global y más heterogéneo al mismo tiempo*»[1082]. Derivado de lo anterior, en 2018 se ha creado la *Public Technical Identifiers (PTI)* [1083] para dar solución a una de las condicionantes planteadas en 2014 por el Departamento de Comercio de los Estados Unidos, cuyo objetivo es realizar la gestión de las funciones IANA en nombre de la ICANN [1084]. Así pues, los gobiernos mantienen una participación activa dentro de la ICANN por medio del GAC, debido a su labor asesora «*en cuestiones en las que se intersectan las actividades y políticas de ICANN y las leyes nacionales o los tratados internacionales*» [1085]; cuestión de especial importancia para el derecho actual, específicamente la integración de la gobernanza global, concretamente de Internet, al denominado Derecho administrativo global (*Global Administrative Law* -GAL-)[1086].

[1081] *Íd.* El modelo *multistakeholder* «*se define como una forma de gobernanza y de toma de decisiones basada en la cooperación entre distintos grupos de interés para encontrar soluciones a sus problemas u objetivos comunes*», definición de ADAM PEAKE citado en FRÍAS, Z., PÉREZ, J. Y STECK, CH., *op. cit.*, p. 534.

[1082] FRÍAS, Z., PÉREZ, J. Y STECK, CH., *op. cit.*, p. 537.

[1083] *Vid. Articles of incorporation Public Technical Identifiers,* disponible en: https://pti.icann.org/iana_pti_docs/141-articles-of-incorporation-v-09aug16 (consulta: 10 de julio de 2019).

[1084] *Íd.*

[1085] FRÍAS, Z., PÉREZ, J. Y STECK, CH., *op. cit.*, p. 538.

[1086] El Derecho Administrativo Global o Global Administrative Law (GAL), parte de «*constatar la existencia de una quiebra de la separación tradicional entre la esfera interna y la esfera externa de actuación de los Estados*», continúa señalando que: «*Esta quiebra se corresponde, por un lado, con el denominado proceso de internacionalización del Derecho Administrativo*», *Vid.* DARNACULLETA GARDELLA, M., «El Derecho Administrativo Global ¿Un nuevo concepto clave del Derecho Administrativo?» (en línea), *Revista de administración pública*, 2016, p. 31-32. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5492352.pdf (consulta: 7 de julio de 2019). Además de contemplar como parte del mismo a las organizaciones supranacionales, también incorpora dentro de la disciplina a las organizaciones privadas; por su parte los autores KINGSBURY, B., KRISCH, N. Y STEWART, R. B., definen al GAL como «*as comprising the mechanisms, principles, practices, and supporting social understandings that promote or otherwise affect the accountability of global administrative bodies, in particular by ensuring they meet adequate standards of transparency, participation, reasoned decision, and legality, and by providing effective review of the rules and decisions they make. Global administrative bodies include formal intergovernmental regulatory bodies, informal intergovernmental regulatory networks and coordination arrangements, national regulatory bodies operating with reference to an international intergovernmental regime, hybrid public–private regulatory bodies, and some private regulatory bodies exercising transnational governance functions of particular public significance*», Cfr. BENEDICT KINGSBURY, *et al.*, «The Emergence of Global Administrative Law», *Law and Contemporary Problems, Summer 2005*, 68, 15-62 Disponible en: https://scholarship.law.duke.edu/lcp/vol68/iss3/2 (consulta: 11 de junio de 2019). Dos de las

2. LOS NUEVOS SERVICIOS Y HERRAMIENTAS WEB.

Las tecnologías de la información y comunicación se podrían definir como aquellas herramientas tecnológicas que son creadas a partir de «la informática, la microelectrónica y las telecomunicaciones»[1087] las cuales permiten el acceso a la información y permiten la difusión de la misma[1088]. Como se explicó anteriormente, dentro del objeto de estudio de la informática se sitúa así Internet y dentro de este se desarrolla la web. Estas nuevas herramientas tienen su origen en el cambio que trajo consigo la web 2.0, debido a que permiten comunicarnos con facilidad, de manera interactiva e intuitiva, y normalmente estas herramientas suelen tener objetivos definidos como permitir la difusión de la información, mejorar la comunicación a nivel global y ofrecer una buena experiencia al usuario. En la medida en que la web evoluciona estas también lo hacen, diversificando las finalidades y usos.

2.1 Las redes sociales y profesionales

El ser humano siempre ha tenido la necesidad de relacionarse con otros, hecho que se constata desde la antigüedad, según Aristóteles el ser humano es desde siempre un *zoon politikón,* debido a su habilidad de relacionarse con otros y desarrollar su naturaleza política cuando este vive en sociedad. Las relaciones

cuestiones de gran importancia (que no las únicas) que atañen a estas dos disciplinas, serían por una parte si el Derecho Administrativo Global, admite y valga la redundancia como derecho a los acuerdos tomados por la Junta Directiva de la ICANN; por otra parte, la compatibilidad de los valores y principios aplicables a las corporaciones privadas al formar parte del denominado derecho administrativo global, por ejemplo, en el ámbito de Internet, encontramos unos principios específicos que regulan esta tecnología, los cuales, sin ser vinculantes para los Estados *«parten de la necesidad el reconocimiento de los derechos online y offline», Vid.* FRÍAS, Z., PÉREZ, J. Y STECK, CH., *op. cit.*, p. 544. Están recogidos en «La Declaración multisectorial de Sao Paulo de NETmundial», *vid.* https://netmundial.org/sites/default/files/InternetGovernancePanel-Report.pdf); y que estos a su vez sean compatibles con los valores y principios derivados del Derecho administrativo nacional, como bien menciona DARNACULLETA GARDELLA, M., «*no existe, sin embargo, un consenso, ni sobre el Derecho Administrativo nacional del cual se está hablando, ni sobre los mecanismos a través de los cuales puede y/o debe producirse esta extensión*», Cfr. DARNACULLETA GARDELLA, M., *op. cit.*, p. 31-32.

[1087] BELLOCH ORTÍ citando a CABERO, Cfr. BELLOCH ORTÍ., C., «Las tecnologías de la información y comunicación (T.I.C.)» (en línea). Disponible en: https://www.uv.es/~bellochc/pdf/pwtic1.pdf (consulta: 1 de abril de 2019).

[1088] Quizás una definición más completa sobre las tecnologías de la información y comunicación es aquella dada por BELLOCH ORTÍ: «*son el conjunto de tecnologías que permiten el acceso, producción, tratamiento y comunicación de información presentada en diferentes códigos (texto, imagen, sonido...)*», *ib.*, p.1.

personales pueden ser de distinta naturaleza traducidas en relaciones de amistad, afectuosas, profesionales, etc.

El Diccionario de la lengua española define como red social a la «*plataforma digital de comunicación global que pone en contacto a un gran número de usuarios*»[1089]; lo cual refleja el traslado de nuestras relaciones personales al ámbito digital, incluso hay personas que han ido más allá creando una relación de afinidad con personas a las cuales nunca han visto, en gran medida gracias a la web, la cual nos permite romper barreras espacio-temporales, permitiendo incorporar a nuestro círculo social a personas de otras partes del mundo.

Antes de hablar de los conceptos propios de la era digital, es conveniente saber cómo han ido evolucionado conceptualmente lo que hoy denominamos redes sociales. Han sido muchos teóricos desde el siglo XIX los que trataron de explicar las relaciones personales. Uno de ellos fue Émile Durkheim[1090], en palabras de MORENO PÉREZ «*porque él no considera a la sociedad como un organismo, viendo en ella un sistema biológico, un gran organismo, tanto en su estructura como en sus funciones, el cual reflejaría el mismo tipo de unidad que el organismo del individuo, siendo las células de la sociedad las personas individuales, y sus órganos y sistemas, las asociaciones e instituciones. Se ha señaló que en su forma extrema la teoría organicista identifica las estructuras específicas de la sociedad con los órganos y sistemas biológicos*»[1091]. Para el sociólogo y filósofo francés era importante la interacción con otros en el ámbito laboral y, es ahí donde alcanza su estatus de ser social. Así pues, la sociedad estaría dividida en una con carácter orgánico y otra con carácter mecánico. La primera de ellas se constituye de personas con autonomía individual, las cuales realizan un trabajo definido, y estas no tienen por qué desnaturalizarse por la existencia de un cuerpo superior llamado sociedad al que está integrado. La sociedad «*no aparece solamente como una fuerza de presión (coacción social), sino*

[1089] *Vid.* https://dle.rae.es/?id=VXs6SD8 (consulta: 2 de abril de 2019).
[1090] Emile Durkheim, padre de la sociología francesa, sus estudios fueron publicados a finales del siglo XIX y principios del siglo XX, entre los que destaca su tesis doctoral «De la división del Trabajo Social» (1893).
[1091] MORENO PÉREZ, J. L., «El pensamiento político-jurídico de Durkheim: solidaridad, anomia y democracia (I)» (en línea), *Revista de derecho constitucional europeo,* núm. 10, 2008, p. 398 Disponible en: https://dialnet.unirioja.es/descarga/articulo/3014022.pdf (consulta: 22 de enero de 2018).

que es esencialmente para el individuo un medio de elevación y expansión de la propia personalidad y dignidad humana. La solidaridad orgánica supone el avance del individualismo moral»[1092]. En cambio, en las sociedades mecánicas no es preminente esa diferenciación del trabajo que realizan los individuos. En este sentido FREEMAN, haciendo referencia a la teoría de Durkheim, establece que «*la solidaridad mecánica, que ligaba a individuos de características similares a través de lazos sociales normativos, y solidaridad orgánica que, en sociedades modernas y urbanas, hacía que los individuos cooperaran a través de la división del trabajo*»[1093].

Lo idílico para Durkheim sería vivir en una sociedad orgánica o evolucionada, en este tipo de sociedad desarrollaríamos, autonomía individual y una conciencia colectiva, esta última es un conjunto de ideales y creencias aceptados por el promedio de sus miembros. Si trasladamos esta teoría a la actualidad podríamos decir que efectivamente en la web y específicamente en las redes sociales, los individuos cuentan con una conciencia individual y otra conciencia colectiva, ya que cada uno discernimos acerca del contenido que queremos en nuestras redes sociales, sin embargo, hay una especie conciencia colectiva respecto al contenido de nuestras redes sociales y de lo que se considera aceptable para la sociedad; sin embargo, estos parámetros pueden variar dependiendo de la época y lugar en donde se situé el individuo. Considero que la globalización y los avances tecnológicos son determinantes para que estos parámetros sean cada vez más estandarizados.

Otro teórico que estudió las relaciones personales fue FERDINAND TÖNNIES, en su obra Comunidad y sociedad (*Gemeinschaft und Gessellschaft)*, donde las define como el conjunto de «l*as distintas voluntades humanas»*[1094], este estudio solamente se centra en las que para él tienen naturaleza positiva, es decir, aquellas que son recíprocas, «*Cada una de estas relaciones representa una unidad en lo plural o una pluralidad en lo unitario. Consiste en estímulos, prestaciones, servicios que las partes intercambian entre sí y que se consideran expresión de las diversas voluntades y de las fuerzas respectivas. El grupo formado por el tipo positivo de relación recibe el nombre*

[1092] *Íd.*
[1093] FREEMAN, L. C., *El desarrollo del análisis de redes sociales, un estudio de sociología de la ciencia*, Trad. Alcántara Valverde, N. Palibrio, EE.UU. p.14
[1094] TÖNNIES, F., *Comunidad y Asociación, comunismo y socialismo como formas de vida social*, Trad. JOSÉ-FRANCISCO IVARS. Badalona, Ed. Península, 1979, p. 27.

de ligamen (Verbindung) cuando se concibe en calidad de ser o cosa que actúa como unidad tanto hacia su núcleo como hacia su exterior»[1095].

Para este autor, las relaciones sociales podían desarrollarse en dos ámbitos, ya sea dentro de *Gemeinschft* (comunidad), las cuales tienen un carácter orgánico y real, este tipo de relaciones se desarrollan primordialmente en el seno familiar, bien dentro de la *Gesellschft* (sociedad o asociación), este tipo de relaciones las denomina como mecánicas e instrumentales; las relaciones originarias y las más antiguas son las primeras. Si trasladamos la teoría de TÖNNIES al entorno digital no podríamos encontrar relaciones de comunidad virtuales ni con nuestros familiares, por ejemplo, si los miembros de nuestra familia contaran con redes sociales y también fuésemos amigos en cualquier red social elevando dicha relación al entorno digital, dicha relación se desnaturalizaría esa comunidad de conformidad con su teoría. Respecto a las demás relaciones sociales, que no se hayan en la comunidad, estas tendrían la calidad de instrumentales dentro del seno de la asociación, con fines definidos por intereses comunes, ya sean personales o profesionales, es decir, en toda clase de redes sociales digitales encontraríamos relaciones de esta índole (Facebook, LinkedIn, Instagram, Flickr, etc.).

La definición de comunidad según el Diccionario de la lengua española establece en su primera acepción, aquello que es relativo a una cualidad en común, por lo que son estas cualidades, los avances en el entorno digital (TIC) y la forma de comunicarnos que nos hacen darle un nuevo sentido al contenido de la palabra comunidad. HOWARD RHEINGOLD, en su obra «*La comunidad virtual, una sociedad sin fronteras*», se encarga por vez primera en acuñar la expresión de «comunidad vitual» para referirse a «*agregados sociales que surgen de la Red cuando una cantidad suficiente de gente lleva a cabo estas discusiones públicas durante un tiempo suficiente, con suficientes sentimientos humanos como para formar redes de relaciones personales en el espacio cibernético*». Por lo que resulta inevitable pensar que las «comunidades virtuales» concebidas por RHEINGOLD aplicando la teoría de TÖNNIES, no serían comunidades, sino asociaciones guiadas por un interés común, en donde

[1095] *Íd.*

sus miembros «*permanecen esencialmente separados a pesar de todos los factores tendentes a su unificación*»[1096].

Otro teórico alemán que estudia las relaciones personales es GEORG SIMMEL, para este, existe una dicotomía entre la libertad y represión en un entorno social, en palabras de BREIGER para definir estos dos conceptos de SIMMEL «*la represión que la sociedad impone al individuo como un objeto pasivo puede darse la vuelta –al mismo tiempo, aunque desde un punto de vista opuesto- para revelar que los individuos se ejercitan como sujetos activos que gobiernan las formas sociales*»[1097]. Es dentro de esta libertad, donde encontramos la potestad de decidir si queremos pertenecer a un grupo, entendiendo a esta como la acción social «*fundamentada en el simple hecho de que el individuo está vinculado a otros y vincula a los otros*»[1098]. De hecho, se le atribuye a él, la implementación del término «red social». Para SIMMEL las personas son nodos de conexión con otras y estas a su vez forman parte de una red social, que es básicamente la idea general de las que hoy concebimos como redes sociales en el ámbito digital.

A principios del siglo XX, FRIGYES KARINTHY mediante su cuento «*Chains*», crea la teoría de los seis grados de separación, la trama está basada en que (ya en esa época) las personas podrían llegar a cualquier otra persona en el mundo por medio de seis grados consistentes en relaciones personales. Básicamente las personas son eslabones de una cadena de seis, donde el primero es la persona que desea llegar a la sexta y las intermedias son puentes ligados por sus relaciones personales con otras. En el año 2011, *Facebook* en su página publicó un estudio realizado en colaboración con la Universidad de Milán[1099], en donde se afirma que este eslabón de seis ya es cosa del pasado, actualmente se necesita un promedio de 4.78 saltos a nivel global para llegar a la persona deseada y en una esfera más reducida, en un mismo país, solo serían necesarios cuatro grados (tres saltos) para lograr nuestro

[1096] *Ib.,* p. 67.
[1097] BREIGER, R., «Control social y redes sociales: Un modelo a partir de Georg Simmel», Trad. PIZARRO, N. (en línea), *Política y sociedad,* p. 63 Disponible en: https://revistas.ucm.es/index.php/POSO/article/download/POSO0000130057A/24603 (consulta: 25 de enero de 2018).
[1098] *Ib.,* p. 64.
[1099] Dicho estudio se titula «*Anatomy of Facebook».* Disponible en: https://www.facebook.com/notes/facebook-data-team/anatomy-of-facebook/10150388519243859 (consulta: 6 de abril de 2019).

cometido. Lo anterior, refleja claramente el nivel de globalización, la popularidad de las redes sociales que se hacen más necesarias para los usuarios cada día, pero ante todo la eficiencia e implementación del avance tecnológico en su forma de relacionarse con los demás.

Ahora que conocemos de grosso modo los antecedentes sociológicos de las redes sociales digitales, es menester proceder al estudio de estas desde la perspectiva digital. Según el Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), las redes sociales son aquellos sitios «*en la red cuya finalidad es permitir a los usuarios relacionarse, comunicarse, compartir contenido y crear comunidades, o como una herramienta de "democratización de la información que transforma a las personas en receptores y en productores de contenidos*»[1100]. El Grupo de trabajo del artículo 29 las definió como *«plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes»*[1101].

Varios autores se han dado a la tarea de definirlas, POMMI define a las redes sociales como *«una estructura de social compuesta de personas (u organizaciones) llamados "nodos", los cuales están ligados (conectados) por uno o más tipos específicos de interdependencia, tales como amistad, parentesco, intereses comunes, intercambio financiero, aversión, relaciones sexuales, o las relaciones de creencias, conocimientos o prestigio»*[1102]. SIMÓN CASTELLANO entiende que los Servicios de red social (SRS) son «*aquellos servicios Web que permiten a los individuos constituir un perfil público, articular una lista de otros usuarios del sistema con los que poder compartir la información y visualizar las listas de otros usuarios del sistema»*[1103]. Por su parte, BOYD, D. M. y ELLISON, N. B. en su artículo «*Social Network Sites: Definitio, History, and*

[1100] En ONTSI, Estudio sobre el conocimiento y uso de las redes sociales en España (en línea), Disponible en: https://www.ontsi.red.es/ontsi/sites/ontsi/files/redes_sociales-documento_0.pdf (consulta: 6 de abril de 2019).
[1101] Dictamen 5/2009 sobre las redes sociales en línea adoptado el 12 de junio de 2009, por el Grupo de Trabajo sobre protección de Datos del Artículo 29 (01189/09/ES WP 13) p. 5.
[1102] Trad. Del inglés: *«A social network is a social structure made up of individuals (or organizations) called "nodes" which are tied (connected) by one or more specific types of interdependency, such as friendship, kinship, common interest, financial exchange, dislike, sexual relationships, or relationships of beliefs, knowledge or prestige»*, *Vid.* POMMI, S., *et al.*, «Social Networking Websites» (en línea), 2011. Disponible en: http://14.139.186.108/jspui/bitstream/123456789/2760/1/pommi.pdf (consulta octubre 2016).
[1103] SIMÓN CASTELLANO, P., «*El régimen. …», op. cit,* p. 23.

Scholarship» definen a las redes sociales como «*web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system*»[1104]. AGUSTINOY GUILAYN, A. y MONCLÚS RUIZ, J., definen red social «*como aquella plataforma tecnológica que permite a sus usuarios, a través de sus correspondientes perfiles, vincularse entre sí, creando sistemas cruzados e interactivos de generación y difusión de información»*[1105].

El primer antecedente de red social en el ámbito digital es «*clasemates*»[1106], la cual tiene su origen en el año 1995, la misión de esta web es reencontrar a compañeros de universidad, colegio, trabajo y hasta compañeros del ejército en Estados Unidos. Este tipo de páginas han ido mejorando con el paso del tiempo sobre todo con la introducción de las mejoras implementadas en la web 2.0, incluso en la actualidad los desarrolladores de las denominadas «redes sociales» introducen cambios que consideran idóneos para mejorar la experiencia de sus usuarios.

Para tener acceso a estas las personas deben realizar un perfil propio, el cual puede tener carácter abierto o restringido, la diferencia entre estos dos tipos de perfiles radica en la visibilidad que tienen otros usuarios de los datos y el contenido multimedia. Los datos que deben ser aportados en el registro de las redes sociales tienen carácter personal, pues se requiere el nombre y apellidos, sexo, fecha de nacimiento, país de origen, algún número telefónico, correo electrónico, entre otros; datos que sin dudad alguna nos hace plenamente identificables. Una vez creado el perfil, este puede servir como puente de comunicación con otras personas, sin limitación de espacio y tiempo.

[1104] En BOYD, D. M. y ELLISON, N. B., «Social Network Sites: Definition, History, and Scholarship» (en línea), *Journal of Computer- Mediated Communication,* Diciembre 2007. Disponible en: https://doi.org/10.1111/j.1083-6101.2007.00393.x (consulta: 6 de abril de 2019). Trad. del inglés: «*servicios dentro de las webs que permiten al usuario 1) construir un perfil público o semi-público dentro de un sistema limitado, 2) articular una lista de otros usuarios con los que comparte una conexión y 3) visualizar y rastrear su lista de contactos y las elaboradas por otros usuarios dentro del sistema*», de ONTSI, *op. cit.*

[1105] AGUSTINOY GUILAYN, A. y MONCLÚS RUIZ, J., *Aspectos legales de las redes sociales,* Bosch, Barcelona, 2016, p. 18.

[1106] El nombre de dominio de esta página era: www.classemates.com.

Tal y como señalan los autores AGUSTINOY GUILAYN, A. y MONCLÚS RUIZ, J. las redes sociales tienen diversas clasificaciones en función del tipo de *perfil de los usuarios de sus contenidos* y *teniendo en cuenta los contenidos*. La primera de estas clasificaciones atiende como se adelanta al perfil de los usuarios, sub-clasificándose a su vez en horizontales y verticales, las redes sociales de perfil horizontal tienen «*un ánimo marcadamente generalista, permitiendo a sus usuarios la creación de un perfil para la publicación de contenidos e interacción con otros usuarios sin una vocación específicamente predefinida. Se busca crear un espacio de conexión abierto a diversos usos, desde el personal, pasando por el profesional así como, entre otros el de entretenimiento. Para ello, el operador de la red ofrece a sus usuarios una plataforma para compartir información en múltiples formatos (texto, imagen, audio, vídeo), lo cual acentúa su vocación potencialmente transversal*, añadiría que en este tipo de redes todos los usuarios son iguales en estas plataformas, cada uno es libre de compartir con los demás cuanta información le apetezca a través de su perfil, pudiendo ser de índole personal, familiar y profesional, estas redes nos proporciona gran información de los usuarios, ya que podemos trazar un perfil bastante definido del mismo, entre los ejemplos más destacados de este tipo de redes sociales encontramos a *Facebook*[1107] *y Twitter*[1108].

[1107] Según la descripción dada por la empresa, *«su misión es dar a la gente el poder de compartir y hacer un mundo más abierto y conectado»*. La gente utiliza *Facebook* para estar conectado con amigos y familiares, descubrir lo que está pasando en el mundo y compartir y expresar lo que les importa (trad. del inglés: *Facebook's mission is to give people the power to share and make the world more open and connected. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them*), *vid. Facebook*. Disponible en: https://www.facebook.com/facebook/about/?entry_point=page_nav_about_item&tab=page_info (Consulta: 12 junio 2017). Podemos acceder a ella ya sea mediante la página *Web* o una aplicación para tabletas y móviles, en donde se puede compartir fotos, vídeos, ubicaciones, estados de ánimo, etiquetar a personas en una publicación para que sea también visible en el perfil la persona etiquetada e incluso en 2016 se introdujo la posibilidad de transmitir en directo por medio de un vídeo lo que ocurre a tu alrededor, en el año 2017, al igual que *Instagram* se pueden publicar historias en formato vídeo o fotografía, cuya duración de visibilidad es de 24 horas.

[1108] Es una red social creada en el año 2006, donde los usuarios crean un perfil ya sea personal o corporativo, donde se puede transmitir a las personas que le siguen (sus contactos) un mensaje de hasta 140 caracteres y su principal característica es la inmediatez. Según ALAN RUSBRIDGER, quien hasta 2015 fue editor de *The Guardian*, en una entrevista realizada para el periódico el País, definía a *Twitter* como: *«La herramienta periodística más poderosa de los últimos 10 años», vid.* País, Ediciones, 2017, Entrevista «Debo ser más radical en lo digital», Cfr. El País, Debo ser más radical en lo digital. Disponible en: http://elpais.com/diario/2010/09/12/domingo/1284263555_850215.html (Consulta 12 junio 2017).

Por el contrario, las redes sociales de perfil vertical «*están dirigidas a un perfil de usuario específicamente predefinido (configurándose dichas redes a fin de adaptarse a dicho perfil y sus potenciales necesidades de publicación y distribución de contenidos)*»[1109], pudiendo ser profesionales o de ocio[1110]. En las redes sociales profesionales «*los usuarios generan y comparten en su perfil información relacionada con su carrera o actividades profesionales*»[1111], quizás la más popular sea *LinkedIn*[1112], sin ser la única en su tipo[1113].

Para tener acceso a este tipo de redes también es necesaria la creación de un perfil, cuyo fin sea personal o empresarial. En estas redes se detalla la vida profesional y académica de sus miembros, y en el caso de que el perfil pertenezca a una persona jurídica se detallan los valores y principios corporativos de la misma. Son objetivos comunes de este tipo de redes el relacionar a profesionales de diversas áreas y países, difundir ofertas de empleo publicadas por empresas a través de este medio o en su caso buscar posibles candidatos para alguna vacante en la misma con base en la información suministrada en los perfiles, y dar difusión y «*tratar temáticas específicas vinculadas con un desarrollo profesional*»[1114]. Dentro de esta clasificación podemos encontrar a las redes profesionales dirigidas específicamente

---

1109 *Íd.*

1110 Los autores AGUSTINOY GUILAYN, A. y MONCLÚS RUIZ, J., señalan a las «Redes de difusión del conocimiento» como una tercera subcategoría de esta clasificación, cuyo principal objeto es «*permitir a los usuarios intercambiar de forma altruista información sobre diversos temas, nutriéndose la red en cuestión de contenidos continuamente generados o actualizados por los propios usuarios (como por ejemplo Answers -www.answers.com-, Wikispaces -www.wikispaces.com-, o wikia -www.wikia.com-)*, *vid.* AGUSTINOY GUILAYN, A. y MONCLÚS RUIZ, J., *op. cit.*, p. 22. Sin embargo, difiero con la clasificación debido a que no considero que se trate de una red social, ya que no se genera un perfil, ni tampoco se articula una lista de contactos, la difusión de conocimiento puede darse en redes generalistas. Considero que este tipo de páginas deben considerarse como un servicio.

1111 *Íd.*

1112 LinkedIn se auto define como «*la mayor red profesional del mundo con más de 546 millones de usuarios en más de 200 países y territorios*», esta red social se creó en el 2002, y se lanzó oficialmente el 5 de mayo de 2003, *vid.* https://about.linkedin.com/es-es (consulta: 8 de abril de 2019).

1113 Dentro de estas encontramos a *Xing* , *vid.* https://www.xing.com/es (consulta: 8 de abril de 2019); *Viadeo, vid.* https://es.viadeo.com/es/ (consulta: 8 de abril de 2019), y a *Google +.* Respecto a esta última, antes era catalogada como una red social generalista, es decir, es decir, que cualquier persona podía crearse un perfil en la misma siempre y cuando contara con un correo electrónico de *Google*, y podía compartir cualquier tipo de contenidos como fotos, vídeos, un *microblog*, etc. Actualmente esta red social solamente provee servicios a cuentas de *G Suite* (un paquete de servicios de *Google* ofrecido a empresas o centros educativos, entre los que se encuentra el correo electrónico, calendario, nube, etc.), el servicio a particulares se cerró el 2 de abril de 2019, de ahí su inclusión en este tipo de redes, *vid.* https://support.google.com/plus/?hl=es#topic=9259565 (consulta: 8 de abril de 2019).

1114 DÍAZ VICARIO, A., FERNÁNDEZ DE ÁLAVA, M., Y BARRERA-COROMINAS, A., *op. cit.*, p. 2.

a científicos, investigadores y académicos como *ResearchGate*[1115], *Academia.edu*[1116], *Mendeley*[1117], entre otras, su finalidad principal es darle difusión al trabajo científico, subir artículos o resultados de sus trabajos a la plataforma para compartirlos con los demás investigadores, así como crear una red de contactos.

Las redes sociales también se pueden clasificar por el tipo de contenido que albergan, por lo que se consideran especializadas, el formato de los contenidos de este tipo de red sociales es diverso, de entre las categorías más populares encontramos las que se especializan en vídeo como *YouTube* [1118], *Vimeo* y *Periscope* [1119], «*en este tipo de red, el operador potencia el uso de contenidos en formato audiovisual*»[1120]; las redes sociales de imágenes, almacena «*contenidos en formato fotográfico o grafico en general*»[1121], entre los ejemplos más destacables

[1115] «*ResearchGate is the professional network for scientists and researchers. Over 15 million members from all over the world use it to share, discover, and discuss research. We're guided by our mission to connect the world of science and make research open to all*». Disponible en: https://www.researchgate.net/about (consulta: 6 de abril de 2019).

[1116] «*Academia.edu is a platform for academics to share research papers. The company's mission is to accelerate the world's research. Academics use Academia.edu to share their research, monitor deep analytics around the impact of their research, and track the research of academics they follow. Over 79 million academics have signed up to Academia.edu, adding 22 million papers. Academia.edu attracts over 63 million unique visitors a month*». Disponible: https://www.academia.edu/about (consulta: 6 de abril de 2019).

[1117] «*Mendeley is a free reference manager and academic social network that can help you organize your research, collaborate with others online, and discover the latest research».* Disponible en: https://www.elsevier.com/solutions/mendeley (consulta: 6 de abril de 2019).

[1118] *YouTube* pertenece al grupo *Google,* normalmente los usuarios tienen asociada su cuenta de correo electrónica de Gmail (otro servicio de *Google)* para poder tener acceso a esta red social, alberga principalmente vídeos. De acuerdo con BARRIO ANDRÉS, M., la plataforma de YouTube es un «*servicio de intercambio de vídeos musicales más grande que permite a cualquier persona con acceso a Internet registrarse en una cuenta para publicar y compartir contenidos multimedia. Aloja una variedad de vídeos de películas, programas de televisión y vídeos musicales, así como contenidos amateur de los propios usuarios como videblogs y YouTube Gamming*», Cfr. BARRIO ANDRÉS, M. *op. cit*., p. 110.

[1119] *Pericope,* es una red social que puede estar asociada a una cuenta de *Twitter*, la cual nos permite transmitir en directo desde cualquier parte del mundo en formato vídeo, lo que está ocurriendo a nuestro alrededor, desde nuestra vida cotidiana hasta algún hecho noticiable, en el siguiente link se podrá consultar más al respecto sobre esta aplicación y está disponible en la web, *vid.* Verne, El País, Así es Periscope, la app de Twitter para transmitir tu vida en directo. Disponible en: http://verne.elpais.com/verne/2015/03/28/articulo/1427564916_014554.html (consulta: 21 de mayo de 2019).

[1120] AGUSTINOY GUILAYN, A. y MONCLÚS RUIZ, J., *op. cit*., p. 23.

[1121] *Íd.*

encontramos a *Instagram*[1122], *Flickr*[1123], *Snapchat*[1124]; dentro de la categoría de música estaría , *MySpace*[1125] y por último dentro de las más destacables de las redes de eventos se encontraría *Meetup*[1126], este tipo de red social «*se articulan como plataformas para organizar grupos y eventos presenciales referidos a un ámbito de interés específico».*

2.2 Foros, blogs y wikis

Dentro de las TIC también encontramos los foros, los blogs y los *wikis*. Los primeros son páginas *Web*, que permiten el intercambio de opiniones por los usuarios de algún tema en concreto. GALLEGO VÁZQUEZ los define como «*una herramienta de "muchos para muchos" (muchos hablan, muchos contestan). Los participantes están, como decimos, al mismo nivel, y por los general los foros están dedicados a un tema en particular*»[1127]. Sin embargo, los *blogs* son una especie de bitácora donde el usuario puede subir textos, vídeos, imágenes o cualquier tipo de información sobre temas de su interés, experiencias u opiniones que quedan registradas de manera cronológica y donde la entrada más reciente es la que aparece primero. Los ejemplos más populares de este tipo de páginas *Web* son *Blogger* y

---

[1122] Es una red social, en donde se pueden compartir vídeos cortos e imágenes, con la posibilidad de aplicarles filtros fotográficos y/o editar. Las imágenes o vídeos pueden ser compartidos con sus amigos de la propia red social, e incluso tiene la opción de compartirlo vía *Facebook, Twitter, Tumblr, Swarm y Flickr* (otras redes sociales) iniciando previamente sesión en las mismas y permitiendo compartir la imagen en esa otra red social también.

[1123] *Vid.* https://www.flickr.com/about (consulta: 21 de mayo de 2019).

[1124] También es una red social especializada en fotografía, es famosa por la aplicación de sus filtros, los *snaps* o fotografías que han sido enviadas y no abiertas se eliminan dentro de los siguientes 30 días a su envío, en caso de ser enviados a un chat grupal sin abrir se eliminan a las 24 horas, este último plazo se aplica también para la eliminación de las historias publicadas por los usuarios, *vid.* https://support.snapchat.com/es/a/when-are-snaps-chats-deleted (consulta: 21 de mayo de 2019).

[1125] *MySpace* inicio como una red social generalista, sin embargo, actualmente es una red social que gira en torno a la música, *vid.* https://myspace.com/ (consulta: 21 de mayo de 2019). De conformidad con lo establecido por GALLEGO VÁZQUEZ, J. A., esta empresa nació en 2003 y ha sido «*la primera red social verdaderamente global, y la primera que ha generado un debate general sobre la rentabilidad de las redes sociales (…) Fueron las bandas de Indie de Los Ángeles las que empezaron a utilizar de manera masiva MySpace como plataforma de promoción, y detrás de las bandas vineron los fans*», Cfr. GALLEGO VÁZQUEZ, J. A., *Comunidades virtuales y redes sociales* (en línea), Creative Commons Reconocimiento NoComercial CompartirIgual, Madrid, 2012. Disponible en: http://www.comunidadenlared.com/mi-libro-comunidades-virtuales-y-redes-sociales-en-libre-descarga/ (consulta y descarga: 23 de mayo de 2019).

[1126] En esta red social la gente se encuentra con otros incluso en el mundo analógico, se autodefine como «*una plataforma para encontrar y construir comunidades locales. Las personas usan Meetup para conocer gente nueva, aprender cosas, encontrar apoyo, salir de sus zonas de confort y perseguir sus pasiones juntas*», *vid.* https://www.meetup.com/es-ES/about/ (consulta: 21 de mayo de 2019).

[1127] GALLEGO VÁZQUEZ, J. A. *op. cit.*

Wordpress. GALLEGO VÁZQUEZ también nos ofrece una definición acerca de los Blogs, los define como una herramienta que «*se asemeja más bien a un "discurso"o "charla magistral", donde el ponente, al final del mismo, permite a sus oyentes un turno de "preguntasy respuestas". En cualquier caso, el Blogger es el que "controla" la conversación, y el que marca las directrices*»[1128].

También existe el *microblogging,* el cual es una versión mucho más dinámica de los blogs tradicionales, tienen un número restringido de caracteres, se ordenan de manera cronológica (*TimeLine),* y en algunos casos puntuales como *Twitter* también pueden ser estos espacios considerados como una red social debido a sus características. *Twitter* es la plataforma de *microblogging*[1129] con más popularidad, hasta mediados de 2017 la extensión de sus entradas era de 140 caracteres[1130], a partir de septiembre de ese año se amplió el límite a 280 en casi todo el mundo, salvo para los idiomas japones, chino y coreano[1131]. Esta plataforma «creada y diseñada por Evan Williams en el año 2006»[1132], conforme al informe Digital de la empresa *Hootsuite* en 2019 contaba ya con más de 6 millones de usuarios activos mensuales[1133].

De conformidad con BALCELLS, J., PADRÓ-SOLANET, A. y SERRANO, I., «*Twitter*» «*consiste en una plataforma en la que cualquier usuario registrado puede publicar mensajes cortos (como los SMS) que pueden ser leídos por cualquier otro usuario de la plataforma…Los usuarios de Twitter disponen de distintas formas de filtrar la información que les puede interesas, la más importante consiste en "seguir" (follow) a*

[1128] *Íd.*

[1129] De conformidad con DAVARA FERNÁNDEZ DE MARCOS, L. citando a ACED, C. (en nota a pie 83): el *microbogging* «*es blogging a tiempo real y tiene sentido para usuarios que pasan muchas horas conectados a Internet y para aquellos que navegan desde dispositivos móviles. Dada la brevedad de los mensajes, que recuerda a los SMS del móvil, es habitual compartir enlaces y apuntar ideas que muchas veces se complementan con otras plataformas 2.0 como los blogs*», Cfr. DAVARA FERNÁNDEZ DE MARCOS, L., *op. cit.,* p. 62.

[1130] Por el fallo de la Sentencia 235/2014 del Juzgado de Primera Instancia de Sevilla (AC\2014\1875; ECLI:ES:JPI:2014:154), se ordena efecto «*a publicar el fallo de la sentencia a través de la cuenta de Twitter del demandado mediante la Transcripción del fallo en un Tweet usando una herramienta creada al efecto para aumentar el número de caracteres permitidos, publicándolo durante treinta días».*

[1131] Cfr. Twitter, *Giving you more characters to express yourself* (en línea). Jueves 26 de septiembre de 2017. Disponible en: https://blog.twitter.com/official/en_us/topics/product/2017/Giving-you-more-characters-to-express-yourself.html (consulta: 19 de octubre de 2020).

[1132] DAVARA FERNÁNDEZ DE MARCOS, L., *op. cit.*, p. 64.

[1133] Cfr. https://hootsuite.com/pages/digital-in-2019#accordion-115547 (consulta: 27 de mayo de 2019).

otros usuarios. De este modo, los menajes de estos usuarios "seguidos" (followed) aparecen en nuestra "línea del tiempo" (Time Line)…la relación entre seguidores y seguidos, da cuenta primariamente de Twitter como una red social» [1134], este elemento de red social se hace manifiesto con la respuesta de manera directa a los Tweets de otros usuarios, o marcar un mensaje que consideramos importante con un retweet o un «me gusta» haciendo clic en el corazón. Por su parte DAVARA FERNÁNDEZ DE MARCOS, L., considera que todas estas características hacen de Twitter «una red social de *Microblogging*» [1135], quizás dentro de las herramientas utilizadas por esta plataforma la de mayor popularidad sea el Hashtag, este se forma con el signo de almohadilla [1136] y que de acuerdo con la Fundación del Español Urgente (Fundéu) «es una palabra, frase o grupo de caracteres alfanuméricos que se emplea en las redes sociales para agrupar varios mensajes sobre un mismo tema, se identifica fácilmente, ya que está compuesto por el símbolo # (hash) y un nombre o etiqueta (tag)» [1137]. Los *hastag* entonces sirven para clasificar información por palabras o frases en relación con el contenido de la publicación, además están estrechamente ligados con la folksonomía, un término acuñado por Thomas Vander Wal [1138] «*proviene del inglés folksonomy, derivado de folk (en inglés, popular) + taxonomía, que procede a su vez de los términos griegos taxis (clasificación) + nomos (ordenar gestionar); y se emplea para designar a un sistema de etiquetado o clasificación de objetos web no jerárquico que nace de forma natural y democrática de*

[1134] BALCELLS, J., PADRÓ-SOLANET, A. y SERRANO, I., «La adopción y gestión de redes sociales en los ayuntamientos catalanes», CRIADO, I. (Editor), *Nuevas tendencias en la gestión pública. Innovación abierta, gobernanza inteligente y tecnologías sociales en unas administraciones públicas colaborativas.* Ed. Instituto Nacional de Administración Pública, Madrid, 2016, p. 173.
[1135] DAVARA FERNÁNDEZ DE MARCOS, L., *op. cit*., p. 62.
[1136] En comandos informáticos para su formación son utilizados de manera simultánea alt y 35.
[1137] Cfr. https://www.fundeu.es/recomendacion/etiqueta-mejor-que-hashtag-958/ (consulta: 27 de mayo de 2019).
[1138] De acuerdo con el autor la «*folksonomía*» es el resultado del etiquetado de información para su propia recuperación, también se utiliza para el equitetado en un entoro social y este acto lo realiza una persona consumidora de información, (trad. *result of personal free tagging od information and objects for one´s own retrieval. Tagging in a social environment (shared and open). Act of tagging is done by the person consuming the information,* Cfr. VANDER WAL, T., «Folksonomy, presented: online information», London, 30 December 2005 (en línea), p. 3. Disponible en: http://vanderwal.net/essays/051130/folksonomy.pdf (consulta: 1 de diciembre de 2020).

los propios internautas –que son quienes asignan las etiquetas espontáneamente- y de cuya gestión se encarga un sistema automático»[1139].

Por su parte los sitios Wikis es una tecnología propia de la web 2.0 que «*permite la fácil creación, edición vinculación mediante links y rastreo de cambio de una o varias páginas web por un grupo de usuarios mediante su navegador de Internet. La función de la wiki es soportar tecnológicamente la creación por varios usuarios de hiper-documentos y administrar procesos basados en conocimiento, a través de un simple navegador de internet. En otras palabras, servir de medio para la creación y gestión de información en forma colaborativa*»[1140] . La modificación del contenido de la página web, es decir, la información puede ser modificada por cualquier usuario tenga o no tenga una cuenta de usuario en la página web[1141], en este último caso el usuario web no identificado podrá llevar a cabo los cambios pero bajo advertencia de que en caso de grabar cambios de este modo, la dirección IP de esa persona «quedará registrada públicamente en el historial de la página». Técnicamente funciona de la siguiente manera: «*el "editor" en la wiki es el ambiente de texto del navegador del usuario. Mediante el uso del protocolo para solicitar leer contenido (get) y el protocolo para escribir texto (post), el usuario requiere la página actual, la cual le es enviada (en texto fuente), posteriormente por él editada y una vez guardados los cambios, es remitida de vuela al servidor, el cual remplaza el contenido antiguo de la página por el nuevo en la base de datos*»[1142].

[1139] DÍAZ PIRAQUIVE, F. N., JOYANES AGUILAR, L. y MEDINA GARCÍA, V. H., «Taxonomía, ontología y folksonomía, ¿qué son y qué beneficios u oportunidades presentan para los usuarios de la web» (en línea), *Universidad & Empresa*, núm. 16, vol. 11, 2009, p. 253. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5096735.pdf (consulta y descarga: 27 de mayo de 2019).

[1140] SERENO RESTREPO, J. S., «Contenido generado por usuarios (ugc), Wikies, y derecho de autor» (en línea), *Revista La Propiedad Inmaterial,* Universidad Externado de Colombia, noviembre 2010, p. 210. Disponible en: https://revistas.uexternado.edu.co/index.php/propin/article/view/2480 (consulta: 28 de mayo de 2019).

[1141] Formulario para creación de cuentas en Wikipedia *vid.* https://es.wikipedia.org/w/index.php?title=Especial:Crear_una_cuenta&returnto=Discusi%C3%B3n%3ARevoluci%C3%B3n+Industrial&returntoquery=action%3Dedit%26section%3D1 (consulta: 28 de mayo de 2019).

[1142]Trad. del inglés: *«"the editor" for a wiki is a very primitive affair-it is your Web browser's text-in-a-form environment. Using the server protocol get (request to read content) and post (request to write content), you receive the current page (the source text) in a form, make your edits, and submit the changed page back to the server. The server then replaces the page content in the database*» de BO LEUF, WARD CUNNINGHAM por SERENO RESTREPO, J. S., *op. cit.,* p. 212.

En las wikis intervienen dos partes, por un lado se encuentra el administrador, que realmente es el software que se pone a disposición de los usuarios para que puedan editar el contenido de la información que se aloja en la página web por medio del navegador y los usuarios quienes colaborativamente tienen la posibilidad de modificar lo que ya está escrito, también pueden crear nuevos artículos, insertar enlaces interno o externos, traducir de otros idiomas los existentes, compartir fotos y realizar comentarios[1143]. El ejemplo más famoso de este tipo de sitios *Web* es *Wikipedia,* la cual es una «*enciclopedia en línea donde los usuarios contribuyen escribiendo artículos, definiciones, etc. Es completamente editada y mantenida por los usuarios»*[1144]*,* otros sitios como *Wikiquote, Wikilibros y Wikidiccionarios,* etc., integran este tipo de sitios *Web*.

2.3 Motores de búsqueda

En el espacio Web existe un servicio denominado buscadores o motores de búsqueda, estos son *«servicios que ayudan a los usuarios a encontrar información en Internet. Pueden diferenciarse según el tipo de datos que recaban, incluyendo imágenes y/o vídeos, y/o sonido, o distinto tipo de formatos… los buscadores se han definido como un tipo de servicio de la sociedad de la información, a saber, herramientas de localización de información»* [1145] , indexan las palabras que suministramos en dicho buscador por medio de *robots* o arañas informáticas, lo cual les permite mostrarnos una lista o índice de resultados de las páginas *Web* que contienen la información que buscamos, el usuario visualiza un extracto del contenido de la página web donde alberga la información y un enlace que si es pinchado nos redirige al sitio web donde está lo que buscamos, es decir, «*no crea nuevo contenido autónomo. En su forma más simple, únicamente indica dónde pueden*

[1143] Cfr. https://es.wikipedia.org/wiki/Ayuda:C%C3%B3mo_puedes_colaborar (consulta: 28 de mayo de 2019).
[1144] Trad. del inglés de NAIK, U. and SHIVALINGAIAH, D., *op. cit.*
[1145] Trad. del inglés: «*are services that help their users to find information on the Web. They can be distinguished according to the different types of data they aim to retrieve, including pictures and/or videos and/or sound or different kinds of formats. A new área of devolopment is search engines that are specifically aimed at building profiles of people bases on personal data found anywhere on the* Internet», Opinion 1/2008 on data protection issues related to search engines, adopted on 4 April 2008, of Data Protection Working Party (00737/EN WP148) (en línea), 5. Disponible en: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf

encontrarse contenidos ya existentes, puestos a disposición en Internet por terceros, proporcionando un hipervínculo a la página web que contiene los términos buscados»[1146]. Normalmente los motores de búsqueda utilizan herramientas como direcciones IP [1147], *Server logs* [1148] y *cookies* [1149] para tratar la información y almacenarla.

2.4 Las cookies

Dentro de la web hay destacadas herramientas que hacen más fácil nuestra navegación, sin embargo, pese a los más de 40 años de su creación los usuarios de esta red mundial aun no son totalmente conscientes de los potenciales riesgos que supone su uso. Dentro de estas herramientas encontramos a las *cookies,* las cuales son archivos de almacenamiento de datos relativos a nuestra navegación y actividad en la *web* que se descargan desde nuestros navegadores*. MENÉNDEZ, L.* las define como *«archivos que se descargan, en ordenadores, teléfonos móviles o en tabletas para acceder a determinadas páginas web, y permiten entre otras cosas almacenar y recuperar información sobre los hábitos de navegación de un usuario o de su equipo (…) a través de ellas pueden almacenarse los datos del usuario y contraseña para acceder a diferentes servicios sin tener que escribirlos en cada nuevo acceso. También permiten que las páginas web ofrezcan información de acuerdo a los intereses de cada uno, o introducir mejoras en la navegación»* [1150]. La AEPD las ha definido como archivos que «*permiten el almacenamiento en el terminal del usuario de cantidades*

[1146] Apartado 32 de las Conclusiones del Abogado General Sr. Niilo Jääskinen presentadas el 25 de junio de 2013, en el asunto C-131/12, *Google Spain*, S.L., Google Inc. Contra Agencia Española de Protección de datos (AEPD) y Mario Costeja González (ECLI:EU:C:2013:424).

[1147] *Vid.* p.8.

[1148] Los denominados *Server logs*, según la Agencia Española de Protección de Datos, son *«Unos ficheros que contienen información del usuario tales como los parámetros de búsqueda, la dirección IP asignada al ordenador del usuario, la fecha y la hora de la búsqueda y el identificador de la cookie, así como las preferencias del usuario, las características del navegador, el resultado de la búsqueda, la publicidad que se ha mostrado al resultado de una búsqueda específica y los clicks del usuario»* (En AEPD, «*Declaración sobre buscadores de Internet*», 2007, p. 2). Debido a los *Server logs,* los buscadores son responsables del tratamiento de estos, de conformidad con la normativa comunitaria.

[1149] Específicamente, las que usan el motor de búsqueda son las *cookies red*, las *cookies* permanentes y las *cookies flash*, estas últimas son aquellas con las que cuentan algunas empresas de motores de búsqueda se utilizan por ejemplo como copia de seguridad de las cookies normales o para almacenar información detallada sobre las búsquedas efectuadas por los usuarios.

[1150] MENÉNDEZ, L, «¿Qué son las cookies?», *Escritura Pública* (en línea), núm. 82, julio-agosto 2013, p.16. Disponible en:http://www.notariado.org/liferay/c/document_library/get_file?folderId=12092&name=DLFE-110181.pdf (consulta: octubre de 2016).

de datos que van de unos pocos kilobytes a varios megabytes»[1151]. Sin embargo, no se utiliza siempre la misma terminología cuando se habla de este tipo de tecnología, por ejemplo, PÉREZ BES les da un tratamiento de ficheros[1152] y para GARCÍA-ULL son dispositivos de almacenamiento[1153].

En lo personal, me parece más acertado el término de archivos, pues tal y como señala APARICIO SALOM[1154], es el formato utilizado para la descarga de esta tecnología, precisamente es en ese momento cuando son creados por y para las *cookies* ficheros donde se albergan. Respecto al término «dispositivo de almacenamiento», decir, que normalmente lo relacionamos a un dispositivo físico de almacenamiento como un *pen drive* o una memoria externa, sin embargo, aunque las *cookies* no sean dispositivos tangibles, sí que almacenan información.

Hay varios elementos que son intrínsecos de las «*cookies»* como equipo terminal, navegador *web*, página *web* y datos de navegación, sin ellos es inconcebible tener una idea de lo que son y para qué funcionan. Para tener acceso a *Internet* se necesita un *router*[1155] que permita el acceso a Internet y un equipo terminal, es decir, un ordenador, una tableta o un teléfono inteligente (dónde se descarga la

[1151] AEPD, «*Guía sobre el uso de las cookies*», 2020 p.7. Disponible en: https:// https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdfwww.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (consulta: 29 de julio de 2020).

[1152] Para este autor, «*Las cookies (también conocidas como "chivatos") son unos pequeños ficheros de texto alfanumérico que son almacenados en el disco duro del visitante de una página web a través del navegador», vid.* PÉREZ BES, F., *La publicidad comportamental online,* Ed. UOC, Barcelona, 2012, p. 22.

[1153] GARCÍA ULL, las define como «*dispositivos de almacenamiento y recuperación de datos que se descargan en el equipo terminal de un usuario con la finalidad de almacenar datos que podrán ser actualizados y recuperados por la entidad responsable de su instalación»* en GARCÍA-ULL, F. J., «Las *cookies* en los principales cibermedios generalistas de España» (en línea), *Miguel Hernández Communication Journal*, nº4, artículo nº 11, 2013, p. 236. Disponible en: http://rev.innovacionumh.es/index.php?journal=mhcj&page=article&op=view&path%5B%5D=52&path%5B%5D=102 (consulta: 31 de octubre de 2017).

[1154] Según APARICIO SALOM, las cookies deben ser consideradas como «*archivos que se instalan en el equipo del usuario al descargar un contenido web para su visualización y se mantienen operativas durante cierto tiempo, que puede estar limitado al de permanencia del usuario en el sitio web que instaló la cookie, o subsistir aunque se cierre el navegador*», Cfr. APARICIO SALOM, J., «El régimen jurídico de las *cookies* y su aplicación por la agencia española de protección de datos», *Revista Aranzadi Doctrinal,* núm. 11/2014, parte estudio, p. 1 (descarga y consulta: 3 de octubre de 2017).

[1155] De conformidad con el Diccionario de la lengua española es un «*Dispositivo físico que permite la conexión de una red con otra, encaminando la información hacia la red a la que va destinada y proporcionando conectividad*», cfr. https://dej.rae.es/lema/router (consulta: 4 de junio de 2019).

cookie) que cuente con algún navegador *web*[1156] debido a que «*sirven de unión entre el internauta y la información obviando y haciendo transparente todo ese conglomerado de siglas, protocolos y normas*» [1157], entre los más populares encontramos a *Internet Explorer* (ahora *Microsoft Edge), Google Chrome, Safari, Opera, Mozilla Firefox;* ahora bien; dentro de nuestro navegador en la barra de navegación se puede bien introducir la dirección web que queremos visitar (*Uniform Resource Locator o URL*) o utilizar un motor de búsqueda como *Google*, para encontrar lo que deseamos en la *web*. Las *cookies* se descargan en nuestro equipo terminal cuando visitamos una página *web,* normalmente están asociadas a la publicidad que parece en propio sitio web, la información que almacena son datos relacionados con nuestras preferencias y navegación.

Existen varios sujetos que pueden llegar a intervenir en el uso de este tipo de tecnología: 1) El usuario: es el destinario de las *cookies*, quienes las almacenan en sus equipos terminales; 2) El anunciante es «*la entidad cuyos productos, servicios o imagen se publicitan a través de los espacios publicitarios de los que disponen, en su caso, los editores en sus páginas u otras aplicaciones desde las que prestan los servicios a los usuarios. En este sentido, actúa como demandante de espacios publicitarios*» [1158]. Los anunciantes son los principales demandantes de espacios publicitarios en la web; 3*)* El editor es «*cualquier entidad prestadora de servicios de la sociedad de la información titular de una página web a los que puede acceder un usuario y para cuya prestación se utilizan cookies*» [1159].

Entre estos tres actores principales fungen como intermediarios entidades o aplicaciones que permiten la instalación de cookies: 1) la plataforma de gestión del consentimiento, la cual es «*una herramienta que instala en el soporte del editor, página web o aplicación, y permite que cualquier responsable de la utilización de cookies cumpla sus deberes de información y recogida de consentimiento*», 2) las

[1156] Son considerados «*programas que interpretan los códigos incrustados en los documentos HTML (o páginas web), y muestran los documentos de forma gráfica*», trad. del inglés «*These programs interpret the codes embedded in the HTML documents (or web pages), and display the documents graphically*», Cfr. HENDRIX, P. y BIRKMIRE, M., *Adapting Web Browsers for Accessibility* (en línea), p. 27 y ss. Disponible en: http://files.eric.ed.gov/fulltext/ED432102.pdf (consulta: 4 de junio de 2019).
[1157] *Íd.*
[1158] AEPD, «*Guía sobre el uso de las cookies*», p. 35.
[1159] *Ib.,* p.34.

agencias de publicidad como principales intermediarios[1160]: «*son entidades que se encargan del diseño y ejecución de la publicidad, así como de la creación, preparación o programación de las campañas publicitarias de los anunciantes, actuando en nombre y por cuenta de estos en la contratación de espacios publicitarios*»[1161], junto a los anunciantes también son considerados como demandantes de espacios publicitarios en la web, en la actualidad a estas personas que planean la estrategia de publicidad se les denomina también «*Community Manager*» , en cambio, si es una empresa la que gestiona esta labor se le denomina «Agencia social media», una de las agencias de este tipo más populares en España es «La despensa», encargada de algunas de las principales campañas publicitarias de empresas como *Burger King, Adidas*, Antena 3 y *Coca-Cola*[1162]*;* 3) Redes publicitarias: «*son un conjunto de entidades que, actuando en nombre y representación directa o indirectamente de uno o varios editores, ofrecen, también directamente a los anunciantes o, indirectamente a través otros demandantes, como las Agencias de publicidad, la posibilidad de obtener espacios publicitarios o algún tipo de resultado concreto como clicks, ventas o registros, a través de la gestión y tratamiento de los datos obtenidos de la utilización de las cookies descargadas o almacenadas en los equipos terminales de los usuarios, cuando estos acceden a los servicios prestados por el editor*»[1163], son conocidas también por su nombre en inglés *Adversting networks,* quizás la red publicitaria más conocida a nivel mundial sea *AdSense* de la empresa *Google Inc*[1164]; y 4) un *Trading desk,* compuesto por un «equipo técnico de personas dentro (o fuera, puede ser independiente) de una agencia de medios que a través de la conexión con múltiples DSP (tecnología de puja que permite a anunciantes y/o agencias de medios comprar inventario en diferentes *ad exchanges* —lugares donde se unen oferta y demanda—), optimizan la compra programática de los anunciantes».

[1160] Existen otros intermediarios en el uso y la instalación de cookies. Las plataformas de gestión de consentimiento o *consent magement platform «es una herramienta que instala en el soporte del editor, página web o aplicación, y permite que cualquier responsable de la utilización de cookies cumpla sus deberes de información y recogida de consentimiento»*,

[1161] *Íd.*

[1162] Cfr. https://marketing4ecommerce.net/agencias-social-media-de-espana-2019/ (consulta: 5 de junio de 2019).

[1163] *Ib.,* p. 35.

[1164] *Vid.* https://www.google.com/intl/es_es/adsense/start/how-it-works/#/ (consulta: 5 de mayo de 2019).

Otro actor que puede intervenir en la compra de espacios publicitarios relacionados con el uso de cookies son «las empresas de análisis y medición», las cuales de encargan de medir y/o analizar «*el comportamiento de la navegación de los usuarios en la página web del editor, actuando en su nombre y representación, a través del análisis de datos obtenidos con la utilización de cookies con la finalidad de mejorar el servicio que presta el editor*»[1165], por ejemplo *Google Analytics*[1166].

Aclarados los conceptos será más fácil identificar quienes se encargan de introducir este tipo de tecnología en nuestros equipos terminales, así como conocer el tipo de *cookies* albergada en los mismos. Las cookies se pueden clasificar según su origen (o gestión), su duración y su funcionalidad, «no obstante es necesario tener en cuenta que una misma cookie puede estar incluida en más de una categoría»[1167]:

2.4.1 Según su origen: cookies propias y cookies de terceros.

Para que la publicidad aparezca en una página de web, el editor debe haber reservado un espacio publicitario dentro de la página para su visualización, estos pueden gestionar la publicidad que se visualiza o bien contar con la ayuda de un tercero, que normalmente son las agencias de publicidad o redes de publicidad. En el primer supuesto, el editor de la página de internet puede contratar directamente con el anunciante sobre los espacios ofertados por el mismo[1168], en este caso, si el editor insertase publicidad en alguno de sus espacios reservados para la misma y haga uso de algún tipo de *cookie* para su funcionamiento, estas deberán ser consideradas como *cookies* de origen, ya es el editor es quien directamente las gestiona desde su dominio.

El Grupo de Trabajo del artículo 29 (GT29), ha definido como cookies de origen, a aquellas creadas «por el responsable del tratamiento de datos (o uno de sus procesadores) que opere el sitio web visitado por el usuario, tal como se define

[1165] AEPD, «*Guía sobre el uso de las cookies*», p. 37.
[1166] *Vid.* https://marketingplatform.google.com/about/analytics/?hl=es (consulta: 5 de mayo de 2019).
[1167] AEPD, «*Guía sobre el uso de las cookies*», p. 11.
[1168] La AEPD, los ha definido como «*la entidad cuyos productos, servicios o imagen se publicitan a través de los espacios publicitarios de los que disponen, en su caso, los editores en sus páginas u otras aplicaciones desde las que prestan los servicios a los usuarios. En este sentido, actúa como demandante de espacios publicitarios*», *vid.* AEPD, *ib.,* p. 35.

en la dirección URL que suele aparecer en la barra de direcciones del navegador»[1169], por su parte la AEPD las denominan como cookies propias, ya que «se envían al equipo terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el que se presta el servicio solicitado por el usuario» [1170].

Las *cookies* también pueden ser introducidas directamente en páginas como motores de búsqueda, si estas son gestionadas por el editor se considerarán de origen, estas «contienen *generalmente información relativa al sistema operativo y al navegador del usuario, así como al número de identificación único para cada cuenta de usuario…permiten identificar al usuario con más exactitud que la dirección IP. Por ejemplo, si el ordenador es compartido por varios usuarios que disponen de cuentas distintas, cada usuario tiene su propia cookie que lo define de manera única como usuario del ordenador»*[1171].

El concepto de «*cookies* de terceros» solía traer cierta confusión por lo establecido tanto en 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 ya la libre circulación de estos datos, la cual establecía en su art. 2. f) que se consideraba a tercero a «*la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento*», es decir que las *cookies* de terceros eran aquellas que creaban e introducían aquellas personas que no administran el sitio web que aparece en la barra de direcciones donde aparece el URL. La confusión se puede derivar por el manejo de conceptos, la URL no es lo mismo que el dominio, el primero de ellos como se describió en páginas anteriores se utiliza para localizar los recursos en la web, sin embargo, un nombre de dominio sirve para identificar al responsable, es decir, quien administra la página web, es por ello que el Grupo de Trabajo del Artículo 29 (*Article 29 Working Party* –WP29-), determinó que son consideradas como *cookies* de terceros aquellas que son creadas «*por responsables*

[1169]GT 29, Dictamen de 7 de junio de 2012, p. 5.
[1170] AEPD, «*Guía sobre el uso de las cookies*», p. 11.
[1171] GT29, Opinion 1/2008(…) *op. cit..,* p. 7.

de tratamiento que no operen el sitio web visitado por el usuario»[1172]. Por su parte la Agencia Española de Protección de Datos, y teniendo en cuenta la confusión que puede dar a lugar el uso de la terminología adecuada concreta que este tipo de *cookies* «*son aquellas que se envían al equipo terminal del usuario desde un equipo o dominio gestionado por el propio editor y desde el que se presta el servicio solicitado por el usuario*»[1173].

En el segundo supuesto, si estas no son introducidas por el editor de la página es decir quien gestiona y administra el dominio serán consideradas como «*cookies* de terceros». La AEPD, las ha definido como «*aquéllas que se envían al equipo terminal del usuario desde un equipo o dominio que no es gestionado por el editor, sino por otra entidad que trata los datos obtenidos través de las cookies*»[1174].

2.4.2 Según su duración

Las *cookies* también pueden ser clasificadas según el tiempo que estas permanezcan en el equipo terminal de los usuarios, pudiendo ser de sesión o persistentes. Las *cookies* de sesión son aquellas que están «*diseñadas para recabar y almacenar datos mientras el usuario accede a una página web*»[1175], por lo que se eliminan «*automáticamente cuando el usuario cierra el navegador*»[1176]. Es decir, estas almacenaran información respecto a nuestra navegación durante el tiempo que tengamos abierta esa página de internet en nuestro navegador, en cuanto este sea cerrado por el usuario, de manera automática se eliminaran, en caso de que se vuelva abrir el navegador y se visite el mismo sitio, se descargara una nueva *cookie* durante esa sesión, por lo que aunque se haya visitado muchas veces esa página web cada vez que entre y salga será considerado como un nuevo visitante, lo cual supone que no se almacenarán datos de manera posterior al cierre de la página web. GARCÍA-ULL, las define como aquellas que tienen «*una duración temporal, y se eliminan al cerrar el navegador, una vez finalizada la navegación. La próxima vez que se visita el sitio web, el usuario no es reconocido y tiene el tratamiento de un nuevo usuario, ya*

[1172] GT29, Dictamen 4/2012 sobre la exención del requisito de consentimiento de *cookies*, adoptado el 7 de junio de 2012 (00879/12/ES), p. 5.
[1173] AEPD, «*Guía sobre el uso de las cookies*», p. 11.
[1174] *Íd.*
[1175] *Ib.*, p. 13.
[1176]GT 29, Dictamen de 7 de junio de 2012, p. 4

que no existe ningún archivo en el navegador que permita saber a la web si el usuario ha visitado el portal anteriormente»[1177].

Las cookies permanentes por su parte «mejoran la calidad del servicio, almacenando las preferencias de los usuarios y registrando su prácticas, como la manera en que efectúan las búsquedas»[1178], de forma contraria a las de sesión, son aquellas que no se extinguen con el cierre del navegador, estás cookies permanecen en el equipo terminal de los usuarios por el tiempo que hayan sido programadas, y durante ese tiempo, almacenaran información sobre la navegación, pueden «autentificar la cuenta del usuario, de forma que no tenga que introducir sus datos cada vez que visita la web, así como diversas opciones de personalización de interfaz, como selección de lenguaje, preferencias de menú, etc.»[1179]. De conformidad con el GT 29, la duración de este tipo de cookies «pueden ser minutos, días o años»[1180].

2.4.3 Según su funcionalidad

En esta categoría, se encuadran las *cookies* que han sido diseñadas para cumplir una función específica en la navegación de los usuarios, debido a la gran cantidad y tipos existentes solo haremos mención a las que consideramos las más importantes.

Las cookies técnicas «*son aquéllas que permiten al usuario la navegación a través de una página web, plataforma o aplicación y la utilización de las diferentes opciones o servicios que en ella existan*»[1181], estas cookies, puede que sean las más necesarias en nuestra navegación, ya que su finalidad es proveer de un mejor servicio a los usuarios dentro de la página web, resultan necesarias para mejorar nuestra experiencia en la web.

Las cookies de análisis «son aquéllas que permiten al responsable de las mismas el seguimiento y análisis del comportamiento de los usuarios de los sitios web a los que están vinculadas, incluida la cuantificación de los impactos de los

[1177] GARCÍA-ULL, F. J., *op. cit.,* p. 240.
[1178] *Íd.*
[1179] *Íd.*
[1180] GT 29, Dictamen de 7 de junio de 2012, p. 4.
[1181] AEPD, «*Guía sobre el uso de las cookies*», p. 11.

anuncios»[1182]. Estas también, pueden ser denominadas como cookies de rastreo, si están gestionadas por una red de publicidad[1183]. Dentro de las cookies de rastreo hay una modalidad que incluso permite rastrear las búsquedas de los usuarios[1184].

Las *cookies* de publicidad, como bien describe su nombre son aquellas que tienen como finalidad la gestión de los espacios publicitarios[1185] en «*base a criterios como el contenido editado o la frecuencia en la que se muestran los anuncios*»[1186]. Dentro de esta categoría encontramos a las cookies de publicidad comportamental, las cuales tienen la función, también de gestionar los espacios publicitarios, pero se diferencian de las anteriores debido a que estas «*almacenan información del comportamiento de los usuarios obtenida a través de la observación continuada de sus hábitos de navegación, lo que permite desarrollar un perfil específico para mostrar publicidad en función del mismo*»[1187].

Las *flash cookies*, estas están diseñadas para que sean prácticamente imborrables de nuestro equipo terminal pues «*no pueden borrarse con la configuración tradicional de privacidad de un buscador»*[1188], tienen la función de restaurar las *cookies* que han sido borradas del equipo terminal, son consideradas como «*nuevas tecnologías reforzadas de rastreo»*[1189]*,* pues como indica el GT29, estas se utilizan *«como copia se seguridad de las cookies normales (…) o para almacenar información detallada sobre las búsquedas efectuadas por los usuarios»*[1190]*.*

El art. 4.4 del Reglamento 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

---

[1182] *Ib.,* p. 12.
[1183] También denominadas «*Tracking cookies*», estas según PÉREZ BÉS, son aquellas que «*permiten rastrear la navegación y el comportamiento de un usuario en todas aquellas páginas web en las que se muestre publicidad lanzada desde una misma red publicitaria. En este tipo de cookies, esta opción es posible gracias a las tecnologías de hipertexto que permite el protocolo HTML»,* PÉREZ BES, F., *op. cit*., p. 23.
[1184] De conformidad con lo establecido por el GT 29, estas cookies «*dan la posibilidad de rastrear las búsquedas del usuario a lo largo de un lapso extenso de tiempo y teóricamente en dominios diferentes»,* en GT 29, Dictamen de 22 de junio 2010, p. 6.
[1185] Tal y como lo establece la AEPD, «*Guía sobre el uso de las cookies*», p. 36.
[1186] GARCÍA-ULL, F. J., *op. cit*., p. 241.
[1187] AEPD, «*Guía sobre el uso de las cookies*», p. 12.
[1188]GT 29, Dictamen de 22 de junio 2010, p. 7.
[1189]*Íd.*
[1190] *Ib.,* p. 8.

por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), establece que se entiende como elaboración de perfiles «*a 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*», como pueden llegar a ser las cookies de este tipo, sin embargo, como se verá más adelante las cookies por sí solas no tratan datos de carácter personal, sin embargo, su uso puede afectar la intimidad de los usuarios de internet[1191].

2.5 Servicios de transmisión de archivos.

Aunque convencionalmente el envío de archivos se realiza a través del servicio de correo electrónico, actualmente existe un servicio que simplifica su envío. Los servicios de transmisión de archivos, como su nombre indica permite la transmisión de archivos, principalmente de gran tamaño y en cualquiera de sus

[1191] Como complemento al articulado del RGPD, actualmente se está tramitando mediante procedimiento ordinario la Propuesta de Reglamento del Parlamento Europeo y del Consejo, sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas) COM/2017/010 final-2017/03 (COD), su art. 8 «*restringe el uso de capacidades de tratamiento, almacenamiento y la recopilación de información de los equipos terminales, como pueden ser las cookie. De hecho, se mantienen dos de los supuestos que establecía la normativa anterior, como la de autorizar cookies solo cuando sean estrictamente necesarias y tengan como fin exclusivo "efectuar la transmisión de una comunicación electrónica a través de una red de comunicaciones electrónicas", o bien lo sean en "la prestación de un servicio de la sociedad de la información solicitado por el usuario final". Sin embargo, se añaden dos supuestos más: el primero es que se cuente con el consentimiento del usuario final y el segundo, "cuando sean necesarios para medir la audiencia en la Web, siempre que esa medición corra a cargo del proveedor del servicio de la sociedad de la información solicitado por el usuario final". Por lo que se refiere al consentimiento, la Propuesta de RPCE establece que, mientras sea técnicamente posible, este podrá ser efectuado mediante "la configuración técnica adecuada de una aplicación informática que permita acceder a Internet", es decir, los navegadores y aplicaciones son los coadyuvantes en hacer cumplir esta nueva normativa en pro de un consentimiento informado. Esta medida es desarrollada por el art. 10 de la Propuesta, por lo que podrá llevarse a cabo bien cuando se instale el navegador o aplicación que permita el acceso a la Web, o bien cuando alguno de los dos se actualice. La información que se dará a los usuarios consistirá en hacerles saber cuáles son las opciones con las que cuentan en relación con la confidencialidad. De esta manera, se cumplirá con los parámetros establecidos en los arts. 4.11 y 7 del RGPD, evitando así la instalación de cookies de terceros. Esta medida sustituye al mecanismo anterior, el cual consistía en el anuncio de las políticas de cookies, colocado en las páginas Web, en dónde se informaba al usuario final la utilización de cookies propias y de terceros, y aceptando su instalación por medio de un consentimiento tácito, en caso de que el usuario final continuara navegando en la página Web. Por último, es conveniente mencionar que esta medida, en cuanto a su diseño, es acorde totalmente con el contenido del art. 25 del RGPD»,* el cual prevé la protección de datos desde el diseño y por defecto., *vid.* GONZÁLEZ MENDOZA, D. P., *op. cit.*, p. 78-79.

formatos a uno o varios destinatarios. El envío se puede realizar normalmente de dos formas y dependiendo del proveedor del servicio, por un lado, se debe seleccionar y cargar el archivo a enviar, posteriormente se debe introducir el o los destinatarios mediante sus respectivos correos electrónicos e indicar el nuestro, así como el asunto y en su caso un mensaje opcional. La segunda de las formas es la transmisión del archivo por medio de un enlace web que se envía normalmente al remitente del archivo, pudiendo personalizar el nombre de la transferencia del mismo, así como el enlace, posteriormente se envía el archivo a la cuenta de correo electrónico y si este es clicado se remite a una página web donde se puede descargar el archivo, esta modalidad permite que el enlace sea introducido en una página web o en una red social. Los proveedores de este tipo de servicios más conocidos son: *WeTransfer*[1192], *Transfernow*[1193], *sendthisfile*[1194], *box*[1195], *Adobe document Cloud*[1196], sin perjuicio de la existencia de otros[1197].

2.6 Mensajería instantánea.

La mensajería instantánea o también conocida como *instant messaging,* es otro servicio emergente al que se puede acceder principalmente mediante un dispositivo móvil, aunque también ofrezca versiones web o aplicaciones para ordenadores. De conformidad con la Fundación del español urgente, la mensajería instantánea es «*un sistema de comunicación mediante el intercambio de mensajes que el destinatario recibe al momento en la pantalla de su ordenador o dispositivo móvil y*

[1192] *WeTransfer* fue fundada en 2009, dentro de esta plataforma se pueden transferir archivos de cualquier tipo con una capacidad de 2 GB, *vid.* https://wetransfer.com/about (consulta: 6 d junio de 2019).
[1193] *TransferNow* fue fundada en el año 2013, se autodescribe como «un servicio para compartir y enviar archivos grandes desde el punto A al punto B», la capacidad de envío de archivos es de 20GB y sus valores corporativos son gratitud, desempeño innovación, transparencia y confidencialidad de los datos, cfr. https://www.transfernow.net/es/acerca (consulta: 6 de junio de 2019).
[1194] *Vid.* https://www.sendthisfile.com/features/how-does-it-work/index.jsp (consulta: 6 de junio de 2019).
[1195] *Vid.* https://www.box.com/es-es/file-transfer (consulta: 6 de junio de 2019).
[1196] *Vid.* https://acrobat.adobe.com/es/es/acrobat/how-to/share-pdf-online.html (consulta: 6 de junio de 2019).
[1197] Como *Leaplife:* https://www.leaplife.com/; *MediaFire:* https://www.mediafire.com/; *Senduit:* http://www.senduit.com/, etc.

que se muestran en una pantalla emergente o se indican con alguna señal sonora, de manera que pueden contestarse inmediatamente, y así establecer un chat»[1198].

Este servicio está asociado a número de móvil del usuario, para poder tener acceso a este servicio es imprescindible que el usuario tenga instalada la aplicación en su terminal móvil. La finalidad principal de este servicio es el intercambio instantáneo de mensajes entre usuarios, específicamente a los que aparezcan en la lista de contactos del remitente, aunque también se pueden realizar otras acciones como el envío de archivos multimedia, mensajes de voz, realizar llamadas y video llamadas[1199] con uno o varios destinatarios. Las aplicaciones más populares de mensajería instantánea actualmente son *Whatsapp, Telegram, Line, Viber, Signal, WeChat.*

2.7 La computación en la nube.

Este servicio de conformidad con el *National Institute od Standards and Technology, la computación en la nube «es un modelo para habilitar el acceso a internet en todas partes, conveniente y bajo demanda sobre un conjunto compartido de recursos informáticos (ej.: redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente accedidos con un mínimo esfuerzo de gestión o intervención del proveedor del servicio»*[1200]. CORONA HERRERO, J. U., establece que *«comprende un nuevo modelo de prestación de servicios, de negocio y de tecnología, permitiendo al navegante acceder a un catálogo de servicios estandarizados. Lo que*

[1198] Cfr. https://www.fundeu.es/escribireninternet/mensajeria-instantanea/ (consulta: 7 de junio de 2019).

[1199] Tanto las llamadas como las vídeo llamadas pueden ser realizadas debido a que el desarrollador de la aplicación introduce «Voz sobre Protocolo de Internet» o también conocido «*Voice over IP*» en la aplicación de mensajería instantánea. La AEPD ha determinado al respecto que «*este sistema transmite llamadas de voz de manera similar al envío de correos electrónicos, es decir, convierte la voz en paquetes de datos para poder transmitirlos a través de Internet, como cualquier otro paquete de información*», *vid.* AEPD, «*Recomendaciones dirigidas a usuarios de internet*» (en línea). Disponible en: https://www.unirioja.es/servicios/si/seguridad/difusion/RecomendacionesAGPD.pdf (consulta y descarga: 7 de junio de 2019).

[1200] Trad. del inglés: «*is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction*», Cfr. MELL P. and GRANCE, T., «The NIST defination of Cloud Computing»(en línea), *National Institute os Standars and Technology- Departament of Commerce, USA,* Special Publication 800-145, September, 2011, p. 2. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (consulta: 7 de junio de 2019).

técnicamente podemos definir como una arquitectura que dispone de un conjunto de recursos que son proporcionados por un proveedor externo, que están soportados y son compartidos a través de la red de Internet. En otras palabras, aplicaciones que no están instaladas en el ordenador personal sino alojadas en los servidores externos. Así, nos encontramos con una amplia gama de servicios ofrecidos por los proveedores servicios en la nube, que van desde el procesamiento virtual, hosting de aplicaciones, a soluciones basadas en software online que vienen a reemplazar programas que habitualmente están instalados en todos los ordenadores, como puede ser los procesadores de texto, agendas y calendarios e incluso sistemas de archivo para el almacenamiento de documentos en línea»[1201].

La computación en la nube se caracteriza por ser un servicio bajo demanda., por tener una accesibilidad amplia, el usuario no necesitara ningún tipo de software específico descargado en sus dispositivos, aunque también se ponga a disposición de estas aplicaciones móviles para su mejor funcionamiento; normalmente se cuenta con una capacidad de espacio para almacenamiento, la cual puede variar dependiendo del proveedor del servicio y si este se pone a disposición de manera gratuita o en su modalidad de pago; dentro de este servicio también se ofrece a los usuarios la capacidad de edición de documentos dentro de la web, los cambios no serán almacenados en el dispositivo, estos se guardarán en los servidores

2.8 Real Simple Sindication (RSS).

Es importante mencionar también que dentro de esta *Web* se han desarrollado herramientas como la sindicación de contenidos, mejor conocido como RSS (*Really Simple Sindication*), la cual es una herramienta que se encarga de redifundir la información contenida en páginas *Web* de manera breve y actualizada constantemente, donde el usuario es quién decide qué contenidos desea ver y de qué fuentes (*feeds*), la cual se podrá compartir en otras páginas *Web*. Sin embargo, el dinamismo en la *Web* 2.0 nos transporta a una nueva generación de Sindicación de datos, esta vez desarrollado mediante aplicaciones para los *SmartPhone*. Así, en

[1201] CORONA HERRERO, J. U., «Los datos en la nube: retos actuales en la protección del derecho de propiedad» (en línea), *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 32, mayo-agosto 2013. Disponible en: https://proview.thomsonreuters.com (consulta: 24 de octubre de 2017). BIB\2013\1644.

aplicaciones como *Flipboard* no solo se restringe la sindicación de contenidos de nuestra preferencia, sino que nos da la opción de controlar las *feeds* contenidas en las distintas redes sociales de las cuales se encuentre suscrito el usuario o que habilite. RIBES I GUÀRDIA, F. X., define a un RSS como «*documento que contiene metadatos relacionados con un sitio web en concreto. Los archivos RSS (llamados también feeds RSS o canales RSS) se estructuran en ítems, con el título, el resumen y el enlace de la información que describen y, eventualmente, pueden contener otros datos (fecha de publicación del documento, nombre del autor)*»[1202].

2.9 Big data.

El «*Big Data*» es un conjunto de herramientas que facilitan la recogida, el tratamiento, la medición, la búsqueda y el almacenamiento de datos en cantidades ingentes, principalmente mediante el uso de algoritmos, esta información es obtenida del uso que realizan los usuarios dentro de Internet, esta información suele estar controlada por empresas, autoridades del sector público y organizaciones[1203]. Técnicamente, «*el término hace referencia a sistemas que manipulan enormes cantidades de datos, sobre los que ejecutan diferentes tipos de análisis con técnicas propias de business analytics, data mining o text mining para buscar patrones. Podemos hablar de volúmenes de terabytes, petabytes (1.000.000.000.000.000 bytes, o más*)»[1204]. De acuerdo con la Profesora LLANEZA el big data suele definirse por «*sus "tres Vs" donde el volumen se refiere al conjunto de datos masivos analizar, la velocidad se refiere a datos en tiempo real y la variedad se refiere a las diferentes fuentes de datos*»[1205]. En este sentido la AEPD determinó que «*con dicho término se hace referencia al conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por*

[1202] *Vid.* RIBES I GUÀRDIA, F. X., «El valor de los metadatos y de la inteligencia colectiva» (en línea), *Telos* Disponible en: https://telos.fundaciontelefonica.com/archivo/numero073/el-valor-de-los-metadatos-y-de-la-inteligencia-colectiva/ (consulta 30 de noviembre de 2018).
[1203] *Vid.* GIL, E., *op. cit.*, p.17.
[1204] SERRANO-COBOS, J., «*Big data* y *not so big data*» (en línea) *Anuario ThinkEPI*, v. 7, 2013, p. 161 Disponible en: https://dialnet.unirioja.es/descarga/articulo/4234739.pdf (consulta y descarga: 10 de junio de 2019).
[1205] LLANEZA, P., «Capítulo 9. Dataísmo, transparencia y protección de datos», RODRÍGUEZ MARÍN, S. y MUÑOZ GARCÍA, A. (Coords.), *Aspectos legales de la economía colaborativa y bajo demanda en plataformas digitales*, Wolters Kluwer, 2018, p. 204.

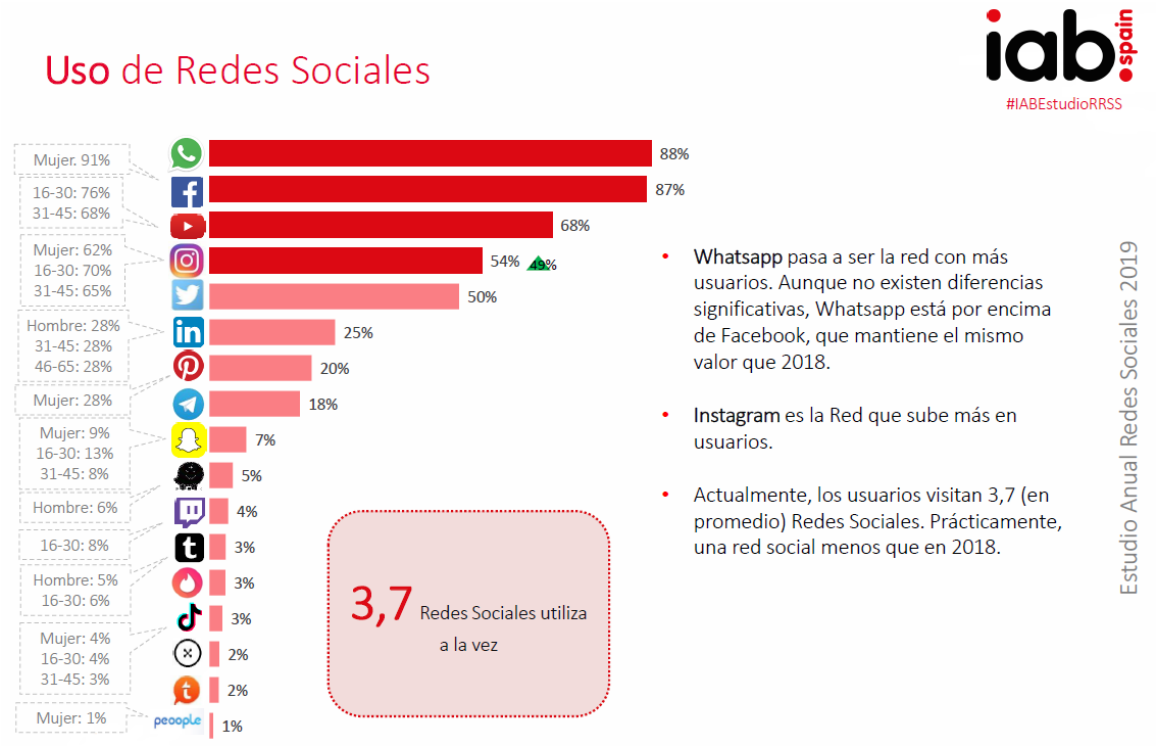
computación en paralelo. Al Big Data frecuentemente se le caracteriza mediante tres "v": Volumen, Variedad y Velocidad»[1206]. Finalmente, es importante señalar también que este tipo de tecnología utilizada para tratar datos de manera masiva hace uso de distintos algoritmos.

[1206] AEPD, «*Código de buenas prácticas en protección de datos para proyectos Big Data*» (en línea). Disponible en: https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf (consulta: 10 de junio de 2019).

ANEXO II.

FIGURAS.

FIGURA 1:USO DE REDES SOCIALES, 2019.



IAB SPAIN, «Estudio anual de Redes sociales», 2020 Disponible en: https://iabspain.es/estudio/estudio-redes-sociales-2020/ (consulta y descarga: 29 de julio de 2020).

FIGURA 2: SENTENCIAS DE LA AUDIENCIA NACIONAL, SALA DE LO CONTENCIOSO, SOBRE EL DERECHO AL OLVIDO.

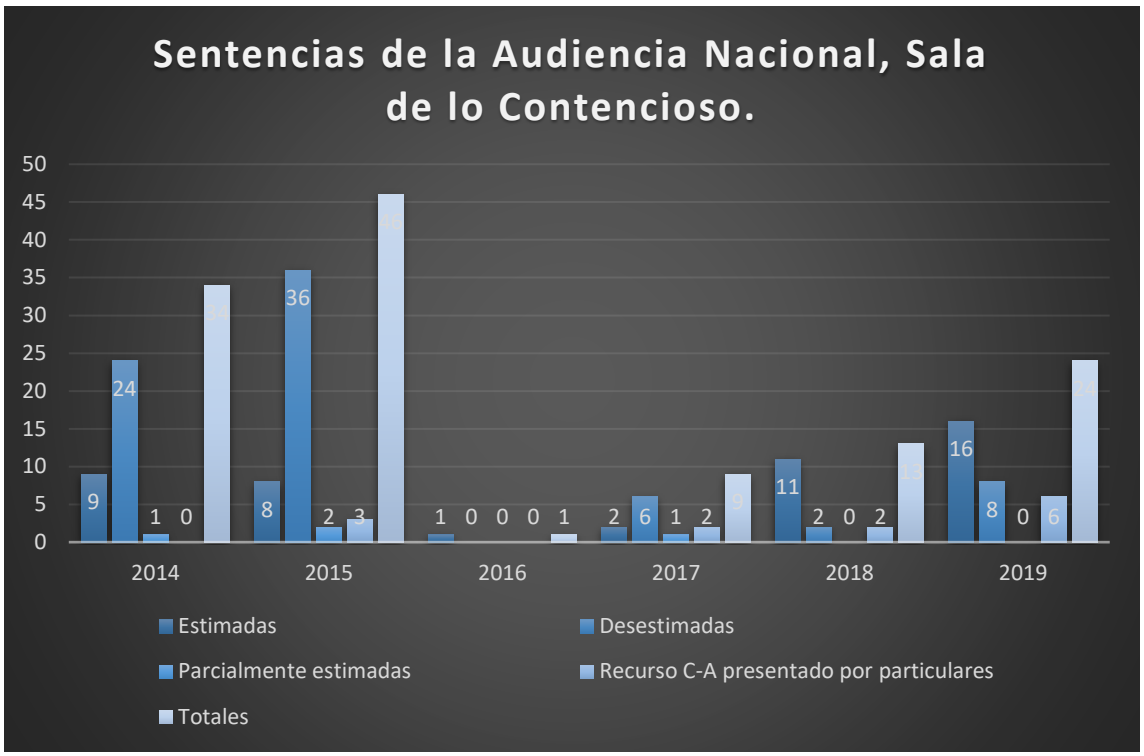
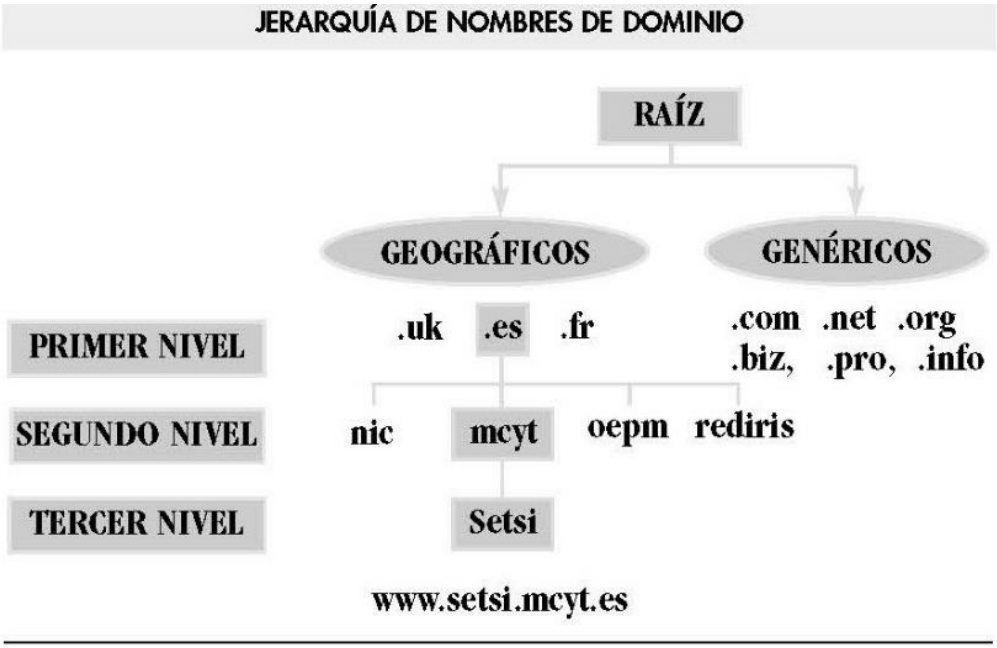
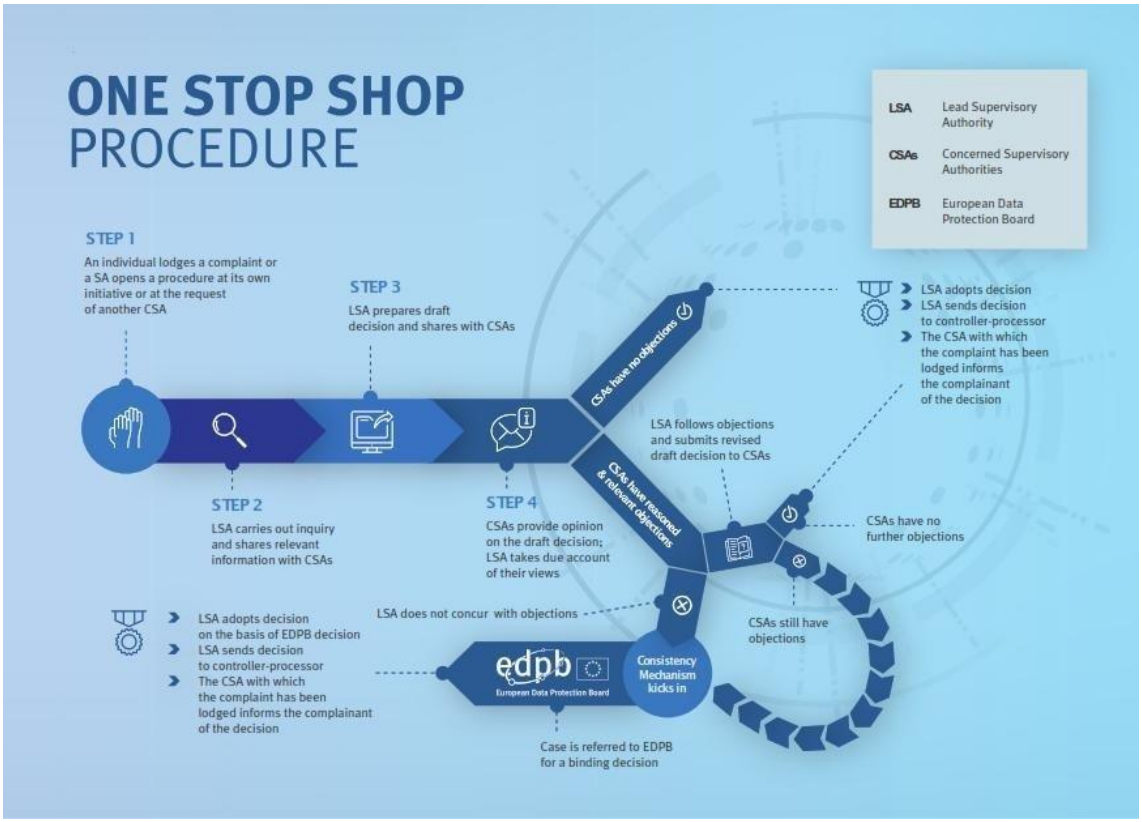


FIGURA 3: EJEMPLO SOBRE LA JERARQUÍA DE NOMBRES DE DOMINIO.



RODRÍGUEZ RAPOSO, A. (2001). *Jerarquía de nombres de dominio*. [imagen] Disponible en: https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEconomiaIndustrial/338/07rodriguez338.pdf [consulta: 14 de noviembre de 2018).

FIGURA 4: PROCEDIMIENTO DE COOPERACIÓN ENTRE LAS AUTORIDADES DE CONTROL (DE VENTANILLA ÚNICA) Y EL DICTAMEN DEL CEPD (ARTS. 63 -65 DEL RGPD).



EDPB (@EU_EDPB). «In need of some extra information on the Art. 65 procedure? We've got you covered! You can consult our FAQ on the Art. 65 procedure on the EDPB website: https://europa.eu/!mn73Dm or take a closer look at the different steps in the procedure in the infographic below:», 15 de diciembre de 2020, 16:39 (Tuit). Disponible en: https://twitter.com/EU_EDPB/status/1338871251608219655 (consulta: 16 de diciembre de 2020).

ANEXO III

Relación de sentencias sobre el «derecho al olvido» emitidas por la Sala de lo Contencioso-administrativo del TS por número de recurso.

- 641/2015 (Sentencia núm. 1381/2016 de 13 junio. RJ 2016\3125; ECLI:ES:TS:2016:2722),
- 642/2015 (Sentencia núm. 1529/2016 de 27 junio. RJ 2016\2842; ECLI:ES:TS:2016:3006),
- 794/2015 (Sentencia núm. 1382/2016 de 13 junio. RJ 2016\3693; ECLI:ES:TS:2016:2699),
- 795/2015 (Sentencia núm. 1610/2016 de 4 julio. RJ 2016\3730; ECLI: ECLI:ES:TS:2016:3333),
- 797/2015 (Sentencia núm. 1611/2016 de 4 julio. RJ 2016\3729; ECLI: ECLI:ES:TS:2016:3313),
- 798/2015 (Sentencia núm. 1383/2016 de 13 junio. RJ 2016\4147; ECLI:ES:TS:2016:2724),
- 799/2015 (Sentencia núm. 1612/2016 de 4 julio. RJ 2016\4329; ECLI:ES:TS:2016:3315),
- 800/2015 (Sentencia núm. 1613/2016 de 4 julio. RJ 2016\4797; ECLI:ES:TS:2016:3336),
- 804/2015 (Sentencia de 15 marzo 2016. RJ 2016\1301; ECLI: ES:TS:2016:1103),
- 807/2015 (Sentencia núm. 1614/2016 de 4 julio. RJ 2016\3747; ECLI:ES:TS:2016:3328),
- 810/2015 (Sentencia núm. 1384/2016 de 13 junio. RJ 2016\3119; ECLI:ES:TS:2016:2723),
- 811/2015 (Sentencia núm. 1615/2016 de 4 julio. RJ 2016\4326; ECLI:ES:TS:2016:3406),
- 984/2015 (Sentencia núm. 1385/2016 de 13 junio. RJ 2016\3324; ECLI:ES:TS:2016:2696),
- 996/2015 (Sentencia núm. 1386/2016 de 13 junio. RJ 2016\3484; ECLI:ES:TS:2016:2707),
- 1072/2015 (Sentencia núm. 1454/2016 de 20 junio. RJ 2016\2767; ECLI:ES:TS:2016:2845),
- 1074/2015 (Sentencia núm. 1455/1960 de 20 junio. RJ 2016\4791; ECLI:ES:TS:2016:2836),
- 1075/2015 (Sentencia núm. 1387/2016 de 13 junio. RJ 2016\2741; ECLI:ES:TS:2016:2725),
- 1078/2015 (Sentencia de 14 marzo 2016. RJ 2016\1525; ECLI:ES:TS:2016:1056),
- 1079/2015 (Sentencia núm. 1531/2016 de 27 junio. RJ 2016\2848; ECLI:ES:TS:2016:3000),
- 1083/2015 (Sentencia núm. 1456/2016 de 20 junio. RJ 2016\4790; ECLI:ES:TS:2016:2876),
- 1084/2015 (Sentencia núm. 1457/2016 de 20 junio. RJ 2016\2778; ECLI:ES:TS:2016:2850),
- 1085/2015 (Sentencia núm. 1532/2016 de 27 junio. RJ 2016\2857; ECLI:ES:TS:2016:3048),
- 1086/2015 (Sentencia núm. 1689/2016 de 11 julio. RJ 2016\3763; ECLI:ES:TS:2016:3489),
- 1087/2015 (Sentencia núm. 1533/2016 de 27 junio. RJ 2016\3350; ECLI:ES:TS:2016:2997),
- 1091/2015 (Sentencia núm. 1690/2016 de 11 julio. RJ 2016\4796; ECLI:ES:TS:2016:3347),
- 1142/2015 (Sentencia núm. 1797/2016 de 18 julio. RJ 2016\3775; ECLI:ES:TS:2016:3687),
- 1143/2015 (Sentencia núm. 1534/2016 de 27 junio. RJ 2016\2841; ECLI:ES:TS:2016:2998),
- 1194/2015 (Sentencia núm. 1535/2016 de 27 junio. RJ 2016\3713; ECLI:ES:TS:2016:2996),
- 1195/2015 (Sentencia núm. 1388/2016 de 13 junio. RJ 2016\4146; ECLI:ES:TS:2016:2702),
- 1293/2015 (Sentencia núm. 1618/2016 de 4 julio. RJ 2016\4798; ECLI:ES:TS:2016:3316),
- 1294/2015 (Sentencia núm. 1799/2016 de 18 julio. RJ 2016\3794; ECLI:ES:TS:2016:3676),

- 1296/2015 (Sentencia núm. 1458/2016 de 20 junio. RJ 2016\4792; ECLI:ES:TS:2016:2837),
- 1297/2015 (Sentencia núm. 1800/2016 de 18 julio. RJ 2016\3792; ECLI:ES:TS:2016:3669),
- 1298/2015 (Sentencia núm. 1801/2016 de 18 julio. RJ 2016\3774; ECLI:ES:TS:2016:3668),
- 1300/2015 (Sentencia núm. 1459/2016 de 20 junio. RJ 2016\4793; ECLI:ES:TS:2016:2842),
- 1301/2015 (Sentencia núm. 1693/2016 de 11 julio. RJ 2016\3734; ECLI:ES:TS:2016:3359),
- 1302/2015 (Sentencia núm. 1802/2016 de 18 julio. RJ 2016\3910; ECLI:ES:TS:2016:3667),
- 1304/2015 (Sentencia núm. 1803/2016 de 18 julio. RJ 2016\3909; ECLI:ES:TS:2016:3671),
- 1385/2015 (Sentencia núm. 1694/2016 de 11 julio. RJ 2016\3736; ECLI:ES:TS:2016:3362),
- 1386/2015 (Sentencia núm. 1695/2016 de 11 julio. RJ 2016\3732; ECLI:ES:TS:2016:3361),
- 1389/2015 (Sentencia núm. 1696/2016 de 11 julio. RJ 2016\3899; ECLI:ES:TS:2016:3370),
- 1482/2015 (Sentencia de 11 marzo 2016. RJ 2016\1519; ECLI:ES:TS:2016:1055),
- 1485/2015 (Sentencia núm. 1805/2016 de 18 julio. RJ 2016\3793; ECLI:ES:TS:2016:3675),
- 1497/2015 (Sentencia núm. 1697/2016 de 11 julio. RJ 2016\3733; ECLI:ES:TS:2016:3349),
- 1666/2015 (Sentencia núm. 1460/2016 de 20 junio. RJ 2016\2768; ECLI:ES:TS:2016:2847),
- 1667/2015 (Sentencia núm. 1910/2016 de 21 julio. RJ 2016\3626; ECLI:ES:TS:2016:3727),
- 1753/2015 (Sentencia núm. 1806/2016 de 18 julio. RJ 2016\3788; ECLI:ES:TS:2016:3690),
- 1756/2015 (Sentencia núm. 1807/2016 de 18 julio. RJ 2016\3783; ECLI:ES:TS:2016:3674),
- 1859/2015 (Sentencia núm. 1911/2016 de 21 julio. RJ 2016\3433; ECLI:ES:TS:2016:3733),
- 1863/2015 (Sentencia núm. 1536/2016 de 27 junio. RJ 2016\2831; ECLI:ES:TS:2016:3005),
- 1866/2015 (Sentencia núm. 1808/2016 de 18 julio. RJ 2016\3789; ECLI:ES:TS:2016:3693),
- 1867/2015 (Sentencia núm. 1912/2016 de 21 julio. RJ 2016\3620; ECLI:ES:TS:2016:3722),
- 2276/2015 (Sentencia núm. 1913/2016 de 21 julio. RJ 2016\3438; ECLI:ES:TS:2016:3725),
- 2355/2015 (Sentencia núm. 1915/2016 de 21 julio. RJ 2016\3627; ECLI:ES:TS:2016:3746),
- 2789/2015 (Sentencia núm. 1809/2016 de 18 julio. RJ 2016\3414; ECLI:ES:TS:2016:3860),
- 2798/2015 (Sentencia núm. 1916/2016 de 21 julio. RJ 2016\3624; ECLI:ES:TS:2016:3717),
- 2863/2015 (Sentencia núm. 1810/2016 de 18 julio. RJ 2016\3785; ECLI:ES:TS:2016:3694),
- 2866/2015 (Sentencia núm. 1917/2016 de 21 julio. RJ 2016\3625; ECLI:ES:TS:2016:3721),
- 2867/2015 (Sentencia núm. 1918/2016 de 21 julio. RJ 2016\4098; ECLI:ES:TS:2016:3695),
- 3275/2015 (Sentencia núm. 1919/2016 de 21 julio. RJ 2016\3623; ECLI:ES:TS:2016:3706),
- 3279/2015 (Sentencia núm. 1920/2016 de 21 julio. RJ 2016\3919; ECLI:ES:TS:2016:3713).

BIBLIOGRAFÍA

TRATADOS Y MONOGRAFÍAS.

AGUSTINOY GUILAYN, A. y MONCLÚS RUIZ, J., *Aspectos legales de las redes sociales,* Bosch, Barcelona, 2016, pp. 386. ISBN: 978-84-9090-105-2.

ALEGRE MARTÍNEZ, M.A., *El Derecho a la Propia Imagen,* Tecnos, Madrid, 1997, pp. 169. ISBN: 84-309-3105-8.

ALLESSIE, D., SOBOLEWSKI, M. and VACCARI, L., «Blockchain for digital goverment. An assessment of pioneering implementations in public services» (en línea), *Publications Office of European Union, Luxembourg*, 2019, pp. 88 (consulta y descarga: 22 de febrero de 2020). ISBN 978-92-76-00581-0. DOI: 10.2760/942739.

ÁLVAREZ CARO, M., *Derecho al Olvido en Internet: El nuevo paradigma de la privacidad en la era Digital*, Madrid, Reus, 2015, pp. 143. ISBN: 978-84-290-1836-3.

BALLESTEROS MOFFA, L. Á., *Las fronteras de la privacidad. El conflicto entre seguridad pública y datos personales en una sociedad amenazada y tecnológica,* Comares, Granada, 2020, pp. 264. ISBN: 978-84-1369-048-3.

BARRIO ANDRÉS, M., *Fundamentos de Derecho de Internet,* Centro de Estudios Políticos y Constitucionales, Madrid, 2017, pp. 533. ISBN 978-84-259-1754-7.

BERNERS-LEE, T., *Tejiendo la red*, Edición traducida por RUBIO FERNÁNDEZ, M. Weaving the WEB: The Original Desing and Ultimate Destinity of the World Wide Web by Its Inventor, Madrid, Siglo veintiuno de España Editores, 2000, pp. 237. ISBN 84-323-1040-9.

CAPILLA RONCERO, F., *et al.* (Dir.), *Derecho Digital: Retos y cuestiones actuales.* Aranzadi, Navarra, 2018, ISBN: 978-84-9197-070-5:

CARBAJO CASCÓN, F., *Conflictos entre signos distintivos y nombres de dominio en Internet*, Ed. Aranzadi, Navarra, 1999, pp. 249. ISBN: 84-8410-369-2.

CUETO PÉREZ, M., *Régimen jurídico de la investigación científica: la labor investigadora en la Universidad,* Centro de Estudios de Derecho, Economía y Ciencias Sociales Cedecs, Barcelona, 2002, pp. 288. ISBN: 84-95665-13-1.

DAVARA FERNÁNDEZ DE MARCOS, L., *Implicaciones Socio-Jurídicas de las Redes Sociales,* Ed. Aranzadi, Navarra, 2015, pp. 507. ISBN 978-84-9098-910-4.

DÁVARA RODRÍGUEZ, M.A., *La protección de datos en Europa: principios, derechos y procedimiento,* Ed. Asnef, Madrid, 1998, pp. 204. ISBN 84-923731-0-5.

DURÁN CARDO, B. *La figura del responsable en el Derecho a la Protección de datos.* Wolters Kluwer España, Madrid, 2016, ISBN: 978-84-9020-553-2

ÉCIJA BERNAL, Á., *El ciberespacio, un mundo sin Ley. Internet: la revolución que cambió las normas del juego* (en línea), Wolters Kluwer, 2017, pp. 138. Disponible en: http://ciberderecho.com/El ciberespacio un mundo sin ley.pdf (consulta 7 de diciembre de 2018).

FERNÁNDEZ SALMERÓN, M., *La protección de los datos personales en las Administraciones Públicas,* Thomson Civitas, 2003, pp. 498. ISBN: 84-470-2105-X.

FERRAJOLI, L., *Los fundamentos de los derechos fundamentales*. Edición traducida de CABO DE y PISARELLO, Ed. Trotta, Madrid, 2001, pp. 180. ISBN 84-8164-436-6.

FREEMAN, L. C., *El desarrollo del análisis de redes sociales, un estudio de sociología de la ciencia.* Trad. ALCÁNTARA VALVERDE, N. Palibrio, EE.UU., pp. 193, ISBN: 978-1-4633-3085-9.

FUENTE MIGUÉLEZ, A. DE LA, *El secreto estadístico. Factor clave en la Administración pública,* Mc Graw Hill INAP, Madrid, 2018, pp. 217. ISBN: 978-847351-638-9.

GALLEGO VÁZQUEZ, J. A., *Comunidades virtuales y redes sociales* (en línea), Creative Commons Reconociemiento NoComercial CompartirIgual, Madrid, 2012. Disponible en: http://www.comunidadenlared.com/mi-libro-comunidades-virtuales-y-redes-sociales-en-libre-descarga/ (consulta y descarga: 23 de mayo de 2019).

GARCÍA DE ENTERRÍA, E. y FERNÁNDEZ, T-R., *Curso de Derecho Administrativo I,* Decimoctava edición, Tomo I, Thomson Reuters Civitas, Navarra, 2017, pp. 871. ISBN: 978-84-9152-872-2.

GARCÍA MORALES, M.J., *Transparencia y rendición de cuentas de las relaciones de cooperación intergubernamental en el Estado autónomico,* Generalitat de

Catalunya. Institut d´Estudis de l´Autogovern Palau Centelles, Barcelona, 2017, p. 339. ISBN: 978-84-393-9590-4.

GIL, E., *Big data, privacidad y protección de datos* (en línea), AEPD y BOE, Madrid, 2016, p. 149 Disponible en: https://www.aepd.es/media/premios/big-data.pdf. ISBN: 978-84-340-2309-3 (consulta y descarga: 10 de junio de 2019).

GÓMEZ SÁNCHEZ, Y., *Constitucionalismo multinivel: Derechos fundamentales,* 3ª ed., Sánz y Torres/UNED, Madrid, 2015, pp. 584. ISBN: 978-84-15550-97-6.

HERNÁNDEZ FERNÁNDEZ, A., *El honor, la intimidad y la imagen como derechos fundamentales,* Madrid, Colex, 2009, p. 1142. ISBN 978-84-8342-176-5.

LESMES SERRANO, C., *et al.*, *La ley de Protección de Datos, análisis y comentario de su jurisprudencia.* Valladolid, Lex Nova, 2008. 860 p. ISBN 978-84-85012-91-6.

LÓPEZ ZAMORA, P., *El ciberespacio y su ordenación*, Grupo difusión, Madrid, 2006, pp. 323. ISBN 84-96705-05-6.

LOSANO, M., PÉREZ LUÑO, A. Y GUERRERO MATEUS, M., *Libertad Informática y Leyes de Protección de Datos Personales,* Ed. Centro de Estudios Constitucionales, Bilbao, 1989, p. 213. ISBN: 8425908418.

LUCAS VERDÚ, P., *Estimativa y política constitucionales (los valores y principios rectores del ordenamiento constitucional español)*, Universidad de Madrid, Madrid, 1984, pp. 212. ISBN: 9788460036014.

MARZAL RAGA, R., *El apercibimiento: una nueva sanción en materia de protección de datos.* (en línea), Tirant lo Blanch, 2015, pp. 153 (consulta: 12 de octubre de 2020). ISBN: 9788490863831.

MENÉNDEZ SEBASTIÁN, E. Mª., *Las garantías del interesado en el procedimiento administrativo electrónico. Luces y sobras de las nuevas leyes 39 y 40/2015,* Tirant lo Blanch, Valencia, 2017, pp. 116. ISBN: 978-84-9169-097-9.

MUÑOZ MACHADO, S., *La regulación de la red. Poder y Derecho en Internet*, Ed. Taurus, Madrid, 2000, pp. 281. ISBN: 84-306-0415-4.

NAVARRO SCHLEGEL, A., Diccionario de términos de comunicaciones y redes, Ed. Pearson Educación, Madrid, p. 632. ISBN: 84-205-3471-4.

PASCUAL MEDRANO, A., *El derecho Fundamental a la Propia Imagen. Fundamento, contenido y límites,* Ed. Aranzadi, Navarra, 2003, pp. 177. ISBN 84-9767-168-6.

PÉREZ BES, F., *La publicidad comportamental online,* Ed. UOC, Barcelona, 2012, pp. 96. ISBN: 978-87-9788-998-8.

PÉREZ LUÑO, A., *La tercera generación de Derechos Humanos,* Ed. Aranzadi, Navarra, 2006, pp. 319. ISBN 84-9767-640-8.

PÉREZ LUÑO, A., Los *derechos fundamentales,* 7ª Ed. Madrid*,* Ed. Tecnos, 1998, pp. 231. ISBN 84-309-3266-6.

REBOLLO DELGADO, L., *El derecho fundamental a la intimidad,* Ed. Dykinson, Madrid, 2000, pp. 299. ISBN 84-8155-581-9.

RODRÍGUEZ PALOP, M.A., *La nueva generación de Derechos Humanos,* Ed. Dykinson, Madrid, 2002, p. 481. ISBN: 84-8155-883-4.

SÁNCHEZ MORÓN, M., *Derecho administrativo. Parte general.* 18ª edición, Madrid, 2019, pp. 974. ISBN: 9788430977437.

SERRANO PÉREZ, M. M., *El derecho fundamental a la protección de datos. Derecho español y comparado,* Thomson Civitas, Madrid, 2003, pp. 518. ISBN 84-470-2106-8.

SIMÓN CASTELLANO, P., *El régimen constitucional del derecho al olvido digital,* Tirant lo Blanch, Valencia, 2012, pp. 254. ISBN 978-84-9033-005-0.

TALENS OLIAG, S. Y HERNÁNDEZ ORALLO, J., *Internet. Redes de computadores y sistemas de información,* Ed. Paraninfo, segunda edición, España, 1998, pp. 721. ISBN: 84-283-2334-8.

TERRÓN SANTOS, D. y DOMÍNGUEZ ÁLVAREZ, J.L., *Nueva regulación de la protección de datos y su perspectiva digital,* Comares, Granada, 2019, pp. 246. ISBN: 978-84-9045-844-0.

TORRE DE SILVA Y LÓPEZ DE LETONA, J., *Internet, propiedad industrial y competencia desleal,* Centro de Estudios Políticos y Constitucionales, Madrid, 2002, pp. 160. ISBN: 978-84-2591-182-8.

TOURIÑO PENA, A., *El derecho al Olvido y a la Intimidad en Internet*, Ed. Catarata, Madrid, 2014, pp. 142 ISBN 978-84-8319-880-3.

TÖNNIES, F., *Comunidad y Asociación, comunismo y socialismo como formas de vida social,* Trad. JOSÉ-FRANCISCO IVARS. Badalona, Ed. Península, 1979, pp. 282. ISBN: 84-297-1499-5.

TRAYTER JIMÉNEZ, J. M., *Derecho administrativo. Parte general,* Cuarta edición, Atelier, 2019, pp. 554. ISBN: 978-84-17466-65-7.

URÍAS, J., *Lecciones de Derecho de la Información*. Madrid, Ed. Tecnos, 2003, pp. 269. ISBN 84-309-4033-2.

VERDAGUER LÓPEZ, J., *et al*, *Todo Protección de Datos.* Valencia, CISS, 2011, pp. 889. ISBN 978-84-9954-372-7.

ARTÍCULOS Y CAPÍTULOS DE LIBROS.

ABUÍN VENCES, N. Y VINADER SEGURA, R., «El desarrollo de la World Wide Web en España» (en línea), *Razón y palabra*, núm. 75, 2011, pp. 24 Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3689999&orden=304611&info=link (consulta: 4 de diciembre de 2018). ISSN-e 1605-4806.

ALAMILLO DOMINGO, I., «Capítulo 16. Esquema Nacional de Seguridad: La administración electrónica y la seguridad de la información», CAMPOS ACUÑA, C. (Dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, Segunda edición, Wolters Kluwer, 2019, pp. 607-639.

ALAMILLO DOMINGO, I., «Identidad y firma electrónica. Nociones técnicas y marco jurídico general. Identificación y autenticación de los ciudadanos», GAMERO CASADO, E. (Dir.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*. Tomo I. Tirant lo Blanch, Valencia, 2017, pp. 675-768. ISBN 978-84-9143-635-5.

ALAMILLO DOMINGO, I., «Las tecnologías de registro distribuido (blockchain) y la transformación del procedimiento administrativo» (en línea), *Consultor de los ayuntamientos y de los juzgados: Revista técnica especializada en administración local y justicia municipal,* núm. 1 (enero), 2019. Disponible en: smarteca.es (consulta 9 de enero de 2021). ISSN: 0210-2161.

ALMEIDA, F., «Concept and Dimensions of web 4.0» (en línea), *International journal of computers & technology* pp. 7040-7046. DOI: 10.24297/ijct.v16i7.6446 (consulta 28 de noviembre de 2018). ISSN-e:2277-3061.

ÁLVAREZ CARO, M. «El derecho a la supresión o al olvido», PIÑAR MAÑAS, J.L. (Dir.). *Reglamento General de Protección de Datos Personales. Hacia un nuevo modelo europeo de privacidad*, Reus, Madrid, 2016, pp. 241-256. ISBN: 978-84-290-1936-0.

ÁLVAREZ RIGAUDIAS, C., «Capítulo XXI. Tratamiento de datos con fines de investigación científica y/o médica», RALLO LOMBARTE, A. (Dir.), *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales,* Tirant lo blanch, Valencia, 2019, pp. 707-740. ISBN: 978-84-1313-282-2.

AMARO LÓPEZ, J. A., «El proyecto Tor» (en línea), *Paakat: Revista de Tecnología y Sociedad*, núm. 9 Disponible en: http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/246/385 (consulta: 11 de noviembre de 2018). ISSN: 2007-3607.

AMARO LÓPEZ, J.A., *et al.*, «La web oculta y cómo los buscadores encuentran la información» (en línea), *Paakat: Revista de tecnología y sociedad*, número 7, volumen 4, 2014-2015, pp. 5. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5695439.pdf (consulta: 23 de octubre de 2017). ISSN: 2007-3607.

APARICIO SALOM, J., «El régimen jurídico de las *cookies* y su aplicación por la agencia española de protección de datos» (versión electrónica-base de datos Aranzadi Instituciones), *Revista Aranzadi Doctrinal,* núm. 11/2014, Parte estudio, (descarga y consulta: 3 de octubre de 2017). Referencia: BIB 2014\675.

APARICIO VAQUERO, J. P., «La protección de datos que viene: el nuevo Reglamento General Europeo», *Ars Iuris Salamanticensis. Tribuna actualidad.* Vol. 4, diciembre 2016, pp. 27-34, ISSN-e: 2340-5155.

ARJONEZ GIRÁLDEZ, D., «La neutralidad de la red desde su arquitectura por capas ¿de transportistas públicos a gestores de contenidos?», CERRILLO I MARTÍNEZ, A., *et al.* (Coords.), *Neutralidad de la red y otros retos para el futuro de internet. Actas del VII Congreso Internacional internet, derecho y política. Universitat oberta de Catalunya*, Huygens, España, 2011, pp. 53-65. ISBN: 978-84-694-7037-4

BALCELLS, J., PADRÓ-SOLANET, A. y SERRANO, I., «La adopción y gestión de redes sociales en los ayuntamientos catalanes», CRIADO, I. (Ed.), *Nuevas tendencias en la gestión pública. Innovación abierta, gobernanza inteligente y tecnologías sociales en unas administraciones públicas colaborativas,* Ed. Instituto Nacional de Administración Pública, Madrid, 2016, p. 165-188. ISBN: 978-84-7351-525-2.

BELLOCH ORTÍ, C., «Las tecnologías de la información y comunicación (T.I.C.)» (en línea). Disponible en: https://www.uv.es/~bellochc/pdf/pwtic1.pdf (consulta: 1 de abril de 2019).

BENEDICT KINGSBURY, *et al.*, «The Emergence of Global Administrative Law», *Law and Contemporary Problems*, Summer 2005- 68, pp. 15-62. Disponible en: https://scholarship.law.duke.edu/lcp/vol68/iss3/2 (consulta: 11 de junio de 2019). ISSN 1945-2322.

BERNAL BLAY, M.Á., «Las "leyes del contrato" (los pliegos): Contenido esencial y formas de control», GIMENO FELIU, J. M. (Dir.), *Estudio sistemático de la Ley de Contratos del Sector Público* (en línea), Thomson Reuters Aranzadi, Capítulo 25, 2018Disponible en: https://proview.thomsonreuters.com (consulta: 30 de octubre de 2020). ISBN: 978-84-9177-626-0.

BIURRUN ABAD, F.J., «"Accountability" o responsabilidad activa en el Reglamento General de Protección de Datos», *Actualidad jurídica,* Aranzadi, núm. 927/2017, pp. 28. BIB 2017\732.

BLANCO ANTÓN, M.J., «Autoridades de control independientes (Arts. 51-59 RGPD). Autoridades de Protección de Datos (Arts. 44-59 y Disposición adicional cuarta LOPDGDD)», LÓPEZ CALVO, J., *La adaptación al nuevo marco de*

protección de datos tras el RGPD y la LOPDGDD, Wolters Kluwer Bosch, España, 2019, pp. 601-635. ISBN: 978-84-9090-345-2.

BOTELLA PAMIES, E., «Artículo 37. Intervención del delegado de protección de datos en caso de reclamación ante las autoridades de protección de datos», ARENAS RAMIRO, M. y ORTEGA GIMÉNEZ, A. (Dirs.), *Protección de datos. Comentarios a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales (en relación con el RGPD)*, Sepín, Madrid, 2019, pp. 198-200. ISBN: 978-84-17414-92-4.

BOTO ÁLVAREZ, A., «Capítulo 19. La determinación administrativa de derechos fundamentales: Autoridades independientes y órganos de resolución de recursos especiales», PUNSET BLANCO, L. y ÁLVAREZ ÁLVAREZ, L. (Coords.), *Cuatro décadas de una constitución normativa (1978-2018). Estudios sobre el desarrollo de la Constitución Española,* Thomson Reuters- Civitas y Universidad de Oviedo, Navarra, 2018, pp. 477-494. ISBN: 978-84-9177-683-3.

BOTO ÁLVAREZ, A., «La protección administrativa de la identidad personal: desafíos jurídicos y dilemas sociales», BARRIO ALONSO, C., *et al.* (Eds.), *Fronteras de la ciencia: dilemas,* Biblioteca nueva, Madrid, 2014, pp. 73-85. ISBN: 978-84-1617084-5.

BOYD, D. M. Y ELLISON, N. B., «Social Network Sites: Definition, History, and Scholarship» (en línea), *Journal of Computer- Mediated Communication,* Diciembre 2007, Disponible en: https://doi.org/10.1111/j.1083-6101.2007.00393.x (consulta: 6 de abril de 2019).

BREIGER, R., «Control social y redes sociales: Un modelo a partir de Georg Simmel», Trad. PIZARRO, N. (en línea), *Política y sociedad,* pp. 57-72 Disponible en: https://revistas.ucm.es/index.php/POSO/article/download/POSO0000130057A/24603 (consulta: 25 de enero de 2018).

BUEYO DÍEZ JALÓN, M., «El tratamiento de datos de carácter personal por las Administraciones públicas versus el Derecho Fundamental a la Privacidad:

los ficheros públicos», *Revista General de Derecho Administrativo*, núm. 23, 2010, pp. 39.

BUSTILLO SÁIZ, Mª M., «Hacia la patentabilidad de los programas de ordenador: Un diálogo particular entre Derecho y la Economía», *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm.16, 2008. BIB 2008\109.

BUSTOS GISBERT, R., «El concepto de libertad de información a partir de su distinción de la libertad de expresión», *Revista de estudios políticos,* núm. 85, 1994, pp. 261-290. ISSN 0048-7694.

CÁCERES ZAPATERO, Mª D., *et al.,* «Construcción social de la realidad en los nativos digitales: una revisión teórica desde la perspectiva narrativa» (en línea), *Prisma Social. Revista de ciencias sociales*, núm. 3, junio 2010 Disponible en: https://www.researchgate.net/publication/277262741 Construccion social de la realidad en los nativos digitales Una revision teorica desde la perspertiva narrativa (consulta 4 de diciembre de 2018).

CALDEVILLA DOMINGUEZ, D., «Las Redes Sociales. Tipología, uso y consumo de las redes 2.0 en la sociedad actual» (en línea), *Documentación de las Ciencias de la Información,* núm. 33, 2010, pp. 45-68. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=3250105&orden=260817&info=link (consulta: 19 de junio de 2017).

CAMPOS ACUÑA, C., «El procedimiento administrativo electrónico en la Ley 39/2015», PINTOS SANTIAGO, J. (Dir.), *La implantación de la administración electrónica y de la e-factura,* Wolters Kluwer, Madrid, 2017, pp. 73-146. ISBN: 978-84-7052-730-2.

CARRILLO, M., «Los ámbitos del derecho a la intimidad en la sociedad de la comunicación», *XX Jornadas de la Asociación de Letrados del Tribunal Constitucional. El derecho a la privacidad en un nuevo entorno tecnológico.* Centro de Estudios Políticos y Constitucionales, Madrid, 2016, pp. 11-70, ISBN: 978-84-259-1703-5.

CEBRIÁN HERREROS, M., «La Web 2.0 como red social de comunicación e información», *Estudios sobre el mensaje periodístico,* núm. 14, 2008, pp. 345-361. ISSN 1134-1629.

CERRILLO I MARTÍNEZ, A., «Capítulo V. El gobierno abierto» (formato electrónico), CERRILLO I MARTÍNEZ, A. (Coord.), *A las puertas de la administración digital. Una guía detallada para la aplicación de las leyes 39/2015 y 40/2015*, Instituto Nacional de Administración Pública, Madrid, 2016, pp. 233. ISBN: 978-84-7351-562-7. NIPO: 635-16 -052-6.

CERRILLO I MARTÍNEZ, A., «Cooperación entre Administraciones públicas para el impulso de la administración electrónica», GAMERO CASADO, E. y VALERO TORRIJOS, J. (Coords.) *La Ley de administración electrónica. Comentario sistemático a la Ley 11/2007, de acceso electrónico de los ciudadanos a los servicios públicos*. Thomson-Aranzadi, Navarra, 2008, pp. 757-810.

CERRILLO I MARTÍNEZ, A., «El difícil equilibrio entre transparencia pública y protección de datos personales», *Cuadernos de derecho local*, núm. 45, 2017, pp. 127-156.

CERRILLO I MARTÍNEZ, A., «Transparencia y buen gobierno en las Administraciones locales de Cataluña: Una aproximación a la Ley 19/2014, de 29 de diciembre», VILLORIA MENDIETA, M. (Dir.), *Buen gobierno, transparencia e integridad institucional en el Gobierno Local.* Ed. Tecnos, Barcelona, 2015, pp. 80-104, ISBN: 978-84-9803-712-8.

CERVERA NAVAS, L., «Las instituciones y organismos europeos de protección de datos: El Supervisor Europeo y el Comité Europeo de Protección de Datos», *El Cronista del Estado Social y Democrático de Derecho,* mayo-junio 2020, núm. 88-89, pp. 104-115.

CORONA HERRERO, J. U., «Los datos en la nube: retos actuales en la protección del derecho de propiedad» (en línea), *Revista Aranzadi de Derecho y Nuevas Tecnologías,* núm. 32, mayo-agosto 2013 (consulta: 24 de octubre de 2017), BIB\2013\1644.

COTINO HUESO, L., «El reconocimiento y contenido internacional del acceso a la información pública como derecho fundamental», *Teoría y realidad constitucional*. Núm. 40, 2017, p. 279-316.

CUETO PÉREZ, M., «La organización de los Organismos Públicos de Investigación Estatales», DÍEZ BUESO, L., *La organización de la ciencia a revisión: Administración General del Estado, Cataluña, Madrid y País Vasco,* Huygens, 2020, pp. 11-52.

DARNACULLETA GARDELLA, M., «El Derecho Administrativo Global ¿Un nuevo concepto clave del Derecho Administrativo?» (en línea), *Revista de administración pública*, 2016, pp. 11-50, ISSN: 0034-7639 Disponible en: https://dialnet.unirioja.es/descarga/articulo/5492352.pdf (consulta: 7 de julio de 2019).

DÍAZ DÍAZ, E., «El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones». En Revista Aranzadi Doctrinal, nº 6 (parte Estudio), 2016, pp. 155-190.

DÍAZ PIRAQUIVE, F. N., JOYANES AGUILAR, L. y MEDINA GARCÍA, V. H., «Taxonomía, ontología y folksonomía, ¿qué son y qué beneficios u oportunidades presentan para los usuarios de la web» (en línea), *Universidad & Empresa*, núm. 16, vol. 11, 2009, pp. 242 - 261. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5096735.pdf (consulta y descarga: 27 de mayo de 2019).

DÍAZ REVORIO, F. J., «Los valores superiores del ordenamiento jurídico», PENDÁS, B. (Dir.), *España constitucional (1978-2018). Trayectorias y perspectivas,* Tomo III, Centro de Estudios Políticos y Constitucionales, Madrid, 2018, pp. 1749-1764.

DÍAZ VICARIO, A., FERNÁNDEZ DE ÁLAVA, M., y BARRERA-COROMINAS, A., «Creación y gestión del conocimiento en redes profesionales virtuales: Análisis de experiencias en empresas» (en línea), *Estilos de aprendizaje: investigaciones y experiencias: V Congreso Mundial de Estilos de Aprendizaje*, GUERRA LÓPEZ, F., GARCÍA RUIZ, R., GONZÁLEZ FERNÁNDEZ, N., RENÉS ARELLANO P., y CASTRO ZUBIZARRETA A (Coords.), Santander: 27, 28 y 29 de junio de 2012, pp. 10. Disponible en:

https://dialnet.unirioja.es/descarga/articulo/4664051.pdf (consulta: 10 de junio de 2019).

DOPAZO FRAGUÍO, P., «La protección de datos en el derecho europeo: principales aportaciones doctrinales y marco regulatorio vigente (Novedades del Reglamento General de Protección de Datos», *Revista Española de Derecho Europeo,* nº 68 (parte Estudios), 2018, pp. 113-148.

ESTRADA CORONA, A., «Protocolos TCP/IP de Internet» (en línea), *Revista Digital Universitaria*, México, 2004, vol. 5, núm. 8, pp. 1-7. ISSN 1067-6079. Disponible en: https://biblat.unam.mx/es/revista/revista-digital-universitaria/articulo/protocolos-tcpip-de-internet (consulta: 14 de mayo de 2018).

FERNÁNDEZ ACEVEDO, J., «Disposiciones relativas a situaciones específicas de tratamiento (Arts. 85-91 RGPD. Disposición adicional segunda y vigésimo segunda LOPDGDD), LÓPEZ CALVO, J. (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 715-755. ISBN: 978-84-9090-345-2.

FERNÁNDEZ, C. B. y MÉLER, N., «*Machine learning* para reconocimiento facial y otros ejemplos de los retos que supone la computación en la nube» (en línea), *Diario La Ley,* 28-06-2017 (consulta: 30 de octubre de 2017).

FERNÁNDEZ DE MARCOS, E. «La evaluación de impacto en protección de datos: aspectos de interés» (en línea), *Actualidad Administrativa,* Wolters Kluwer, nº 4, marzo, 2018 (consulta: 15 de diciembre de 2019).

FERNÁNDEZ NIETO, A. y RIVERO ORTEGA, R., «La administración sin papel: registro, expediente, archivo electrónico, ¿Estamos preparados?», *Revista Vasca de Administración Pública*, núm. 105, 2016, pp. 453-471. ISSN: 0211-9560.

FERNÁNDEZ RODRÍGUEZ, J. J., «Aproximación general a la reforma normativa: El Reglamento Europeo y la Ley Orgánica española. Principios generales», CAMPOS ACUÑA Mª C., *Aplicación práctica y adaptación de la protección de datos en el ámbito local. Novedades tras el RGPD y la LOPDGDD.* 2ª ed., Madrid, 2019, pp. 35-68. ISBN: 978-84-9052-472-1.

FERNÁNDEZ SALMERÓN, M. y VALERO TORRIJOS, J. «Las infracciones de las Administraciones Públicas», TRONCOSO REIGADA, A. (Dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal»*. Civitas-Thomson Reuters, Navarra, 2010, pp. 2187-2213, ISBN: 978-84-470-3423-9.

FERNANDO PABLO, M.M. y TERRÓN SANTOS, D., «Sobre la gobernanza de la Inteligencia Artificial» (versión electrónica), GUAYO CASTIELLA, I. DE y FERNÁNDEZ CARBALLAL, A. (Coords.), *Los desafíos del Derecho público en el siglo XXI. Libro conmemorativo del XXV Aniversario del acceso a la Cátedra del Profesor Jaime Rodríguez-Arana Muñoz,* Instituto de Administración Pública, Madrid, 2019, pp. 1019. ISBN: 978-84-7351-674-7. NIPO: 278-19-003-2.

FRÍAS, Z., PÉREZ, J. Y STECK, CH., «Gobernanza de Internet y derechos digitales», QUADRA-SALCEDO, T. Y PIÑAR MAÑAS, J. L. (Dirs.) *Sociedad digital y derecho*. B.O.E., Madrid, 2018, p. 533-552.

FONDEVILA ANTOLÍN, J., «Capítulo III. La Administración electrónica en la Ley 40/2015, de Régimen Jurídico del Sector Público», PINTOS SANTIAGO, J. (Dir.), *La implantación de la administración electrónica y de la e-factura*, Wolters Kluwer, Madrid, 2017, pp. 147-250. ISBN: 978-84-7052-730-2.

FROSINI, V., «Los derechos humanos en la era tecnológica», PÉREZ LUÑO, A. (Coord.), *Derechos humanos y constitucionalismos ente el tercer milenio*, Ed. Marcial Pons, Madrid, 1996, pp. 87-96. ISBN: 84-7248-394-0.

FUERTES, M., «Defensa de Derechos y neutralidad de la red», QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO T. DE LA y PIÑAR MAÑAS, J.L. (Dirs.), *Sociedad Digital y Derecho*, BOE, Madrid, 2018, p. 491-509.

FUERTES, M., «Soberanía digital europea», *El cronista del Estado Social y Democrático de Derecho,* núm. 90-91, diciembre 2020-enero 2021, 2021, pp.56-71. ISSN: 1889-0016.

GALINDO AYUDA, F. «Democracia, Internet y Gobernanza: una concreción». En *Seqüência: estudos jurídicos e políticos*. Brasil, vol. 33, núm. 65, 2012, p. 37-38. DOI: https://doi.org/10.5007/2177-7055.2012v33n65p33

GAMERO CASADO, E., «El Delegado de Protección de Datos en las Administraciones públicas: ombudsperson de los datos», JIMÉNEZ DE CISNEROS CID, F.J., *Homenaje al Profesor Ángel Menéndez Rexach*. Thomson Reuters-Aranzadi, Navarra, 2018, pp. 267-283. ISBN: 978-84-9197-653-0.

GAMERO CASADO, E., «Objeto y ámbito de aplicación de la ley 11/2007», MURILLO DE LA CUEVA, P.L. (Dir.), *La protección de datos en la administración electrónica,* Aranzadi, Navarra, 2009, pp. 109-146.

GAMERO CASADO, E., «Interoperabilidad y Administración electrónica: conéctese, por favor», *Revista de Administración pública.* Núm., 179, Madrid, 2009, pp. 291-332.

GARCÍA AREITO, L., «¿Web 2.0 vs Web 1.0?» (en línea), *Didáctica, Innovación y Multimedia,* núm. 10, 2007, pp. 8. Disponible en: https://www.raco.cat/index.php/DIM/article/view/76637/98327 (consulta: 30 de noviembre de 2018).

GARCÍA GUARDIA, Mª L., GARCÍA GARCÍA, F Y NÚÑEZ GÓMEZ, P., «Teorías sobre el hipertexto» (en línea), *Admira*, 1, pp. 142 – 154 Disponible en: https://idus.us.es/xmlui/handle/11441/76104 (consulta 4 de diciembre de 2018).

GARCÍA MARTÍNEZ, A. T., «Estructura Tecnológica e Institucional de Internet» (en línea), *Puertas a la lectura,* núm. 17, 2004, pp. 1-15. Disponible en https://dialnet.unirioja.es/descarga/articulo/1071306.pdf (consulta 3 de diciembre de 2018).

GARCÍA PÉREZ, C.L., «La responsabilidad civil de los medios de comunicación por vulneración del derecho al honor» (en línea), *Revista Doctrinal Aranzadi Civil-Mercantil*, núm. 1/2015, pp. 1-17 (consulta: 15 de enero de 2020). BIB 2015\716.

GARCÍA-ULL, F. J., «Las cookies en los principales cibermedios generalistas de España» (en línea), *Miguel Hernández Communication Journal*, núm. 4, artículo nº 11, 2013, pp. 233-261, Disponible en: https://revistas.innovacionumh.es/index.php/mhcj/article/view/52/102 (consulta: 31 de octubre de 2017).

GÓMEZ DEL CASTILLO SEGURADO, M.A., «Evolución de la Informática en el ámbito Educativo Español», *EA. Escuela abierta: revista de Investigación Educativa*, núm.4, 2001, pp.143-156. ISSN: 1138-6908.

GÓMEZ DÍAZ, D., «La historia económica en internet» (en línea), *Historia actual online,* núm. 3, 2003, pp. 91-124. Disponible en: https://dialnet.unirioja.es/descarga/articulo/829457.pdf (consulta: 23 de noviembre de 2017).

GONZÁLEZ MENDOZA, D. P., «Panorama jurídico actual sobre la elaboración de perfiles a partir de cookies y dirección IP», BUENO DE MATA, F. (Dir.). *Fodertics 7.0. Estudios sobre Derecho digital.* Comares, Granada, 2019, pp. 71-80. ISBN: 978-84-9045-765-8.

GUASP MARTÍNEZ, V., «Tratamientos concretos de datos personales en la LOPDGDD (Arts. 19-27 LOPDGDD)», LÓPEZ CALVO, J. (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 173-215. ISBN: 978-84-9090-345-2.

GUDÍN RODRÍGUEZ-MAGARIÑOS, F., «La lucha contra el ciberblanqueo como vía para acabar con el phishing» (en línea), *Revista Aranzadi Doctrinal* (estudios) núm. 9, 2014 (consulta: 6 de diciembre de 2018). BIB 2014\4287.

GUICHOT, E., «Aspectos constitucionales del derecho de la comunicación», GUICHOT, E. (Coord.), *Derecho de la Comunicación,* Ed. Iustel, *España*, 2011, pp. 304. ISBN 978-84-0890-163-4.

GUICHOT REINA, E., «Transparencia y protección de datos en las Universidades Públicas», *Revista Española de Derecho Administrativo.* Nº 193, pp. 85-126.

HENDRIX, P. y BIRKMIRE, M., *Adapting Web Browsers for Accessibility* (en línea), pp. 9 Disponible en: http://files.eric.ed.gov/fulltext/ED432102.pdf (consulta: 4 de junio de 2019).

HEREDERO CAMPO, Mª T., «WEB 2.0: Afectación de derechos en los nuevos desarrollos de la Web corporativa», *Cuadernos Red de Cátedras Telefónica*, n°6, mayo 2012, pp. 1-40. ISSN 2174-7628.

HERNÁNDEZ RAMOS, M., «El Derecho al olvido digital en la web 2.0» (en línea), *Cuaderno de Red de Cátedras Telefónica,* núm. 11, 2013, pp. 44 Disponible en: https://dialnet.unirioja.es/descarga/articulo/4498471.pdf (consulta y descarga: 26 de junio de 2017).

HUERGO LORA, A., «Peculiaridades de la potestad sancionadora en materia de protección de datos», *La potestad sancionadora de la Agencia Española de Protección de Datos*, Thomson Aranzadi-AEPD, Navarra, 2008, pp. 149-159. ISBN: 978-84-8355-894-2.

IGLESIA PRADOS, E. DE LA., «La responsabilidad de las redes sociales por la difusión de actos de vulneración del honor y la intimidad», CAPILLA RONCERO, F., *et al.* (Dir.), *Derecho digital y cuestiones actuales,* Aranzadi, 2018, pp. 203-220, ISBN: 978-84-9197-070-5.

IRURZUN MONTORO, F., «XXVII. Cooperación y coherencia entre autoridades de control», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2016, pp. 513-526.

ISLAS CARMONA, O., «Internet 2.0: El territorio digital de los prosumidores» (en línea), *Revista Estudios Culturales*, núm. 5, 2010, pp. 22. Disponible en: https://dialnet.unirioja.es/descarga/articulo/3739971.pdf (consulta: 6 de abril de 2019).

JOVE VILLARES, D., «Consecuencias en la ley de investigación biomédica del RGPD», *Revista General de Derecho Constitucional,* núm. 28, 2018, pp. 25.

JOYANES AGUILAR, L., «Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial, Industria 4.0 versus ciberseguridad 4.0» (en línea), *Cuadernos de estrategia*, núm. 185, 2017, pp. 19-64. ISSN: 1697-6924. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6115620.pdf (consulta 29 de noviembre de 2018).

KLEINWÄCHTER, W., «Good governance of the borderless Internet: Who should do what?» (en línea), *Telos,* núm. 80. Disponible en: https://telos.fundaciontelefonica.com/archivo/numero080/good-

governance-of-the-borderless-internet-who-should-do-what/ (consulta: 5 de julio de 2019).

KOBEISSI, N., «An Analysis of the ProtonMail Cryptographic Architecture» (en línea), *Cryptology ePrint Archive:Report 2018/1121.* Disponible en: https://eprint.iacr.org/2018/1121 (consulta: 18 de diciembre de 2018).

LLANEZA, P., «Capítulo 9. Dataísmo, transparencia y protección de datos», RODRÍGUEZ MARÍN, S. y MUÑOZ GARCÍA, A. (Coords.), *Aspectos legales de la economía colaborativa y bajo demanda en plataformas digitales,* Wolters Kluwer, 2018, pp. 199-219. ISBN: 978-84-9090-273-8.

LÓPEZ ÁLVAREZ, L. F., «Blockchain y protección de datos», LÓPEZ CALVO, J. (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp.1011-1031. ISBN: 978-84-9090-345-2.

LÓPEZ CALVO, J., «Cooperación y coherencia (Arts. 60-76. Arts. 60-62 LOPDGDD)», LÓPEZ CALVO, J., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Wolters Kluwer Bosch, España, 2019, pp. 637-661. ISBN: 978-84-9090-345-2.

LUCAS VERDÚ, P., «Sobre los valores» (en línea), *Teoría y realidad constitucional,* núm. 23, 2009, pp. 117-132. Disponible en: https://dialnet.unirioja.es/descarga/articulo/3003932.pdf (consulta: 17 de julio de 2019).

MARÍN JIMÉNEZ, R., «Evaluación de impacto en la Protección de Datos. Paralelismos» (en línea), *Revista de la Sociedad española de informática y salud*, núm. 134, abril 2019, pp. 24-26. Disponible en: https://seis.es/is-134-abril-2019/ (consulta 1 de enero de 2021).

MARTÍN DELGADO, I., «El acceso electrónico a los servicios públicos: hacia un modelo de administración digital auténticamente innovador», QUADRA-SALCEDO, T. DE LA y PIÑAR MAÑAS, J. L. (Dir.). *Sociedad digital y Derecho*. BOE, Madrid, 2018, p. 183.

MARTÍN DELGADO, I., «La configuración legal de las autoridades de transparencia», MARTÍN DELGADO, I., GUICHOT REINA, E. y CARRILLO I MARTÍNEZ, A., *Configuración legal, actuación y funciones de las autoridades de transparencia. Algunas*

propuestas de mejora, Ed. MIC, Barcelona, 2019, pp. 13-40, ISBN: 978-84-120267-1-9.

MARTÍNEZ AYUSO, M. Á., «Las redes P2P y la descarga ilegal de contenidos» (en línea), *Revista Aranzadi de Derecho de Deporte y Entretenimiento,* núm. 18/2006, 3 parte secciones, pp. 18 (consulta: 5 de noviembre de 2018). BIB 2006\1788.

MARTÍNEZ GUTIÉRREZ, R., «El régimen jurídico de la Administración digital: aspectos procedimentales», MARTÍN DELGADO, I. (Dir.), *El procedimiento administrativo y el régimen jurídico de la Administración pública desde la perspectiva de la innovación*, Iustel, Madrid, 2020, pp. 143-223. ISBN: 978-84-9890-394-2.

MATE SATUÉ, L.C., «¿Qué es realmente el Derecho al Olvido?» (en línea), *Revista de Derecho Civil*, núm. 2, vol. 3, (abril-junio), 2016, pp. 187-222. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5560514&orden=0&info=link (consulta: 26 de junio de 2017).

MARTÍNEZ CABALLERO, J., «Cómo conjugar el derecho al olvido», *Revista Jurídica de Castilla-La Mancha*, núm. 57, 2015, pp. 143-185. ISSN 0213-9995.

MEDINA GUERRERO, M., «Capítulo VII. Categorías especiales de datos», RALLO LOMBARTE, A. (Dir.), *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales*, Tirant lo blanch, Valencia, 2019, pp. 251-273.

MEDINA VARGAS, Y. T. Y MIRANDA MNEDEZ, H. A., «Comparación de algoritmos basados en la criptografía simétrica DES, AES y 3DES» (en línea), *Mundo FESC,* vol. 5, núm. 9, 2015, pp. 14-21. ISSN-e: 2216-0388. Disponible en: https://dialnet.unirioja.es/descarga/articulo/5286657.pdf (consulta: 10 de enero de 2019).

MELL P. and GRANCE, T., «The NIST defination of Cloud Computing»(en línea), *National Institute os Standars and Technology- Departament of Commerce, USA,* Special Publication 800-145, September, 2011, pp. 3. Disponible en: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf (consulta: 7 de junio de 2019).

MENÉNDEZ, L., «¿Qué son las cookies?», *Escritura Pública* (en línea), núm. 82, julio-agosto 2013, pp. 16-18. Disponible en: http://www.notariado.org/liferay/c/document_library/get_file?folderId=12092&name=DLFE-110181.pdf (consulta: octubre de 2016).

MENÉNDEZ SEBASTIÁN, E. Mª, «El contrato de servicios», GIMENO FELIU, J. M. (Dir.), *Estudio sistemático de la Ley de Contratos del Sector Público* (en línea), Thomson Reuters Aranzadi, 2018 Disponible en: https://proview.thomsonreuters.com (consulta: 30 de octubre de 2020).

MENON, S., *et al*., «Progression of Web 3.0 (semantic Web) from Web 1.0: A survey» (en línea), 2009, pp.5 Disponible en: https://www.researchgate.net/publication/305443181_PROGRESSION_OF_WEB_30SEMANTIC_WEB_FROM_WEB_10_A_SURVEY (Consulta: 17 de mayo de 2018).

MESEGUER YEBRA, J. y IBÁÑEZ PASCUAL, A., «Capítulo I. Transparencia y acceso a la información pública en el nuevo contexto de la administración electrónica», PINTOS SANTIAGO, J. (Dir.), *La implantación de la Administración electrónica y de la e-factura,* Wolters Kluwer, Madrid, 2017, pp. 19-71. ISBN: 978-84-7052-730-2.

MIGUEL ASENCIO, P. A. DE., «Caracterización y organización de Internet: perspectiva jurídica» (en línea), *Derecho Privado de Internet.* Aranzadi, enero, 2015 (consulta 14 de diciembre de 2018). BIB 2015\8.

MOINE, J. M., HAEDO, A. S. y GORDILLO, S. E., «Estudio comparativo de metodologías para minería de datos» (en línea), *XIII Workshop de Investigadores en Ciencias de la Computación: mayo 2011,* pp. 278-281. Disponible en: http://sedici.unlp.edu.ar/handle/10915/20034.(consulta 5 de diciembre de 2018).

MORENO PÉREZ, J. L., «El pensamiento político-jurídico de Durkheim: solidaridad, anomia y democracia (I)» (en línea), *Revista de derecho constitucional europeo,* núm. 10, 2008, pp. 387-434. Disponible en:

https://dialnet.unirioja.es/descarga/articulo/3014022.pdf (consulta: 22 de enero de 2018).

NAIK, U. y SHIVALINGAIAH, D., «Comparative Study of Web 1.0, Web 2.0 and 3.0» (en línea), pp. 12. Disponible en: DOI: 10.13140/2.1.2287.2961 (consulta 27 de noviembre de 2018).

NEIRA BARRAL, D., «Autoridades de control en el nuevo Reglamento General de Protección de Datos 2016/679 y la Ley Orgánica 3/2018», CAMPOS ACUÑA, C. (Dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local,* Segunda edición, Wolters Kluwer, 2019, pp. 688. ISBN: 9788470524721.

NÚÑEZ GARCÍA, J., L., «El encargado del tratamiento», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad*, Reus, Madrid, 2011, pp. 321-334. ISBN: 978-84-290-1936-0.

O´CALLAGHAN MUÑOZ, X., «Personalidad y derechos de la personalidad (honor, intimidad, imagen) del menor, según la Ley de Protección de Menor», *La Ley: Revista jurídica española de doctrina, jurisprudencia y bibliografía,* núm. 4, 1996, pp.1247- 1251.

OEHLING DE LOS REYES, A., «El concepto constitucional de dignidad de la persona: Forma de comprensión y modelos predominantes de recepción en la Europa continental», *Revista Española de Derecho Constitucional*, Centro de Estudios Políticos y Constitucionales. Madrid, 2011, pp. 135-178.

ORTEGA DOMÉNECH, J., «La difícil convivencia del derecho de cita en el mundo de los enlaces digitales», *Anuario de Propiedad intelectual*. Núm. 2011, 2012, pp. 417-476. ISSN: 1889-724X.

PANEA MÁRQUEZ, J. M., «La imprescindible dignidad», RUIZ DE LA CUESTA, A. (Coord.), *Bioética y derechos humanos: implicaciones sociales y jurídicas*, Universidad de Sevilla, España, 2005, p. 17- 28.

PASCUAL MEDRANO, A., «La dignidad humana como principio jurídico del ordenamiento constitucional español», CHUECA, R. (coord.), *Dignidad humana y derecho fundamental*, Centro de Estudios Políticos y Constitucionales, Madrid, 2015, pp. 295-333.

PEMÁN GAVÍN, J. M., «Lección 1. El Derecho administrativo en España. Una introducción», MENÉNDEZ, P. y EZQUERRA, A. (Dirs.), *Lecciones de Derecho administrativo,* Thomson Reuters Civitas, 2019, pp. 51-97. ISBN: 978-84-9197-970-8.

PÉREZ LUÑO, A. E., «Impactos sociales y jurídicos de Internet» (en línea), *Argumentos de razón técnica: revista española de ciencia, tecnología y sociedad y filosofía de la tecnología*, núm. 1, pp. 33-48. Disponible en: https://idus.us.es/xmlui/handle/11441/57678 (consulta: 11 de enero de 2019).

PÉREZ VELAZCO, M. M., «Intercambio de datos entre administraciones públicas», *IDP: revista de Internet, derecho y política. Revista d'Internet, dret i política*, núm. 2, 2006, pp. 45-51. ISSN: 1699-8154.

PIÑAR MAÑAS, J. L., «Identidad y persona en la sociedad digital», QUADRA-SALCEDO, T. y PIÑAR MAÑAS, J. L. (Dirs.), *Sociedad digital y derecho*. B.O.E., Madrid, 2018, pp. 95-111.

PIÑAR MAÑAS, J. L., «I. Introducción. Hacia un nuevo modelo europeo de protección de datos», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos Personales. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2016, pp. 15-22. ISBN: 978-84-290-1936-0.

POMMI, S., *et al*., «Social Networking Websites» (en línea), 2011, pp. 10. Disponible en: http://14.139.186.108/jspui/bitstream/123456789/2760/1/pommi.pdf (consulta octubre 2016).

POVEDANO ALONSO, D., «Capítulo 11. Especialidades del DPO en el ámbito local: un enfoque práctico», CAMPOS ACUÑA, C. (Dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, Segunda edición, Wolters Kluwer, 2019, pp. 423-449. ISBN: 978-84-7052-472-1.

PRIETO ÁLVAREZ, T., «Luces y sombras de la integración europea en derechos de la persona. En particular, en riesgo de que la base del sistema jurídico se traslade desde la dignidad humana a la autonomía personal», LAGUNA DE LA PAZ, J. C., SANZ RUBIALES, I. Y MOZOS Y TOUYA, I. M. DE LOS (Coords.), *Derecho*

administrativo e integración europea. Estudios homenaje al Profesor José Luis Martínez López-Muñiz, Madrid, Reus, 2017, pp. 187-206.

PRIETO SERRANO, R., «Internet», *Ciencia e Ingeniería Neogranadina*, núm. 1, Vol. 4, 1996, p. 9-18. ISSN-E: 0124-8170.

PUENTE, A., «El derecho al olvido», PÉREZ BES, F. (Coord.), *El derecho de Internet,* Atelier libros jurídicos, 2016, pp. 181-224. ISBN: 978-84-16652-07-5.

PUYOL MONTERO, J., «IX. Los principios del Derecho a la protección de datos», PIÑAR MAÑAS, J.L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad*, Reus, 2016, pp. 135-150. ISBN: 978-84-290-1936-0.

RALLO LOMBARTE, A., «El Derecho al olvido y su protección a partir de la protección de datos», *Telos: Cuadernos de comunicación,* núm. 85, 2010, pp. 104-108. ISSN: 0213-084X.

RAZQUIN LIZARRAGA, M. M., «El necesario equilibrio entre transparencia y protección de datos personales», ZEGARRA VALDIVIA, D. La proyección del Derecho Administrativo Peruano. Ed. Palestra, Lima, 2019, pp.137-164. ISBN: 978-612-325-091-1.

REBOLLO DELGADO, L., «Derechos de la personalidad y los datos personales», *Revista de Derecho Político*, núm. 44, 1998, pp. 146-206.

RECARTE PÉREZ, J. M., «Diseccionando la red Tor» (en línea), *Quadernos de criminología: revista de criminología y ciencias forenses*, núm. 41, 2018, pp. 46-52 Disponible en: https://dialnet.unirioja.es/descarga/articulo/6478986.pdf (consulta: 11 de diciembre de 2018).

RECIO GAYO, M., «XXII. El Delegado de Protección de Datos», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo de privacidad,* Reus, Madrid, 2016, pp. 367-387. ISBN: 978-84-290-1936-0.

RIBES I GUÀRDIA, F. X., «El valor de los metadatos y de la inteligencia colectiva» (en línea), *Telos* Disponible en: https://telos.fundaciontelefonica.com/archivo/numero073/el-valor-de-los-

metadatos-y-de-la-inteligencia-colectiva/ (consulta 30 de noviembre de 2018).

RIQUELME, J. C., RUÍZ, R. Y GILBERT, K., «Minería de Datos: Conceptos y Tendencias» (en línea), *Inteligencia Artificial. Revista Iberamericana de Inteligencia Artificial,* vol. 10, núm. 29, 2006, pp. 11-18 Disponible en: https://www.redalyc.org/pdf/925/92502902.pdf (consulta y descarga: 5 de diciembre de 2018).

RIVAS LÓPEZ, J.L., «Auditoría y seguridad de datos: Análisis de riesgos», CAMPOS ACUÑA, C., *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, segunda edición, Wolters Kluwer, 2019, p. 641-678.

RODRÍGUEZ-AMAT, J. R., *et al.,* «Gobernanza de Internet y libertad de expresión», CORREDOIRA Y ALFONSO, L. y COTINO HUESO, L. (Dirs.), *Libertad de expresión e información en Internet: amenazas y protección de los derechos personales,* Centro de Estudios Políticos y Constitucionales, 2013, pp.75-98. ISBN:978-84-259-1561-1.

RODRÍGUEZ DE LAS HERAS BALLELL, T., «La responsabilidad por «software» defectuoso en la contratación mercantil» (en línea), *Revista Aranzadi de Derecho y Nuevas Tecnologías.* Núm. 10, 2006-1, parte Doctrina (consulta: 10 de diciembre de 2018). BIB 2006\108.

RODRÍGUEZ RAPOSO, A., «Los nombres de dominio de internet: Presente y futuro de la situación de España» (en línea), *Economía industrial*, núm. 338, 2001, pp. 71-78 Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=266339&orden=197762&info=link (consulta: 14 de noviembre de 2018).

ROLLNERT LIERN, G., «El derecho de acceso a la información pública como derecho fundamental: una valoración del debate doctrinal a propósito de la Ley de Transparencia», *Teoría y realidad constitucional,* núm. 34, 2014, pp. 349-368.

ROMEO RUÍZ, A., «La responsabilidad proactiva de las administraciones públicas en protección de datos personales» (en línea), *Revista Vasca de Gestión de Personas y Organizaciones Públicas,* núm. 18, 2020, pp. 146. Disponible en: https://www.ivap.euskadi.eus/contenidos/informacion/18_revgp/eu_def/Romeo_138_153.pdf (consulta: 1 de enero de 2021).

ROMEO RUIZ, A., «Conflictos entre protección de datos personales y publicidad activa sobre retribuciones de empleados públicos. A propósito de la Sentencia de la Audiencia Nacional 2386/2019, de 26 de marzo de 2019», *Revista Vasca de Administración Pública*, núm. 116, enero-abril, 2020, pp. 191-210.

ROUVROY, A., «Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?, *La sécurité de l'individu numérisé. Réflexions prospectives et internationales*» (en línea), 2008, pp. 34 Disponible en: https://works.bepress.com/antoinette_rouvroy/5/(consulta: 19 de junio de 2016).

RUBÍ NAVARRETE, J., «La Agencia Española de Protección de Datos», RALLO LOMBARTE, A. (Dir.), *Tratado de protección de datos. actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*», Tirant lo Blanch, Valencia, 2019, pp. 491-520.

RUBÍ NAVARRETE, J., «La Agencia Española de Protección de Datos Personales», *El Crónista del Estado Social y Democrático de Derecho,* mayo-junio 2020, núm. 88-89, pp. 96-103.

RUÍZ-GIMÉNEZ CORTÉS, J. y RUÍZ-GIMÉNEZ ARRIETA, I., «El artículo 10 Derechos Fundamentales de la persona», ALZAGA VILLAAMIL, O. (Coord.). *Comentarios a la Constitución Española de 1978,* Tomo II, De derecho reunidas, Madrid, 1997, pp. 37-107.

SÁNCHEZ ORS, C., «Capítulo 20. El Delegado de Protección de Datos (Arts. 37-39 RGPD. Arts. 34-37 LOPDGDD», LÓPEZ CALVO, J. (Coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD,* Wolters Kluwer, Madrid, 2019, pp. 493- 548. ISBN: 978- 84-9090-346-9.

SANCHIS CRESPO, C., «La tutela judicial del derecho al honor, Internet y la blogosfera», *Diario La Ley*, núm. 8035, sección Doctrina, 4 de marzo de 2013, pp. 22.

SANZ MARCO, LL., «Capítulo 8. Medidas organizativas para la implantación del marco legal de protección de datos personales. El registro de actividades de tratamiento», CAMPOS ACUÑA, C. (Dir.), *Aplicación práctica y adaptación de la protección de datos en el ámbito local*, Segunda edición, Wolters Kluwer, 2019, pp. 321-341. ISBN: 978-84-7052-477-6.

SENSO RUÍZ, J. A., «Navegadores semánticos o semantizar el navegador» (en línea), *Anuario ThinkEPI,* 2008, pp. 30-33. Disponible en: https://recyt.fecyt.es/index.php/ThinkEPI/article/download/32033/17026 (consulta: 10 de diciembre de 2018).

SERENO RESTREPO, J. S., «Contenido generado por usuarios (ugc), Wikies, y derecho de autor» (en línea), *Revista La Propiedad Inmaterial,* Universidad Externado de Colombia, noviembre 2010, pp. 209-260, disponible en: https://revistas.uexternado.edu.co/index.php/propin/article/view/2480 (consulta: 28 de mayo de 2019).

SERRANO-COBOS, J., «Big data y not so big data» (en línea), *Anuario ThinkEPI*, v. 7, 2013, pp. 161-163. Disponible en: https://dialnet.unirioja.es/descarga/articulo/4234739.pdf (consulta y descarga: 10 de junio de 2019).

SIMÓN CASTELLANO, P., «La protección de datos en el sector público: efectos y transformaciones tras la LOPDGDD», *Actualidad Administrativa* (en línea), núm. 9, septiembre 2020. Disponible en: smateca.es (consulta: 4 de enero de 2020).

SOUVIRÓN MORENILLA, J.M., «Consideraciones sobre la función estadística pública» (en línea), *Revista de Administración Pública,* núm. 134, mayo-agosto, 1994, pp. 425-469. ISSN: 1989-0656.

SUÁREZ VILLEGAS, J.C., «El derecho al olvido, base de tutela de la intimidad. Gestión de los datos personales en la Red» (en línea), *Telos: Cuadernos de comunicación e innovación*, núm. 97, (febrero-mayo) 2014. Disponible en: https://telos.fundaciontelefonica.com/url-direct/pdf-generator?tipoContenido=articuloTelos&idContenido=2014042310020002&idioma=es(consulta: 19 de junio de 2017).

SWAN, M., «Blockchain Temporality: Smart Contract Time Specifiability with Blocktime» (en línea), *Springer International Publishing Switzerland 2016*, p. 186. DOI: 10.1007/978-3-319-42019-6_12.

TERWANGNE, C. DE, «Privacidad en Internet y el derecho a ser olvidado/derecho al olvido» (en línea), I*DP: Revista de Internet, Derecho y Política*, núm. 13, 2012, pp. 53-66 Disponible en: https://www.raco.cat/index.php/IDP/article/view/251842/337491 (consulta: 22 de noviembre de 2020).

TOLIVAR ALAS, L., «¿Debe sustantivarse el derecho al nombre en la constitución? Reflexiones sobre el *Ius nomine* y el deber de identificación», BAÑO LEÓN, J. Mª (Coord.), *Memorial para la reforma del Estado. Estudios en homenaje al Profesor Santiago Muñoz Machado,* Tomo I, Centro de Estudios Políticos y Constitucionales, Madrid, 2016, pp. 497-514. ISBN: 978-84-259-1694-6.

TOLIVAR ALAS, L., «Leyes Orgánicas», PENDÁS, B. (Dir.), *España Constitucional (1978-2018) Trayectorias y perspectivas*, Tomo III, Centro de Estudios Políticos y Constitucionales, Madrid, 2018, pp. 2033-2050. ISBN: 978-84-259-1963-9.

TRIGO ARANDA, C., «Historia y evolución de Internet» (en línea), *Manual formativo de acta*, núm. 33, 2004, págs. 1-11 Disponible en: http://www.acta.es/medios/articulos/comunicacion_e_informacion/033021.pdf(consulta: 23 de noviembre de 2017).

TRONCOSO REIGADA, A., «Las agencias de protección de datos como administración independiente», PAUNER CHULVI, C. y TOMÁS MALLÉN, B. (Coords.), *Las Administraciones independientes,* Tirant lo Blanch, Valencia, 2009, p. 27-216.

TRONCOSO REIGADA, A., «XXVI. Autoridades de control independientes», PIÑAR MAÑAS, J. L. (Dir.), *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de privacidad,* Reus, Madrid, 2016, pp. 461-512. ISBN: 978-84-290-1936-0.

VALCÁRCEL ASENCIOS, V., «Data Mining y el descubrimiento del conocimiento» (en línea), *Indutrial Data,* núm. 2, vol. 7, julio-diciembre 2004, pp. 83-86. Disponible en: https://www.redalyc.org/pdf/816/81670213.pdf (consulta 5 de diciembre de 2018).

VALERO TORRIJOS, J., «Acceso a los servicios y a la información por medios electrónicos», VALERO TORRIJOS, J. y GAMERO CASADO, J. (Coords.), *La ley de Administración electrónica. Comentario sistemático a la Ley 11/2007, de 22 de*

junio, de acceso electrónico de los ciudadanos a los servicios públicos, Thomson Reuters Aranzadi, Madrid, 2008, pp. 345-414. ISBN: 978-84-9903-707-3.

VALERO TORRIJOS, J., «Implicaciones de la protección de datos de carácter personal para la Administración electrónica», *La protección de datos en la Administración electrónica*, Navarra, 2009, pp. 177-198.

VALÍN LÓPEZ, M., «Las autoridades autonómicas de protección de datos», RALLO LOMBARTE, A. (Dir.), *Tratado de protección de datos. actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales*, Tirant lo blanch, Valencia, 2019, pp. 521-547.

VALERO TORRIJOS, J., «Protección de datos de carácter personal, datos abiertos y reutilización de la información del sector público», MARTÍN DELGADO, I. (Dir.), *El procedimiento administrativo y el régimen jurídico de la Administración pública desde la perspectiva de la innovación*, Iustel, Madrid, 2020, pp. 417-447. ISBN: 978-84-9890-394-2.

VANDER WAL, T., «Folksonomy, presented: online information», London, 30 December 2005 (en línea), pp. 13. Disponible en: http://vanderwal.net/essays/051130/folksonomy.pdf (consulta: 1 de diciembre de 2020).

VERGÉS RAMÍREZ, S., «La dignidad del hombre según Kant», *Letras de Deusto*, núm. 42, vol. 18, pp. 5-20. ISSN: 0210-3516.

VIDAL MARÍN, T., «Derecho al honor, personas jurídicas y tribunal constitucional» (en línea), *Indret: Revista para el Análisis del Derecho,* 2007, núm. 1, pp. 18. Disponible en: http://www.indret.com/pdf/397_es.pdf

VILLAR PALASÍ, J.L., «Nombres de dominio y Protocolo de internet», CREMADES, J., FERNÁNDEZ-ORDÓNEZ, M. Á. Y ILLESCAS, R. VILLAR PALASÍ, J.L., *Régimen jurídico de Internet* (Coords.), Ed. La ley, Madrid, 2002, pp. 393-406. ISBN: 84-9725-147-4.

VILLORIA MENDIETA, M. y CRUZ-RUBIO, C.N., «Gobierno abierto, transparencia y rendición de cuentas: marco conceptual», VILLORIA MENDIETA, M. (Dir.), *Buen*

gobierno, transparencia e integridad institucional en el Gobierno Local, Ed. Tecnos, Barcelona, 2015, pp. 80-104, ISBN: 978-84-9803-712-8.

VILLAVERDE MENÉNDEZ, I., «El marco constitucional de la transparencia», *Revista Española de Derecho Constitucional*, núm. 116, 2019, pp. 167-191. DOI: https://doi.org/10.18042/cepc/redc.116.06

VILLAVERDE MENÉNDEZ, I., «La intimidad, ese "terrible derecho" en la era de la confusa publicidad virtual» (en línea), *Espaço Jurídico: Joural of Law,* vol. 14, núm. 13, pp. 57-72 Disponible en: https://dialnet.unirioja.es/descarga/articulo/4546679.pdf (consulta: 10 de septiembre de 2019).

WARREN, S. D. y BRANDEIS, L. D., «The right to privacy», *Harvard Law Review,* Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220.

OTROS DOCUMENTOS.

AEPD

AEPD, «*Código de buenas prácticas en protección de datos para proyectos Big Data*» (en línea), pp. 40. Disponible en: https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf (consulta: 10 de junio de 2019).

AEPD, «*Declaración sobre buscadores de Internet*», 2007, pp. 15. Disponible en: https://www.facua.org/es/documentos/declaracionsobrebuscadoresdeinternet.pdf (consulta: 26 de junio de 2017).

AEPD, «*El Delegado de Protección de Datos en las Administraciones públicas*»(en línea), pp.4. Disponible en: https://www.aepd.es/sites/default/files/2019-09/funciones-dpd-en-aapp.pdf (consulta: 20 de septiembre de 2020).

AEPD, «*Esquema de certificación de Delegados de protección de datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD)*», 2019, pp. 79. Disponible en: https://www.aepd.es/sites/default/files/2020-07/esquema-aepd-dpd.pdf (consulta: 4 de mayo de 2020).

AEPD, «*Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD*», pp. 42. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf (consulta: 30 de noviembre de 2020).

AEPD, «*Guía orientaciones y garantías en los procedimientos de anonimización de datos personales*», 2016, pp. 28. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-orientaciones-procedimientos-anonimizacion.pdf (consulta: 30 de noviembre de 2020).

AEPD, «*Guía para clientes que contraten servicios de Cloud Computing*» (en línea). 2018, pp. 25. Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-cloud-clientes.pdf (consulta: 8 de octubre de 2020).

AEPD, «*Guía Protección de datos y Administración Local*», Disponible en: https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf (consulta: 22 de septiembre de 2020).

AEPD, «*Guía sobre el uso de las cookies*», julio 2020, pp. 39. Disponible en: https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf (consulta: 29 de julio de 2020).

AEPD, Informe 170/2018, pp. 16. Disponible en: https://www.aepd.es/es/documento/2018-0170.pdf (consulta 31 de diciembre de 2020).

AEPD, Informe 175/2018, pp.24. Disponible en: https://www.aepd.es/es/documento/2018-0175.pdf (consulta: 29 de julio de 2020).

AEPD, «*Lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos según el art. 35.5 RGPD*», pp. 2. Disponible en: https://www.aepd.es/sites/default/files/2019-09/ListasDPIA-35.5l.pdf (consulta: 11 de noviembre de 2020).

AEPD, «*Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)*», pp.4. Disponible en: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf (consulta: 11 de noviembre de 2020).

AEPD, «*Listado de cumplimiento normativo*», pp. 13. Disponible en:https://www.aepd.es/sites/default/files/2019-11/guia-listado-de-cumplimiento-del-rgpd.pdf (consulta: 11 de noviembre de 2020).

AEPD, «*Recomendaciones dirigidas a usuarios de internet*» (en línea). Disponible en: https://www.unirioja.es/servicios/si/seguridad/concienciacion/RecomendacionesAGPD.pdf (consulta y descarga: 7 de junio de 2019).

AEPD, «*Tecnologías y protección de datos en AA.PP.*», pp. 60. Disponible en: https://www.aepd.es/sites/default/files/2020-11/guia-tecnologias-admin-digital.pdf (consulta: 8 de enero de 2021).

CEPD

CEPD, Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia, 21 de abril de 2020,

versión 1.1 (5 de mayo de 2020). Disponible en: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_es.pdf (consulta: junio de 2020).

Comisión Europea

Comisión de las Comunidades Europeas, «Propuesta de Directiva del Consejo, relativa a la protección de las personas en lo referente al tratamiento de datos personales», COM (90) 314 final, de 24 de septiembre de 1990, pp.30. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:1990:0314:FIN (consulta: 15 de abril de 2020).

Comunicación de la Comisión al Consejo, al Parlamento Europeo, al Comité Económico y Social Europeo y al Comité de las Regiones, «El papel de la administración electrónica en el futuro de Europa», COM(2003) 567 final, pp. 27. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52003DC0567&from=ES (consulta: 30 de noviembre de 2020).

Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, «Marco Europeo de Interoperabilidad – Estrategia de aplicación», COM (2017) 134 final, de 23 de marzo de 2017, pp. 10. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2017:134:FIN (consulta: 8 de enero de 2021).

Commission Staff Working Paper, *Impact Assessment,* /* SEC/2012/0072 final */. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52012SC0072 (consulta: 30 de abril de 2020).

Informe de la Comisión al Parlamento Europeo y al Consejo sobre la aplicación, funcionamiento y eficacia del dominio de primer nivel «.eu», de 18 de diciembre de 2015 –COM (2015) 680 final–. Disponible en: http://ec.europa.eu/transparency/regdoc/rep/1/2015/ES/1-2015-680-ES-F1-1.PDF (consulta: 11 de julio de 2019).

Consejo de Europa

Consejo de Europa, Cuadro de firmas y ratificaciones del Convenio 108 para la protección de las personas con respecto al tratamiento automático de sus datos personales. Disponible en:

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=BaeKoI48 (consulta: 6 de octubre de 2020).

Consejo de la Unión Europea

Council of the European Union, Brussels, 10 July 2018, Interinstitutional File: 2017/0003(COD), pp. 25. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_10975_2018_INIT&from=EN (consulta: 21 de diciembre de 2020).

GT29

Dictamen 1/2008 sobre cuestiones de protección de datos relacionadas con motores de búsqueda emitido el 4 de abril de 2008, del Grupo de Trabajo sobre Protección de Datos del Art. 29 (00737/ES WP148).

GT29, Dictamen 5/2009 sobre las redes sociales en línea adoptado el 12 de junio de 2009 (01189/09/ES WP 13).

GT29, Dictamen 1/2010 sobre los conceptos de "responsable del tratamiento" y "encargado del tratamiento", adoptado el 16 de febrero de 2010 (00264/10/ES WP 169).

GT29, Dictamen 2/2010 sobre publicidad comportamental en línea, adoptado el 22 de junio 2010 (00909/10/ES).

GT29, Dictamen 4/2012 sobre la exención del requisito de consentimiento de *cookies*, adoptado el 7 de junio de 2012 (00879/12/ES).

GT29, Dictamen 05/2014 sobre técnicas de anonimización, de 10 de abril de 2014 (0829/14/ES WP216).

GT29, Directrices para determinar la autoridad de control principal de un responsable o encargado del tratamiento, de 13 de diciembre de 2016, versión revisada y adoptada de 5 de abril de 2017 (16/ES/WP 244 rev.01).

GT29, Directrices sobre el consentimiento en el sentido del Reglamento (UE)2016/679, 2017, de 28 de noviembre de 2017, versión revisada y adoptada de 10 de abril de 2018 (17/ES/WP259 y rev.01).

GT29, Directrices sobre los delegados de protección de datos (DPD), de 13 de diciembre de 2016, versión revisada y adoptada de 5 de abril de 2017 (16/ES/WP 243 rev.01).

GT29, Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679, de 4 de abril de 2017, versión revisada y adoptada de 4 de octubre de 2017 (17/ES/ WP 248 rev.01).

ICANN

ICAAN, Articles of incorporation Public Technical Identifiers. Disponible en: https://pti.icann.org/iana_pti_docs/141-articles-of-incorporation-v-09aug16 (consulta: 10 de julio de 2019).

ICAAN, Las funciones de la IANA. Una introducción a las funciones de la Autoridad de Números Asignados en Internet (IANA), pp. 22. Disponible en: https://www.icann.org/es/system/files/files/iana-functions-18dec15-es.pdf (consulta: 9 de julio de 2019).

OMPI

OMPI, La gestión de los nombres y direcciones de internet: cuestiones de propiedad intelectual (en línea), 30 de abril de 1999, pp. 125. Disponible en: http://www.wipo.int/export/sites/www/amc/es/docs/report.pdf (consulta: 28 de noviembre de 2017).

ONTSI

ONTSI, Estudio sobre el conocimiento y uso de las redes sociales en España (en línea), diciembre 2011, pp. 173. Disponible en: https://www.ontsi.red.es/ontsi/sites/ontsi/files/redes_sociales-documento_0.pdf (consulta: 6 de abril de 2019).

ONTSI, Perfil sociodemográfico de los internautas. Análisis de datos, INE 2019, pp.45. Disponible en: https://www.ontsi.red.es/sites/ontsi/files/2020-06/PerfilSociodemograficoInternautas2019.pdf (consulta y descarga: 29 de julio de 2019).

Parlamento Europeo

Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la

protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM (2012)0011 – C7-0025/2012 – 2012/0011(COD)), Procedimiento legislativo ordinario: primera lectura, Disponible en: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//ES (consulta 17 de octubre de 2019).

Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Brussels, 4 November 2020 (OR. en) 9931/20. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52017PC0010 (consulta: 20 de diciembre de 2020).

RECURSOS EN LÍNEA Y ENLACES WEB.

Academia.edu, About Academia. Disponible en: https://www.academia.edu/about (consulta: 6 de abril de 2019).

Adobe, Cómo compartir archivos PDF y revisarlos en línea. Disponible en: https://acrobat.adobe.com/es/es/acrobat/how-to/share-pdf-online.html (consulta: 6 de junio de 2019).

AEPD, Derecho de supresión ("al olvido"). Disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-supresion-al-olvido (consulta: 19 de junio de 2017).

AEPD, Información de carácter institucional, organizativa y de planificación. Disponible en: https://www.aepd.es/es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/organigrama-AEPD/la-directora (consulta 15 de noviembre de 2020).

AGEA LÓPEZ, E., ALCARAZ ESPÍN, J. J. Y GARCÍA HARO, J., Propuesta de Trabajos de Practicas: Simulación de los mecanismos de control de congestión en TCP/IP (en línea). *Escuela Politécnica de Cartagena, Escuela Técnica Superior de Ingeniería de Telecomunicación*, pp. 24 Disponible en: http://www.upct.es/~orientap/TCP.pdf (consulta 14 de diciembre de 2018).

Boletín de Jurisprudencia Constitucional, IV Jurisprudencia Constitucional Extranjera «Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983 (versión traducida al Castellano)». Disponible en: https://www.u-cursos.cl/derecho/2008/0/DIPDERINFO/1/material_docente/bajar?id_material=163485 (consulta: 26 de junio de 2017).

Box, File transfer. Disponible en: https://www.box.com/es-es/file-transfer (consulta: 6 de junio de 2019).

Cambridge Dictionary, término «Snap». Disponible en: http://dictionary.cambridge.org/es/diccionario/ingles-espanol/snap (consulta: 14 de junio de 2017).

Centro Criptológico Nacional, Ficha técnica (AMPARO). Disponible en: https://www.ccn-cert.cni.es/pdf/documentos-publicos/4262-datasheet-amparo.html (consulta: 9 de enero de 2021).

Clave permanente, Requisitos de seguridad las contraseñas. Disponible en: https://clave.gob.es/clave_Home/Clave-Permanente/Seguridad.html (consulta: 3 de octubre de 2020).

Comisión Europea 2012 (consulta: 15 de junio de 2017). Disponible en http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf

Council of European National Top-Level Domain Registries, About. Disponible en: https://centr.org/about/about-centr.html (consulta: 13 de noviembre de 2018).

Cumbre mundial sobre la sociedad de la información. Disponible en: https://www.itu.int/net/wsis/index-es.html (consulta: 1 de diciembre de 2020).

Dle, «dignidad». Disponible en: https://dle.rae.es/?id=DlX5ZXZ (consulta: 1 de septiembre de 2019).

Dle, «digno». Disponible en: https://dle.rae.es/?id=DldD5zV (consulta:1 de septiembre de 2019).

Dle, «gobernanza». Disponible en: https://dle.rae.es/?id=JHRSmFV (consulta: 10 de julio de 2019).

Dle, «internet». Disponible en: https://dle.rae.es/internet (consulta: 2 de diciembre de 2020).

Dle, «red». Disponible en: https://dle.rae.es/?id=VXs6SD8 (consulta: 2 de abril de 2019).

Dle, «router». Disponible en: https://dej.rae.es/lema/router (consulta: 4 de junio de 2019).

Dle, «segmento». Disponible en: https://dle.rae.es/segmento?m=form (consulta: 10 de diciembre de 2019).

Dle, «software». Disponible en: Disponible en: http://dle.rae.es/?id=YErlG2H (consulta: 10 de julio de 2019).

Diccionario panhispánico del español jurídico, «router». Disponible en: https://dej.rae.es/lema/router (consulta: 4 de junio de 2019).

Dirección de Tecnologías de la Información y las Comunicaciones (DTIC), Declaración de servicios compartidos, pp. 76. NIPO: 630-15-211-9. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:ed0ea576-d9fc-4c7f-a8bf-45314ea5aaab/20151002-Declaracion-servicios-compartidos.pdf (consulta: 9 de enero de 2021).

Dirección de Tecnologías de la Información y las Comunicaciones (DTIC). Documento electrónico. Guía de aplicación de la Norma Técnica de Interoperabilidad (en línea). 2ª ed., Ministerio de Hacienda y Administraciones Públicas, 2016, pp. 54. Disponible en: https://administracionelectronica.gob.es/pae_Home/dam/jcr:5881e773-6d5d-48b6-b4a6-7760e63fcfef/Guia_NTI_documento_electronico_PDF_2ed_2016.pdf (consulta: 15 de noviembre de 2020).

Dirección de Tecnologías de la Información y las Comunicaciones (DTIC), «Guía de aplicación de la Norma Técnica de Interoperabilidad de Política de gestión de documentos electrónicos (2ª edición electrónica)». P. 31. Disponible esta publicación en el Portal de Administración Electrónica (PAe): http://administracionelectronica.gob.es/ (consulta 8 de enero de 2021).

EDPB (@EU_EDPB), «In need of some extra information on the Art. 65 procedure? We've got you covered! You can consult our FAQ on the Art. 65 procedure on the EDPB website: https://europa.eu/!mn73Dm or take a closer look at the different steps in the procedure in the infographic below:», 15 de diciembre de 2020, 16:39 (Tuit). Disponible en: https://twitter.com/EU_EDPB/status/1338871251608219655 (consulta: 16 de diciembre de 2020).

Google, Google Domains. Disponible en: https://domains.google/intl/es-419_ALL/learn/the-difference-between-a-url-domain-website-more.html#/ (consulta: 7 de noviembre de 2018).

Facebook, Anatomy of Facebook. Disponible en: https://www.facebook.com/notes/facebook-data-team/anatomy-of-facebook/10150388519243859 (consulta: 6 de abril de 2019).

Facebook, Información de la empresa Facebook. Disponible en: https://www.facebook.com/facebook/about/?entry_point=page_nav_about_item&tab=page_info (Consulta: 12 junio 2017).

Facultad de Derecho, Boletín de jurisprudencia Constitucional, IV Jurisprudencia constitucional extranjera. Disponible en: https://www.u-cursos.cl/derecho/2008/0/DIPDERINFO/1/material_docente/bajar?id_material=163485 (consulta: 15 de junio de 2017).

Flickr, https://www.flickr.com/about (consulta: 21 de mayo de 2019).

Fundéu, «bot». Disponible en: https://www.fundeu.es/recomendacion/bot-acortamiento-valido-en-espanol/ (consulta: 19 de diciembre de 2019).

Fundéu, «prosumidor». Disponible en: https://www.fundeu.es/recomendacion/prosumidor-en-espanol-mejor-que-prosumer-1292/ (consulta: 6 de abril de 2019).

Fundéu, «mensajería instantánea». Disponible en: https://www.fundeu.es/escribireninternet/mensajeria-instantanea/ (consulta: 7 de junio de 2019).

Fundéu, «etiqueta mejor que hashtag». Disponible en: https://www.fundeu.es/recomendacion/etiqueta-mejor-que-hashtag-958/ (consulta: 27 de mayo de 2019).

GARCÍA-ESCUDERO MÁRQUEZ, P., «Sinopsis artículo 81» (en línea), *Constitución española,* disponible en: https://app.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=81&tipo=2 (consulta: 4 de enero de 2021).

Google, Políticas de privacidad. Disponible en: https://www.gstatic.com/policies/privacy/pdf/20190122/f3294e95/google_privacy_policy_es_eu.pdf (consulta: 30 de noviembre de 2019).

Google, ¿Cómo podemos ayudarte? Disponible en: https://support.google.com/plus/?hl=es#topic=9259565 (consulta: 8 de abril de 2019).

Google, AdSense. Disponible en: https://www.google.com/intl/es_es/adsense/start/how-it-works/#/ (consulta: 5 de mayo de 2019).

Google, Domains Beta. Disponible en: https://domains.google/intl/es-419_ALL/learn/the-difference-between-a-url-domain-website-more.html#/ (consulta: 7 de noviembre de 2018).

Google, Google Maketing Platform. Disponible en: https://marketingplatform.google.com/about/analytics/?hl=es (consulta: 5 de mayo de 2019).

Hootsuite, The Global State of Digital in 2019 Report. Disponible en: https://hootsuite.com/pages/digital-in-2019#accordion-115547 (consulta: 27 de mayo de 2019).

ICAAN, Governmental Advisory Committee. Disponible en: https://gac.icann.org/ (consulta: 9 de julio de 2019).

ICAAN, Public Technical Identifiers: https://pti.icann.org/ (consulta: 11 de julio de 2019).

ICAAN, ¿Qué hace el ICAAN?. Disponible en: https://www.icann.org/resources/pages/what-2012-02-25-es (consulta: 9 de julio de 2019).

IBM, comparación de IPv4 y IPv6 Disponible en: https://www.ibm.com/support/knowledgecenter/es/ssw_ibm_i_73/rzai2/rzai2compipv4ipv6.htm#rzai2compipv4ipv6_compdns (consulta: 11 de noviembre de 2018).

Internet Governance panel, Towards a Collaborative, Decentralized Internet Governance Ecosystemvid. Report by the Panel on Global Internet Cooperation and Governance Mechanisms, mayo 2014. Disponible en: https://netmundial.org/sites/default/files/InternetGovernancePanel-Report.pdf (consulta: 29 de septiembre de 2020).

JIMÉNEZ ASENSIO, R., «La figura del delegado de protección de datos en las organizaciones públicas» (en línea). Disponible en: https://rafaeljimenezasensio.files.wordpress.com/2018/03/articulo-dpd-4.pdf (consulta: 29 de diciembre de 2020).

Le Sénat, Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique: https://www.senat.fr/dossier-legislatif/ppl09-093.html (consulta: 19 de junio de 2017).

LinkedIn, Acerca de LinkedIn. Disponible en: https://about.linkedin.com/es-es (consulta: 8 de abril de 2019).

MeetUp, About. Disponible en: https://www.meetup.com/es-ES/about/ (consulta: 21 de mayo de 2019).

Mendeley, About. Disponible en: https://www.elsevier.com/solutions/mendeley (consulta: 6 de abril de 2019).

Merriam-Webster, «browser». Disponible en: https://www.merriam-webster.com/dictionary/browser (consulta: 6 de noviembre de 2018).

Ministerio de Hacienda y Administraciones Públicas. Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2016-10108 (consulta: 25 de septiembre de 2020).

Normas técnicas de interoperabilidad del ENI: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html#CATALOGOESTANDARES (consulta: 29 de septiembre de 2020).

OpenJur (consulta: 15 de junio de 2017). Disponible en: https://openjur.de/u/268440.html.

Orden ITC/1542/2005, de 19 de mayo, que aprueba el Plan Nacional de nombres de dominio de Internet bajo el código de país correspondiente a España («.es»). Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2005-8902 (consulta: 9 de julio de 2019).

Organización Internacional de Normalización, Public Available Standars. Disponible en: https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html (consulta 08 de octubre de 2020).

Panda security media center, Tor y Deep web: todos los secretos del lado oscuro de la red, junio 2016. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/tor-y-deepweb-todos-los-secretos/ (consulta 7 de diciembre de 2018).

Periscope, How to save a Periscope broadcast: https://help.twitter.com/en/using-twitter/save-broadcast (consulta: 17 de diciembre de 2019).

Poder Judicial de España. Disponible en: http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Noticias-Judiciales/La-Audiencia-Nacional-establece-los-criterios-para-reconocer-el--derecho-al-olvido- (consulta: 19 de junio de 2017).

Portal de administración electrónica, Normas técnicas de interoperabilidad. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html#CATALOGOESTANDARES

Protonmail, Detalles de seguridad, Disponible en: https://protonmail.com/es/security-details(consulta: 18 de diciembre de 2018).

Red.es, cuanto cuesta. Disponible en: https://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/sobre-registros-de-dominios/cuanto-cuesta (consulta: 9 de julio de 2019).

Red.es, Instrucción procedimientos dominios. Disponible en: https://www.dominios.es/dominios/es/todo-lo-que-necesitas-saber/normativa/instruccion-procedimientos-de-dominios (consulta: 9 de julio de 2019).

Researchgate, about. Disponible en: https://www.researchgate.net/about (consulta: 6 de abril de 2019).

Senado Francés [consulta: 19 de junio de 2017]. Disponible en: https://www.senat.fr/dossier-legislatif/ppl09-093.html.

Sendthisfile, Do You Know How to Send Large Files? Disponible en: https://www.sendthisfile.com/features/how-does-it-work/index.jsp (consulta: 6 de junio de 2019).

Snapchat, ¿Cuándo elimina Snapchat los Snaps y Chats? Disponible en: https://support.snapchat.com/es/a/when-are-snaps-chats-deleted (consulta: 21 de mayo de 2019).

Tabulator, Tabulator proyect. Disponible en: https://www.w3.org/2005/ajar/tab (consulta: 11 de diciembre de 2018).

The Irish Times, Google Ireland takes the reins for European services (consulta: 30 de octubre de 2019). Disponible en: https://www.irishtimes.com/business/technology/google-ireland-takes-the-reins-for-european-services-1.3730721

Transfernow, Nuestra misión. Disponible en: https://www.transfernow.net/es/acerca (consulta: 6 de junio de 2019).

Twitter, @RAEinforma. Disponible en: https://twitter.com/raeinforma/status/451459255590477824 (consulta: 15 de junio de 2017).

Twitter, *Giving you more characters to express yourself* (en línea). Jueves 26 de septiembre de 2017 Disponible en: https://blog.twitter.com/official/en_us/topics/product/2017/Giving-you-more-characters-to-express-yourself.html (consulta: 19 de octubre de 2020).

United States Department of Commerce, The White paper (en línea) Disponible en: https://www.icann.org/resources/unthemed-pages/white-paper-2012-02-25-en (consulta: 9 de julio de 2019).

Wetransfer, About. Disponible en: https://wetransfer.com/about (consulta: 6 d junio de 2019).

Wikipedia, Formulario para creación de cuentas en Wikipedia. Disponible en: https://es.wikipedia.org/w/index.php?title=Especial:Crear_una_cuenta&returnto=Discusi%C3%B3n%3ARevoluci%C3%B3n+Industrial&returntoquery=action%3Dedit%26section%3D1 (consulta: 28 de mayo de 2019).

Wikipedia, Cómo puedes colaborar. Disponible en: https://es.wikipedia.org/wiki/Ayuda:C%C3%B3mo_puedes_colaborar (consulta: 28 de mayo de 2019).

Xing. Disponible en: https://www.xing.com/es (consulta: 8 de abril de 2019).

YouTube, Cómo protege su privacidad e identidad en línea su Navegador Tor. Disponible en: https://www.youtube.com/watch?v=Sz_J6vJ4MYw&list=PLwyU2dZ3LJErtu3GGElIa7VyORE2B6H1H&index=4&t=0s (consulta: 11 de diciembre de 2018).

NOTAS DE PRENSA

El País, Debo ser más radical en lo digital (en línea), 2017. Disponible en: http://elpais.com/diario/2010/09/12/domingo/1284263555_850215.html (Consulta: 12 junio 2017).

El País, Google traslada la gestión de sus pagos online de Londres a Dublín para sortear el brexit. Disponible en: https://cincodias.elpais.com/cincodias/2019/04/03/companias/1554294595_506135.html (consulta: 30 de octubre de 2019).

El País, Más allá de Yahoo, Outlook o Gmail: estos son los correos alternativos. Disponible en: https://elpais.com/tecnologia/2017/10/11/actualidad/1507722458_050123.html (consulta: 18 de diciembre de 2018).

The Irish Times, Google Ireland takes the reins for European services. Disponible en: https://www.irishtimes.com/business/technology/google-ireland-takes-

the-reins-for-european-services-1.3730721 (consulta: 30 de octubre de 2019).

Verne, El País. 31 de marzo de 2015, 07:59 Disponible en: http://verne.elpais.com/verne/2015/03/28/articulo/1427564916_014554.html (consulta: 15 de junio de 2017).

Verne, El País, Así es Periscope, la app de Twitter para retransmitir tu vida en directo, 31 de marzo 2015. Disponible en: http://verne.elpais.com/verne/2015/03/28/articulo/1427564916_014554.html (consulta: 15 de junio de 2017).

APÉNDICE JURISPRUDENCIAL.

TEDH

STEDH de 26 de marzo de 1987, caso Leander contra Suecia (TEDH 1987\4; ECLI:CE:ECHR:1987:0326JUD000924881)

STEDH de 16 diciembre de 1992, Caso Niemietz v. Germany (TEDH 1992\77; ECLI:CE:ECHR:1992:1216JUD001371088).

STEDH de 4 diciembre 2003. Caso Müslüm Gündüz contra Turquía (TEDH 2003\81; ECLI:CE:ECHR:2003:1204JUD003507197).

STEDH de 10 de julio de 2008. Caso Soulas y otros contra Francia (TEDH 2008\42; ECLI:CE:ECHR:2008:0710JUD001594803).

STEDH de 17 de febrero de 2015, caso Guseva contra Bulgaria (TEDH 2015\52590; ECLI:CE:ECHR:2015:0217JUD000698707).

STEDH de 28 de junio de 2018. Caso M.L. et W.W. contra Allemagne (TEDH 2018\67; ECLI:CE:ECHR:2018:0628JUD006079810).

STEDH de 8 de noviembre de 2016, caso Magyar Helsinki Bizottság contra Hungría (JUR\2016\260055; ECLI:CE:ECHR:2016:1108JUD001803011).

TJUE

STJUE 6 de noviembre de 2003, Procedimiento penal contra Bodil Lindqvist. Petición de decisión prejudicial: Göta hovrätt – Suecia, asunto C-101/01 (ECLI:EU:C:2003:596).

STJUE (Gran Sala) de 9 de marzo de 2010, Comisión Europea contra República Federal de Alemania, asunto C-518/07. (TJCE\2010\68; ECLI:EU:C:2010:125).

STJUE (Gran Sala) de 9 de noviembre de 2010, Volker und Markus Schecke GbR y Hartmut Eifert contra Land Hessen, asuntos acumulados: C-92/09 y C-93/09 (ECLO:EU:C:2010:662).

STJUE de 22 de diciembre de 2010, Ilonka Sayn-Wittgenstein y Landeshauptmann von Wien, asunto C-208/09 (ECLI:EU:C:2010:806).

STJUE (Gran Sala) de 13 de mayo de 2014, Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos (AEPD) y Mario Costeja González, asunto C-131/12 (ECLI:EU:C:2014:317).

STJUE (Gran Sala) de 16 de octubre de 2012, Comisión Europea contra República de Austria, asunto C-614/10 (TJCE\2012\287; ECLI:EU:C:2012:631)

STJUE (Gran sala) 8 de abril de 2014, Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources y otros y Kärntner Landesregierung y otros, asuntos acumulados C-293/12 y C-594/12 (TJCE\2014\104; ECLI:EU:C:2014:238).

STJUE (Gran Sala) de 8 de abril de 2014, Comisión Europea contra Hungría, Asunto C-288/12 (TJCE\2014\139; ECLI:EU:C:2014:237).

STJUE (Sala Segunda) de 6 de octubre de 2015, Maximillian Schrems contra Data Protection Commissioner, asunto C-362/14 (TJCE 2015\324; ECLI:EU:C:2015:650).

STJUE (Gran Sala) de 18 de julio de 2017, Comisión Europea contra Patrick Breyer, Asunto C-213/15 P (JUR\2017\199987; ECLI:EU:C:2017:563).

STJUE (Gran Sala) de 24 de septiembre de 2019, Google LLC contra Commission nationale de l'informatique et des libertés (CNIL), asunto C-507/17 (TJCE 2019\203; ECLI:ECLI:EU:C:2019:772).

STJUE (Sala Segunda) de 19 de octubre de 2016, Patrick Breyer contra Bundesrepublik Deutschland, asunto C-582/14, (JUR\2016\268783; ECLI:EU:C:2016:779).

STJUE (Sala Segunda) 29 de julio de 2019, Fashion ID GmbH & Co.KG contra Verbraucherzentrale NRW eV, asunto C-40/17 (TJCE 2019\148; ECLI:EU:C:2019:629).

STJUE (Gran Sala) de 6 de octubre de 2020, La Quadrature du Net and Others v Premier ministre and Others. Requests for a preliminary ruling from the

Conseil d'État (France) and Cour constitutionnelle, asuntos: C-511/18, C-512/18 and C-520/18 (Belgium) (ECLI:EU:C:2020:791).

Conclusiones TJUE

Conclusiones del Abogado General Sr. Niilo Jääskinen presentadas el 25 de junio de 2013, en el asunto C-131/12, Googles Spain, S.L., Google Inc. Contra Agencia Española de Protección de datos (AEPD) y Mario Costeja González (ECLI:EU:C:2013:424) (en línea). Disponible en: http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=ES

TC

Pleno

STC (Pleno) 85/1983 de 25 octubre (RTC\1983\85; ECLI:ES:TC:1983:85).

STC (Pleno) 53/1985, de 11 de abril, (RTC\1985\53; ECLI:ES:TC:1985:53).

STC (Pleno) 27/1987, de 27 de febrero (RTC\1987\27; ECLI:ES:TC:1987:27).

STC (Pleno) 120/1990, de 27 de junio (RTC\1990\120; ECLI:ES:TC:1990:120).

STC (Pleno) 116/1999, de 17 de junio (RTC\1999\116; ECLI:ES:TC:1999:116).

STC (Pleno) 290/2000, de 30 de noviembre (RTC\2000\290; ECLI:ES:TC:2000:290).

STC (Pleno) 292/2000, de 30 de noviembre (ECLI:ES:TC:2000:292).

STC (Pleno) 10/2002, de 17 de enero (RTC 2002\10; ECLI:ES:TC:2002:10)

STC (Pleno) 17/2013, de 31 de enero (RTC 2013\17; ECLI:ES:TC:2013:17).

STC (Pleno) 177/2015, de 22 de julio (RTC 2015\177; ECLI:ES:TC:2015:177).

Sala Primera

STC (Sala Primera) 64/1986, de 21 de mayo (RTC\1986\64; ECLI:ES:TC:1986:64).

STC (Sala Primera) 6/1988, de 21 de febrero (RTC 1988\6; ECLI:ES:TC:1988:6).

STC (Sala Primera) 107/1988, de 8 de junio (RTC 1988\107; ECLI:ES:TC:1988:107).

STC (Sala Primera) 98/1989 de 1 junio (RTC 1989\98; ECLI:ES:TC:1989:98).

STC (Sala Primera) 214/1991, de 11 de noviembre (RTC\1991\214; ECLI:ES:TC:1991:214)

STC (Sala Primera) 223/1992, de 14 de diciembre (RTC 1992\223; ECLI:ES:TC:1992:223).

STC (Primera Sala) 254/1993, de 20 de julio, F.J. 6 (RTC 1993\254; ECLI:ES:TC:1993:254).

STC (Sala Primera) 139/1995, de 26 de septiembre de 1995 (RTC 1995\139; ECLI:ES:TC:1995:139).

STC (Sala Primera)134/1999, de 15 de julio (RTC 1999\134; ECLI:ES:TC:1999:134).

STC (Sala Primera) 202/1999, de 8 de noviembre (RTC 1999\202; ECLI:ES:TC:1999:202).

STC (Sala Primera)139/2001, de 18 de junio (RTC 2001\139; ECLI:ES:TC:2001:139).

STC (Sala Primera) 83/2002, de 22 de abril (RTC\2002\83; ECLI:ES:TC:2002:83)

STC (Sala Primera) 158/2009, de 29 de junio (RTC 2009\158; ECLI:ES:TC:2009:158).

Sala Segunda

STS (Sala Segunda) 6/1981, de 16 de marzo (RTC 1981\6; ECLI:ES:TC:1981:6).

STC (Sala Segunda) 30/1982, de 1 de junio (RTC 1982\30; ECLI:ES:TC:1982:30).

STC (Sala Segunda)137/1985, de 17 de octubre (RTC 1985\137; ECLI:ES:TC:1985:137)

STC (Sala Segunda) 185/1989, de 13 de noviembre (RTC 1989\185; ECLI:ES:TC:1989:185).

STC (Sala Segunda) 85/1992, de 8 de junio (RTC 1992\85; ECLI:ES:TC:1992:85).

STC (Sala Segunda) 219/1992, de 3 de diciembre (RTC 1992\219; ECLI:ES:TC:1992:219).

STC (Sala Segunda)117/1994, de 25 de abril (RTC 1994\117; ECLI:ES:TC:1994:117).

STC (Sala Segunda) 69/1999, de 26 de abril (RTC\1999\69; ECLI:ES:TC:1999:69)

STC (Sala Segunda) 94/1998, de 4 de mayo (RTC 1998\94; ECLI:ES:TC:1998:94)

STC (Sala Segunda) 180/1999, de 11 de octubre (RTC 1999\180; ECLI:ES:TC:1999:180).

STC (Sala Segunda)115/2000, de 5 de mayo (RTC 2000\115; ECLI:ES:TC:2000:115).

STC (Sala Segunda) 81/2001, 26 de marzo (RTC\2001\81; ECLI:ES:TC:2001:81)

STC (Sala Segunda) 156/2001, de 2 de julio (RTC\2001\156; ECLI:ES:TC:2001:156).

STC (Sala Segunda) 14/2003, de 28 de enero (RTC\2003\14; ECLI:ES:TC:2003:14)

STC (Sala Segunda) 176/2013, de 21 de octubre (RTC 2013\176; ECLI:ES:TC:2013:176).

Autos TC

ATC (Sección Primera) 149/1999, de 14 de junio, F.J. 2 (RTC\1999\149 AUTO; ECLI:ES:TC:1999:149A).

ATC (Sección Primera) 28/2004, de 6 de febrero (RTC 2004\28 AUTO; ECLI:ES:TC:2004:28A).

TS

Sala de lo Civil

STS (Sala de lo Civil) 241/2003, de 14 de marzo (Sala 1ª RJ 2003\2586; ECLI:ES:TS:2003:1750)

STS (Sala de lo Civil) 802/2006, de 19 de julio (RJ 2006\3991; ECLI: ES:TS:2006:4495).

STS (Sala de lo Civil) 773/2009 de 9 diciembre (RJ 2010\131; ECLI:ES:TS:2009:7684).

STS (Sala de lo Civil) 805/2013, de 7 de enero de 2014 (RJ 2014\773; ECLI:ES:TS:2014:68).

STS (Sala de lo Civil) 128/2013, de 26 de febrero (RJ 2013\2580; ECLI:ES:TS:2013:1441).

STS (Sala de lo Civil) 217/2015, de 22 de abril (RJ 2015\1358; ECLI:ES:TS:2015:1532).

STS (Sala de lo Civil) 545/2015, de 15 de octubre de 2015 (RJ 2015\4417; ECLI:ES:TS:2015:4132).

STS (Sala de los Civil) de 5 de abril (RJ 2016\1006; ECLI:ES:TS:2016:1280).

STS (Sala de los Civil) 534/2016, de 14 de septiembre (RJ 2016\4826; ECLI:ES:TS:2016:4060).

STS (Sala de lo Civil) 91/2017, de 15 de febrero (RJ 2017\302; ECLI: ES:TS:2017:363).

STS (Sala de lo Civil) 397/2019, de 5 de julio (RJ 2019\2673; ECLI:ES:TS:2019:2255).

Sala de lo Penal

STS (Sala de lo Penal) 259/2011, de 12 de abril (RJ 2011\5727; ECLI:ES:TS:2011:3386).

STS (Sala de lo Penal) 646/2018, de 14 de diciembre (RJ 2018\5588; ECLI:ES:TS:2018:4133).

Sala de lo Contencioso-administrativo

STS (Sala de lo Contencioso-administrativo) de 30 de marzo de 1999 (RJ\1999\3246; ECLI:ES:TS:1999:2206).

STS (Sala de lo Contencioso-administrativo) de 19 de mayo de 2003 (RJ 2003\3834; ECLI: ES:TS:2003:3359).

STS (Sala de lo Contencioso-administrativo) de 11 de marzo de 2006 (RJ 2016\1517; ECLI:ES:TS:2016:1057).

STS (Sala de lo Contencioso-administrativo) de 16 de febrero de 2007 (RJ 2007\739: ECLI:ES:TS:2007:954).

STS (Sala de lo Contencioso-administrativo) de 4 de mayo de 2009 (RJ\2009\5165; ECLI:ES:TS:2009:2651).

STS (Sala de lo Contencioso-administrativo) de 27 de mayo de 2009 (RJ\2009\4517; ECLI:ES:TS:2009:3589).

STS (Sala de lo Contencioso-administrativo) de 2 de diciembre de 2011 (RJ\2012\2585; ECLI:ES:TS:2011:8497).

STS (Sala de lo Contencioso-administrativo) de 11 de enero 2019 (RJ 2019\8; ECLI:ES:TS:2019:19).

Autos TS

ATS (Sala de lo Civil) de 11 de octubre de 2016 (recurso 3083/2015; JUR 2016\224928; ECLI:ES:TS:2016:9170A).

AN

Sala de lo Contencioso

SAN Sección 1ª, de 16 de febrero de 2005 (JUR\2005\222020; ECLI:ES:AN:2005:901).

SAN de 20 de mayo de 2005 (JUR\2005\249468; ECLI:ES:AN:2005:2635).

SAN de 1 de octubre de 2008 (RJCA\2009\310; ECLI: ES:AN:2008:5744).

SAN de 3 de diciembre de 2013 (RJCA 2014\496; ECLI:ES:AN:2013:5414).

SAN de 29 de diciembre de 2014 (RJCA 2015\183; ECLI:ES:AN:2014:5202).

SAN de 29 de diciembre de 2014 (RJCA 2014\1065; ECLI:ES:AN:2014:5129).

SAN de 29 diciembre de 2014 (JUR 2015\26253; ECLI:ES:AN:2014:5211).

SAN de 29 diciembre de 2014 (JUR 2015\26747; ECLI:ES:AN:2014:5198).

SAN de 29 diciembre de 2014 (JUR 2015\27215; ECLI:ES:AN:2014:5210).

SAN de 30 de diciembre de 2014 (JUR 2015\58115; ECLI:ES:AN:2014:5243).

SAN de 29 diciembre de 2014 (JUR 2015\58789: ECLI:ES:AN:2014:5249).

SAN de 29 diciembre de 2014 (JUR 2015\59185; ECLI: ES:AN:2014:5251).

SAN de 30 de diciembre de 2014 (JUR 2015\59844; ECLI:ES:AN:2014:5248).

SAN de 29 de diciembre de 2014 (JUR 2015\68260; ECLI: ECLI:ES:AN:2014:5252).

SAN de 30 de diciembre de 2014 (JUR 2015\57618; ECLI:ES:AN:2014:5241).

SAN de 3 de febrero de 2015 (JUR 2015\58568; ECLI:ES:AN:2015:344).

SAN de 3 de febrero de 2015 (JUR 2015\58992; ECLI:ES:AN:2015:342).

SAN de 12 de febrero de 2015 (JUR 2015\88275; ECLI:ES:AN:2015:643).

SAN de 19 de febrero de 2015 (JUR 2015\88582; ECLI:ES:AN:2015:622).

SAN de 19 de febrero de 2015 (JUR 2015\89367; ECLI:ES:AN:2015:649).

SAN de 17 de febrero de 2015 (JUR 2015\89705; ECLI:ES:AN:2015:661).

SAN de 24 de febrero de 2015 (JUR 2015\82308; ECLI:ES:AN:2015:568).

SAN de 14 de mayo de 2015(RJCA\2015\845; ECLI:ES:AN:2015:2259.)

SAN de 9 de junio de 2015 (RJCA 2015\842: ECLI:ES:AN:2015:2149).

SAN de 2 de octubre de 2015 (RJCA 2015\869; ECLI:ES:AN:2015:3501).

SAN de 6 de octubre de 2015 (JUR 2016\14341; ECLI: ES:AN:2015:4456).

SAN 562/2016, de 18 de noviembre de 2016 (RJCA 2017\466; ECLI:ES:AN:2016:4713).

SAN de 6 de junio de 2017 (JUR 2017\206541; ECLI:ES:AN:2017:3111).

SAN de 11 de mayo de 2017 (RJCA 2017\487; ECLI:ES:AN:2017:2433).

SAN de 19 de junio de 2017 (RJCA 2017\559; ECLI:ES:AN:2017:2562).

SAN de 13 de julio de 2017 (JUR 2017\208178; ECLI:ES:AN:2017:3257).

SAN de 18 de julio de 2017 (JUR 2017\206454; ECLI:ES:AN:2017:3029).

SAN de 25 de julio de 2017 (JUR 2017\207817; ECLI:ES:AN:2017:3260).

SAN de 31 de octubre de 2017(JUR 2017\306556; ECLI:ES:AN:2017:4412).

SAN de 31 de octubre de 2017 (JUR 2018\6478; ECLI:ES:AN:2017:4674).

SAN de 4 de diciembre de 2017 (JUR 2018\12571; ECLI:ES:AN:2017:5091).

SAN de 2 de enero de 2018 (JUR 2018\64230; ECLI:ES:AN:2018:509).

SAN de 27 de abril de 2018 (RJCA 2018\607; ECLI:ES:AN:2018:1929).

SAN de 10 de mayo de 2018 (JUR 2018\144348; ECLI:ES:AN:2018:1932).

SAN de 2 de noviembre de 2018 (JUR 2018\331762; ECLI:ES:AN:2018:4476).

SAN de 11 de diciembre de 2018 (RJCA 2018\1869; ECLI:ES:AN:2018:5427).

SAN de 12 de diciembre de 2018 (RJCA 2018\1657; ECLI:ES:AN:2018:5065).

SAN de 14 de diciembre de 2018 (JUR 2019\48088; ECLI:ES:AN:2018:5038).

SAN de 14 de diciembre de 2018 (JUR 2019\48440; ECLI:ES:AN:2018:5045).

SAN de 19 de diciembre de 2018 (JUR 2019\80800; ECLI:ES:AN:2018:5432).

SAN de 21 de diciembre de 2018 (JUR 2019\48876; ECLI:ES:AN:2018:5066).

SAN de 8 de enero de 2019 (JUR 2019\137033; ECLI:ES:AN:2019:1243).

SAN de 26 de enero de 2018 (JUR 2018\101897; ECLI:ES:AN:2018:1033).

SAN de 26 de diciembre de 2018 (JUR 2019\48444; ECLI:ES:AN:2018:5064).

SAN de 27 de noviembre de 2018 (JUR 2019\26446; ECLI:ES:AN:2018:4712).

SAN 22 de enero de 2019 (JUR 2019\81313; ECLI:ES:AN:2019:507).

SAN de 12 de febrero de 2019 (JUR 2019\77084; ECLI:ES:AN:2019:403).

SAN de 14 de febrero de 2019 (JUR 2019\80463; ECLI:ES:AN:2019:514).

SAN de 26 de febrero de 2019 (JUR 2019\123159; ECLI:ES:AN:2019:998).

SAN de 15 de marzo de 2019 (JUR 2019\111973; ECLI:ES:AN:2019:782).

SAN de 26 de marzo de 2019 (JUR 2019\127544; ECLI:ES:AN:2019:1117).

SAN de 26 de marzo de 2019 (JUR 2019\128004; ECLI:ES:AN:2019:1120).

SAN de 26 de marzo de 2019 (JUR 2019\137227; ECLI:ES:AN:2019:1329).

SAN de 26 de marzo de 2019 (JUR 2019\159830; ECLI:ES:AN:2019:1549).

SAN de 26 de marzo 2019 (JUR\2019\201813; ECLI:ES:AN:2019:2386).

SAN de 2 de abril de 2019 (RJCA 2019\170; ECLI:ES:AN:2019:1805).

SAN de 2 de abril de 2019 (RJCA 2019\564; ECLI:ES:AN:2019:1806).

SAN de 2 de abril de 2019 (RJCA 2019\565; ECLI:ES:AN:2019:1804).

SAN de 22 de abril de 2019 (RJCA 2019\317; ECLI:ES:AN:2019:1996).

SAN de 24 de abril de 2019 (RJCA 2019\571; ECLI:ES:AN:2019:1801).

SAN de 9 de mayo de 2019 (RJCA 2019\781; ECLI:ES:AN:2019:2766).

SAN de 9 de mayo de 2019 (JUR 2019\227525; ECLI:ES:AN:2019:2764).

SAN de 16 de mayo de 2019 (JUR 2019\189339; ECLI:ES:AN:2019:2063).

SAN de 21 de junio de 2019 (JUR 2019\213368; ECLI:ES:AN:2019:2593).

SAN de 21 de junio de 2019 (JUR 2019\231991; ECLI:ES:AN:2019:2899).

SAN de 21 de junio de 2019 (JUR 2019\232080; ECLI:ES:AN:2019:2897).

SAN de 24 de julio de 2019 (JUR 2019\269932; ECLI:ES:AN:2019:3348).

SAN de 13 de septiembre de 2019 (JUR 2019\278879; ECLI:ES:AN:2019:3447).

SAN de 20 de septiembre de 2019 (JUR 2019\281494; ECLI:ES:AN:2019:3483).

Sentencias de Audiencias Provinciales

SAP de A Coruña (Sección 4ª) 88/2017, de 10 marzo (AC 2017\838; ECLI: ES:APC:2017:535).

SAP de Asturias 233/2017, de 10 mayo (JUR 2017\174442; ECLI:ES:APO:2017:1675).

SAP de Alicante (Sección 4ª) 366/2014, de 4 diciembre (AC 2015\401; ECLI:ES:APA:2014:4043).

SAP de León (Sección 2ª) 254/2017, de 27 octubre (JUR 2017\292938; ECLI:ES:APLE:2017:1040).

SAP de Sevilla (Sección 8ª) 259/2015, de 8 septiembre (JUR 2016\231770; ECLI:ES:APSE:2015:3634)

Juzgados de Primera Instancia

Sentencia 235/2014 del Juzgado de Primera Instancia de Sevilla (AC\2014\1875; ECLI:ES:JPI:2014:154).

Bundesverfassungsgericht

OpenJur, BVerfG, Urteil des Ersten Senats vom 15 Dezember 1983 (ECLI:DE:BVerfG:1983:rs19831215.1bvr020983)

RESOLUCIONES

AEPD

Procedimientos de tutela de derechos:

- R/01046/2007 de 20 de noviembre de 2007 (TD/00463/2007).
- R/00155/2009 de 4 de febrero de 2009 (TD/01335/2008).
- R/01680/2010, de 30 de julio de 2010 (TD/00650/2010).

Recursos de reposición:

- Nº RR/00606/2016 (Procedimiento Nº: A/00118/2016).

Resolución de procedimientos de carácter sancionador:

- PS/00361/2018.
- PS/00365/2018.
- PS/00374/2018.
- PS/00393/2018.
- PS/00406/2018.
- PS/00410/2018.
- PS/00430/2018.
- PS/00009/2019.
- PS/00012/2019.
- PS/00073/2019.
- PS/00066/2019.
- PS/00106/2019.
- PS/00171/2019.
- PS/00201/2019.
- PS/00222/2019
- PS/00241/2019.
- PS/00252/2019.
- PS/00318/2019.
- PS/00347/2019.
- PS/00363/2019.
- PS/00376/2019.
- PS/00380/2019.
- PS/00381/2019.
- PS/00382/2019.
- PS/00001/2020.

Archivo de actuaciones:

- Expediente Nº E/00561/2004.

CTBG

Criterios interpretativos

- CI/002/2019, de 20 de diciembre de 2019, Publicidad activa (1). Concepto y naturaleza.
- CI/003/2019, de 20 de diciembre de 2019, Publicidad activa (2). Ámbito subjetivo.

Resoluciones

- Resolución 0075/2016 del CTBG, de 17 de mayo de 2016, p. 9-10.

CTBG y AEPD

Criterios interpretativos

- CI/001/2015 de 24 de junio de 2015, Alcance de las obligaciones de los órganos, organismos y entidades del sector público estatal en materia de acceso a la información pública sobre sus Relaciones de Puestos de Trabajo (RPT), catálogos, plantillas orgánicas, etc…y retribuciones de los empleados públicos.
- CI/002/2015 de 24 de junio, aplicación de los límites al derecho de acceso a la información
- CI/004/2015, de 23 de julio de 2015, Publicidad activa de los datos del DNI y de la firma manuscrita.

Secretaría de Estado de Administraciones Públicas

- Resolución de 7 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de Informe del Estado de la Seguridad. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2016-10108(consulta: 25 de septiembre de 2020).
- Resolución de 28 de junio de 2012, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de

Interoperabilidad de Política de gestión de documentos electrónicos. Disponible en: https://www.boe.es/buscar/act.php?id=BOE-A-2012-10048 (consulta 8 de enero de 2021).

Tribunal Administrativo de Recursos Contractuales de Castilla y León.

- Resolución 118/2019, de 1 de agosto, del Tribunal Administrativo de Recursos Contractuales de Castilla y León, por la que se estima parcialmente el recurso especial en materia de contratación interpuesto por la Empresa ASPY Prevención S.L., contra los pliegos que han de regir el procedimiento de contratación de los Servicios de Prevención de Riesgos Laborales para la Administración de la Comunidad de Castilla y León.

ÍNDICE NORMATIVO

Ámbito internacional

- Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Roma, 4 de noviembre de 1950.
- Pacto Internacional de Derechos Civiles y Políticos, hecho en Nueva York el 19 de diciembre de 1966.
- Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981 (Convenio 108).
- Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, relativo a las autoridades de supervisión y a los flujos transfronterizos de datos (Strasbourg, 08 Nov 2001)
- Protocolo de enmienda del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE N.º 108) (Elsinore, Denmark, 17-18 May 2018).

Normativa comunitaria

- Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01).
- 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.
- 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.
- Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica.

- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior.
- 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.
- Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público.
- Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.
- Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009, por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) no. 2006/2004 sobre la cooperación en materia de protección de los consumidores.
- Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público.
- Directiva 2014/23/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la adjudicación de contratos de concesión Texto pertinente a efectos del EEE.

- Directiva 2014/24/UE del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, sobre contratación pública y por la que se deroga la Directiva 2004/18/CE Texto pertinente a efectos del EEE.
- Directiva 2015/1535, del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por el que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (versión codificada).
- 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 y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.
- Directiva 2018/1972 del Parlamento Europeo y del Consejo, de 11 de diciembre de 2018, por la que se establece el Código Europeo de las Comunicaciones Electrónicas.
- Directiva 2019/1024, del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público (versión refundida).
- Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, 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 (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.
- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 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.

- 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 (Reglamento general de protección de datos -RGPD-).

- Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE (Texto pertinente a efectos del EEE.).

- Reglamento (UE) 2019/517 del Parlamento Europeo y del Consejo, de 19 de marzo de 2019, sobre la aplicación y el funcionamiento del nombre de dominio de primer nivel «.eu», por el que se modifica y se deroga el Reglamento (CE) n.° 733/2002 y se deroga el Reglamento (CE) n.° 874/2004 de la Comisión

- Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, 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 (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 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.

- 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 (Reglamento general de protección de datos -RGPD-).
- Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE (Texto pertinente a efectos del EEE.).
- Reglamento (UE) 2019/517 del Parlamento Europeo y del Consejo, de 19 de marzo de 2019, sobre la aplicación y el funcionamiento del nombre de dominio de primer nivel «.eu», por el que se modifica y se deroga el Reglamento (CE) n.° 733/2002 y se deroga el Reglamento (CE) n.° 874/2004 de la Comisión
- Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, 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 (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.
- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 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.
- 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 (Reglamento general de protección de datos -RGPD-).

- Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE (Texto pertinente a efectos del EEE.).
- Reglamento (UE) 2019/517 del Parlamento Europeo y del Consejo, de 19 de marzo de 2019, sobre la aplicación y el funcionamiento del nombre de dominio de primer nivel «.eu», por el que se modifica y se deroga el Reglamento (CE) n.° 733/2002 y se deroga el Reglamento (CE) n.° 874/2004 de la Comisión
- Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, 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 (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión.
- Reglamento (UE) nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 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.
- 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 (Reglamento general de protección de datos -RGPD-).

- Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.° 45/2001 y la Decisión n.° 1247/2002/CE (Texto pertinente a efectos del EEE.).
- Reglamento (UE) 2019/517 del Parlamento Europeo y del Consejo, de 19 de marzo de 2019, sobre la aplicación y el funcionamiento del nombre de dominio de primer nivel «.eu», por el que se modifica y se deroga el Reglamento (CE) n.° 733/2002 y se deroga el Reglamento (CE) n.° 874/2004 de la Comisión
- Propuesta de Reglamento del Parlamento europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas por el que se deroga la Directiva 2002/58/CE (Reglamento sobre privacidad y comunicaciones electrónicas-e-Privacy-).
- Tratado de Funcionamiento de la Unión Europea (versión consolidada).
- Tratado de la Unión Europea (versión consolidada).

Normativa nacional

Anteproyecto de la Constitución Española, Boletín Oficial de las Cortes el día 5 de enero de 1978.

Diario de Sesiones del Congreso de los Diputados (DSCD) núm. 70, de fecha 19 de mayo de 1978

Constitución Española de 1978.

Ley Orgánica 3/1979, de 18 de diciembre, de Estatuto de Autonomía para el País Vasco.

Ley Orgánica 1/1981, de 6 de abril, de Estatuto de Autonomía para Galicia.

Ley Orgánica 7/1981, de 30 de diciembre, de Estatuto de Autonomía para Asturias.

Ley Orgánica 8/1981, de 30 de diciembre, de Estatuto de Autonomía para Cantabria.

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.

Ley Orgánica 3/1982, de 9 de junio, de Estatuto de Autonomía de La Rioja.

Ley Orgánica 4/1982, de 9 de junio, de Estatuto de Autonomía para la Región de Murcia.

Ley Orgánica 5/1982, de 1 de julio, de Estatuto de Autonomía de la Comunidad Valenciana.

Ley Orgánica 9/1982, de 10 de agosto, de Estatuto de Autonomía de Castilla-La Mancha.

Ley Orgánica 13/1982, de 10 de agosto, de reintegración y amejoramiento del Régimen Foral de Navarra.

Ley Orgánica 3/1983, de 25 de febrero, de Estatuto de Autonomía de la Comunidad de Madrid.

Ley Orgánica 2/1984, de 26 de marzo, reguladora del derecho de rectificación.

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

Ley Orgánica 4/1997, de 4 de agosto, por la que se regula la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad en lugares públicos.

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

Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social.

Ley Orgánica 6/2006, de 19 de julio, de reforma del Estatuto de Autonomía de Cataluña.

Ley Orgánica 1/2007, de 28 de febrero, de reforma del Estatuto de Autonomía de las Illes Balears.

Ley Orgánica 2/2007, de 19 de marzo, de reforma del Estatuto de Autonomía para Andalucía.

Ley Orgánica 5/2007, de 20 de abril, de reforma del Estatuto de Autonomía de Aragón.

Ley Orgánica 14/2007, de 30 de noviembre, de reforma del Estatuto de Autonomía de Castilla y León.

Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.

Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público.

Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Ley 10/2014, de 3 de diciembre, de accesibilidad.

Ley 19/2014, de 9 de mayo, General de Telecomunicaciones.

Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado.

Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LPAC).

Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP).

Legislación autonómica

Andalucía

Ley 4/1989, de 12 de diciembre, de Estadística de la Comunidad Autónoma de Andalucía.

Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.

Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.

Aragón

Ley 6/1986, de 28 de noviembre, de Archivos de Aragón.

Ley 8/2015, de 25 de marzo, de Transparencia de la Actividad Pública y Participación Ciudadana de Aragón.

Asturias

Ley del Principado de Asturias 1/2001, de 6 de marzo, de Patrimonio Cultural.

Ley del Principado de Asturias 7/2006, de 3 de noviembre, de Estadística.

Ley 8/2018, de 14 de septiembre, de Transparencia, Buen Gobierno y Grupos de Interés. Comunidad Autónoma del Principado de Asturias.

Canarias

Ley 19/2014, de 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Extremadura

Ley 4/2003, de 20 de marzo, de Estadística de la Comunidad Autónoma de Extremadura.

Ley 2/2007, de 12 de abril, de Archivos y Patrimonio Documental de Extremadura.

Ley 4/2013, de 21 de mayo, de Gobierno Abierto de Extremadura.

Galicia

Ley 9/1988, de 19 de julio, de Estadística de Galicia.

Ley 7/2014, de 26 de septiembre, de archivos y documentos de Galicia.

Ley 1/2016, de 18 de enero, de transparencia y buen gobierno. Comunidad Autónoma de Galicia.

Islas Baleares

Ley 4/1994, de 24 de mayo, de Archivos y Patrimonio Documental de La Rioja.

Ley 3/2002 de 17 de mayo, de Estadística de las Illes Balears.

Ley 15/2006, de 17 de octubre, de archivos y patrimonio documental de las Illes Balears.

Ley 4/2011, de 31 de marzo, de la buena administración y del buen gobierno de las Illes Balears.

La Rioja

Ley 2/2005, de 1 de marzo, de Estadística de La Rioja.

Ley 3/2014, de 11 de septiembre, de Transparencia y Buen Gobierno de La Rioja.

Madrid

Ley 4/1993, de 21 de abril, de Archivos y Patrimonio Documental de la Comunidad de Madrid.

Ley 2/2004, de 25 de febrero, de Ficheros de Datos de Carácter Personal de Titularidad Pública y de Creación de la Agencia Vasca de Protección de Datos.

Valencia

Ley 5/1990, de 7 de junio, de estadística de la Comunidad Valenciana.

Ley 3/2005, de 15 de junio, de Archivos de Valencia.

Ley 2/2015, de 2 de abril, de Transparencia, Buen Gobierno y Participación Ciudadana de la Comunitat Valenciana.

Reales Decretos-legislativos

Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público.

Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

Reales Decretos

Real Decreto 1517/1981, de 8 de julio, sobre traspasos de servicios de la Seguridad Social a la Generalidad de Cataluña en materia de Seguridad Social

Real Decreto 2434/1982, de 24 de julio, sobre traspaso de funciones y servicios del Estado a la Comunidad Autónoma de Galicia en materia de cultura.

Real Decreto 3023/1983, de 13 de octubre, sobre traspaso de funciones y servicios del Estado a la Comunidad Autónoma de La Rioja en materia de cultura.

Real Decreto 680/1985, de 19 de abril, sobre traspaso de funciones y servicios de la Administración del Estado a la Comunidad de Madrid en materia de cultura

Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos.

Real Decreto 1164/2002, de 8 de noviembre, por el que se regula la conservación del patrimonio documental con valor histórico, el control de la eliminación de otros documentos de la Administración General del Estado y sus

organismos públicos y la conservación de documentos administrativos en soporte distinto al original.

Real Decreto 183/2004, de 30 de enero, por el que se regula la tarjeta sanitaria individual.

Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional.

Real Decreto 424/2005, de 15 de abril, por el que se aprueba el Reglamento sobre las condiciones para la prestación de servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios

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.

Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la administración electrónica (ENI).

Real Decreto 897/2011, de 24 de junio, sobre ampliación de las funciones y servicios de la Administración General del Estado traspasados a la Comunidad Autónoma del País Vasco por el Real Decreto 3069/1980, de 28 de septiembre, en materia de gestión de archivos de titularidad estatal.

Real Decreto 1708/2011, de 18 de noviembre, por el que se establece el Sistema Español de Archivos y se regula el Sistema de Archivos de la Administración General del Estado y de sus Organismos Públicos y su régimen de acceso.

Real Decreto 410/2016, de 31 de octubre, por el que se aprueba el Plan Estadístico Nacional 2017-2020.